CONTEMPORARY MATHEMATICS

224

Recent Progress in Algebra

An International Conference on Recent Progress in Algebra
August 11-15, 1997
KAIST, Taejon, South Korea

Sang Geun Hahn
Hyo Chul Myung
Efim Zelmanov
Editors

American Mathematical Society

http://dx.doi.org/10.1090/conm/224

Selected Titles in This Series

224 **Sang Geun Hahn, Hyo Chul Myung, and Efim Zelmanov, Editors,** Recent progress in algebra, 1999

223 **Bernard Chazelle, Jacob E. Goodman, and Richard Pollack, Editors,** Advances in discrete and computational geometry, 1999

222 **Kang-Tae Kim and Steven G. Krantz, Editors,** Complex geometric analysis in Pohang, 1999

221 **J. Robert Dorroh, Giséle Ruiz Goldstein, Jerome A. Goldstein, and Michael Mudi Tom, Editors,** Applied analysis, 1999

220 **Mark Mahowald and Stewart Priddy, Editors,** Homotopy theory via algebraic geometry and group representations, 1998

219 **Marc Henneaux, Joseph Krasil′shchik, and Alexandre Vinogradov, Editors,** Secondary calculus and cohomological physics, 1998

218 **Jan Mandel, Charbel Farhat, and Xiao-Chuan Cai, Editors,** Domain decomposition methods 10, 1998

217 **Eric Carlen, Evans M. Harrell, and Michael Loss, Editors,** Advances in differential equations and mathematical physics, 1998

216 **Akram Aldroubi and EnBing Lin, Editors,** Wavelets, multiwavelets, and their applications, 1998

215 **M. G. Nerurkar, D. P. Dokken, and D. B. Ellis, Editors,** Topological dynamics and applications, 1998

214 **Lewis A. Coburn and Marc A. Rieffel, Editors,** Perspectives on quantization, 1998

213 **Farhad Jafari, Barbara D. MacCluer, Carl C. Cowen, and A. Duane Porter, Editors,** Studies on composition operators, 1998

212 **E. Ramírez de Arellano, N. Salinas, M. V. Shapiro, and N. L. Vasilevski, Editors,** Operator theory for complex and hypercomplex analysis, 1998

211 **Józef Dodziuk and Linda Keen, Editors,** Lipa's legacy: Proceedings from the Bers Colloquium, 1997

210 **V. Kumar Murty and Michel Waldschmidt, Editors,** Number theory, 1998

209 **Steven Cox and Irena Lasiecka, Editors,** Optimization methods in partial differential equations, 1997

208 **Michel L. Lapidus, Lawrence H. Harper, and Adolfo J. Rumbos, Editors,** Harmonic analysis and nonlinear differential equations: A volume in honor of Victor L. Shapiro, 1997

207 **Yujiro Kawamata and Vyacheslav V. Shokurov, Editors,** Birational algebraic geometry: A conference on algebraic geometry in memory of Wei-Liang Chow (1911–1995), 1997

206 **Adam Korányi, Editor,** Harmonic functions on trees and buildings, 1997

205 **Paulo D. Cordaro and Howard Jacobowitz, Editors,** Multidimensional complex analysis and partial differential equations: A collection of papers in honor of François Treves, 1997

204 **Yair Censor and Simeon Reich, Editors,** Recent developments in optimization theory and nonlinear analysis, 1997

203 **Hanna Nencka and Jean-Pierre Bourguignon, Editors,** Geometry and nature: In memory of W. K. Clifford, 1997

202 **Jean-Louis Loday, James D. Stasheff, and Alexander A. Voronov, Editors,** Operads: Proceedings of Renaissance Conferences, 1997

201 **J. R. Quine and Peter Sarnak, Editors,** Extremal Riemann surfaces, 1997

200 **F. Dias, J.-M. Ghidaglia, and J.-C. Saut, Editors,** Mathematical problems in the theory of water waves, 1996

199 **G. Banaszak, W. Gajda, and P. Krasoń, Editors,** Algebraic K-theory, 1996

(Continued in the back of this publication)

This page intentionally left blank

Recent Progress in Algebra

This page intentionally left blank

CONTEMPORARY MATHEMATICS

224

Recent Progress in Algebra

An International Conference on
Recent Progress in Algebra
August 11–15, 1997
KAIST, Taejon, South Korea

Sang Geun Hahn
Hyo Chul Myung
Efim Zelmanov
Editors

American Mathematical Society
Providence, Rhode Island

The International Conference on Recent Progress in Algebra was held at KAIST, Taejon, South Korea, August 11–15, 1997.

1991 *Mathematics Subject Classification.* Primary 00B20, 05D05, 05E15, 05E25, 11G09, 11F11, 11F75, 11G09, 11R18, 11R33, 17B10, 17B37, 17B65, 17B70, 17D05, 19A31, 20C15, 20C20, 20E18, 20F05, 20F50.

Library of Congress Cataloging-in-Publication Data

International Conference on Recent Progress in Algebra (1997 : Taejŏn-si, Korea)

Recent progress in algebra : an International Conference on Recent Progress in Algebra, August 11–15, 1997, KAIST, Taejon, South Korea / Sang Geun Hahn, Hyo Chul Myung, Efim Zelmanov, editors.

p. cm. — (Contemporary mathematics, ISSN 0271-4132 ; 224)

Includes bibliographical references.

ISBN 0-8218-0972-5 (alk. paper)

1. Algebra—Congresses. I. Hahn, S. G. (Sang Geun) II. Myung, Hyo Chul, 1937– . III. Zelmanov, Efim, 1955– . IV. Title. V. Series: Contemporary mathematics (American Mathematical Society) ; v. 224.

QA150.I568 1997

512—dc21 98-35282

CIP

∞ The paper used in this book is acid-free and falls within the guidelines
established to ensure permanence and durability.
Visit the AMS home page at URL: `http://www.ams.org/`

10 9 8 7 6 5 4 3 2 1 04 03 02 01 00 99

Contents

Foreword

An international conference "Recent Progress in Algebra" was held at the Korea Advanced Institute of Science and Technology (KAIST) and Korea Institute for Advanced Study (KIAS), Korea, during August 11–15, 1997. This conference was primarily organized by the Research Center of Algebra and its Applications at KAIST which was supported by fundings from the Korea Science and Engineering Foundation (KOSEF).

The purpose of this conference was to bring together the central topics and their progress in algebra, combinatorics, algebraic geometry, and number theory. The conference also served as an impetus for research activities by both young and established Korean mathematicians in these fields. The present volume contains selected papers contributed by participants in the conferences. These papers cover a wide range of topics in the aforementioned areas, which in our opinion reflects the true character of modern algebra.

We are grateful to KOSEF who provided generous fundings for the conference through the Research Center of Algebra and its Applications, and to KIAS for the support of additional fundings during the preparation of the conference.

We gratefully acknowledge the valuable assistance of the members of the Local Organizing Committee, S. Bae, S. Kang, D. Kim, J. Koo, H. Lee, and many graduate students at the Mathematics Department of KAIST for the preparation of the conference. We also wish to thank the participants of the conference for their enthusiasm, and in particular, those who presented excellent talks and contributed papers.

Our special thanks goes to Christine Thivierge from the AMS for the thoughtful assistance during the preparation of this volume, and to many anonymous referees who offered valuable suggestions for the final organization of the manuscripts.

May, 1998

Sang Geun Hahn,

Hyo C. Myung,

Efim Zelmanov

Editors

This page intentionally left blank

http://dx.doi.org/10.1090/conm/224/03185

Contemporary Mathematics
Volume **224**, 1999

A double complex for computing the sign-cohomology of the universal ordinary distribution

Greg W. Anderson

1. Introduction

For each positive integer f, a *level* f *ordinary distribution* with values in an abelian group A is a periodic function $\phi : \frac{1}{f}\mathbb{Z} \to A$ of period 1 satisfying the *level* f *distribution relations*

$$\phi(a) = \sum_{i=0}^{g-1} \phi\left(\frac{a+i}{g}\right),$$

where g is any positive integer dividing f and $a \in \frac{g}{f}\mathbb{Z}$. The *universal* level f ordinary distribution $U(f)$ is the quotient of the free abelian group on symbols of the form $[a]$ with $a \in \frac{1}{f}\mathbb{Z}/\mathbb{Z}$, modulo the level f distribution relations. An *ordinary distribution* with values in A is a function $\phi : \mathbb{Q} \to A$ such that for each positive integer f, the restriction of ϕ to $\frac{1}{f}\mathbb{Z}$ is a level f ordinary distribution; the *universal* ordinary distribution U is the direct limit of the groups $U(f)$. The group $G_f := \mathrm{Gal}\left(\mathbb{Q}(\zeta_f)/\mathbb{Q}\right) (= (\mathbb{Z}/f\mathbb{Z})^\times)$ acts naturally on the group $U(f)$, and thus in the limit $G := \mathrm{Gal}\left(\mathbb{Q}(\zeta_\infty)/\mathbb{Q}\right)(= \hat{\mathbb{Z}}^\times)$ acts on U. See Kubert's paper [**11**] or Lang's book [**13**] for background.

Let $G_\infty \subset G$ be the subgroup generated by complex conjugation. Given any abelian group M equipped with an action of G_∞, we define the *sign-cohomology* (resp. *-homology*) of M to be the Tate cohomology (resp. homology) of G_∞ with coefficients in M. The basic facts about the structure and sign-cohomology of the modules $U(f)$ and their limit U are as follows.

- Provided that $f > 1$ and $f \not\equiv 2 \bmod 4$, the sign-cohomology of $U(f)$ is in each degree a vector space over $\mathbb{F}_2$ of dimension 2^{r-1}, where r is the number of distinct primes dividing f.
- The group G_f acts trivially on the sign-cohomology of $U(f)$.
- As an abelian group, $U(f)$ is a free of rank $|G_f|$, and the natural map $U(f) \to U$ is a split monomorphism. (In particular, the limit U is a free abelian group.)
- Provided that $f > 1$ and $f \not\equiv 2 \bmod 4$, the natural map $U(f) \to U$ induces a monomorphism in sign-cohomology.

1991 *Mathematics Subject Classification.* Primary: 11R18, 11R20, 11R27, 11R29. Secondary: 20J05, 20J06.

The first and second results were obtained by Sinnott [**16**] in the course of Sinnott's calculation of unit- and Stickelberger-indices associated to the cyclotomic field $\mathbb{Q}(\zeta_f)$. The third and fourth results were obtained by Kubert [**11**], [**12**].

There is another presentation of the G_f-module $U(f)$ due to Iwasawa, which we now briefly recall. There exists a unique periodic function $u : \mathbb{Q} \to \mathbb{Q}$ of period 1 such that for all positive integers f one has

$$\sum_{\substack{0<a\leq f\\(a,f)=1}} u\left(\frac{a}{f}\right)\chi(a) = \prod_{p|f}(1-\chi(p))$$

for all primitive Dirichlet characters χ of conductor dividing f. Let $U'(f)$ be the $\mathbb{Z}[G_f]$-submodule of $\mathbb{Q}[G_f]$ generated by elements of the form

$$\sum_{\substack{0<a\leq f\\(a,f)=1}} u\left(\frac{a}{g}\right)\sigma_a^{-1} \in \mathbb{Q}[G_f]$$

where g is any positive integer dividing f and $\sigma_a\zeta_f = \zeta_f^a$. One can verify that u is an ordinary distribution; it follows that $U'(f)$ is a quotient of $U(f)$. One can verify that as an abelian group $U'(f)$ is free of rank $|G_f|$; it follows that $U'(f)$ and $U(f)$ are isomorphic G_f-modules because the underlying abelian groups are free of the same rank, namely $|G_f|$.

We hasten now to correct the misleading impression of the history of our subject created by speaking of $U'(f)$ as Iwasawa's presentation of $U(f)$. In fact, it was the module $U'(f)$ that was defined first (Iwasawa introduced it in the course of a pioneering investigation of the index of the Stickelberger ideal) and it was the module $U'(f)$ (denoted U in Sinnott's paper [**16**]) that Sinnott actually worked with. Only later was the module $U(f)$ defined by Kubert [**11**], and then part of the rationale for making the definition was to have a convenient presentation of $U'(f)$ by generators and relations.

The analogue of Sinnott's unit-index calculation [**16**], with the Carlitz module assigned to the role played in classical cyclotomic theory by the multiplicative group, was carried out by Galovich and Rosen [**7**]. Quite recently, L. S. Yin [**17**] attempted to generalize the results of Galovich-Rosen by replacing the Carlitz module with a general sign-normalized rank one Drinfeld module. Yin computed the unit-index conditional on a remarkable conjecture concerning the Galois-module structure of the sign-cohomology of the relevant analogue of $U'(f)$. Yin's conjecture is tantalizing because it seems to be just beyond the reach of the inductive method of computation introduced by Sinnott and employed by Yin.

In this paper we study some problems in the function field setting analogous to that of determining the structure and sign-cohomology of the modules $U(f)$ and their limit U, with the main goal of proving Yin's conjecture. In defining the generalization of $U(f)$ studied here, we more or less follow a definition given by Hayes [**9**] and attributed there to Mazur. In order to prove Yin's conjecture, we identify the analogue of $U'(f)$ coming up in Yin's work with the corresponding analogue of $U(f)$, and we compute the sign-cohomology of $U(f)$ by a new method involving double complexes. Our method keeps track not only of the distribution relations but also of the higher syzygies among the distribution relations. Even in the classical cyclotomic setting our method yields a new insight: provided that $f \not\equiv 2 \bmod 4$, the sign-homology of $U(f)$ is canonically isomorphic to the *Farrell-Tate homology* of the subgroup of $\mathbb{Q}^\times$ generated by -1 and the primes dividing f. The Farrell-Tate theory, which figures prominently in our proof of Yin's conjecture, was devised by Farrell [**6**] to extend Tate's well known theory for finite groups to groups of finite virtual cohomological dimension. See Brown's book [**1**] for background. In turn, Mislin [**14**] has extended Farrell's theory; the generalization, called *complete cohomology*, applies to all groups. The results of this paper suggest that more number-theoretic applications of complete cohomology can be expected. The title of the paper notwithstanding, we actually work with homology rather than cohomology because the former has functorial properties better suited to our purposes.

We mention that techniques developed in this paper have recently been applied by P. Das [**2**], [**3**] to the study of *algebraic* Γ-*monomials*, namely complex numbers of the form

$$\frac{\prod_i \Gamma(a_i)^{m_i}}{(2\pi i)^w}$$

where $a_i \in \mathbb{Q} \cap (0,1)$, $m_i \in \mathbb{Z}$, $w \in \mathbb{Z}$, and for all integers t prime to the denominators of the a_i one has

$$w = \sum_i m_i \langle t a_i \rangle$$

where $\langle x \rangle$ is the fractional part of x. Such numbers are in fact algebraic by a result of Koblitz and Ogus [**4**, Appendix] and figure in a reciprocity law due to Deligne [**4**],[**5**]; the corresponding formal sum $\sum_i m_i[a_i + \mathbb{Z}]$ represents a class in the second degree sign-cohomology of U which strongly influences the Galois-theoretic properties of the monomial. Das has proved a series of results greatly illuminating the structure of the Galois group over $\mathbb{Q}$ of the extension of $\mathbb{Q}(\zeta_\infty)$ generated by the algebraic Γ-monomials. Das has also been able to give elementary proofs of some facts about algebraic Γ-monomials which previously could only be proved with the aid of Deligne's theory of absolute Hodge cycles on abelian varieties. We conclude by noting that a function field analogue of Deligne's reciprocity law recently given by S. Sinha [**15**] suggests that Das's theory of algebraic Γ-monomials might fruitfully be extended to global fields of characteristic $p > 0$.

2. Preliminaries

2.1. Notation. The cardinality of a set S is denoted $|S|$. The difference of sets X and Y is denoted $X \setminus Y$. The group of units of a ring R is denoted $R^\times$. The fiber of a map $f : X \to Y$ at a point $y \in Y$ is denoted $f^{-1}(y)$, and the inverse image of subset $S \subseteq Y$ is denoted $f^{-1}(S)$.

2.2. Abstract nonsense. Let $\mathfrak{A}$ be an abelian category. A *chain complex* X in $\mathfrak{A}$ is a family $\{X_n\}_{n\in\mathbb{Z}}$ of objects of $\mathfrak{A}$ equipped with a family of morphisms $\{\partial_n(X) \in \mathrm{Hom}_{\mathfrak{A}}(X_n, X_{n-1})\}_{n\in\mathbb{Z}}$ such that $\partial_{n-1}(X)\partial_n(X) = 0$. A *chain map* $f : X \to Y$ of chain complexes in $\mathfrak{A}$ is a family $\{f_n \in \mathrm{Hom}_{\mathfrak{A}}(X_n, Y_n)\}_{n\in\mathbb{Z}}$ of morphisms such that $f_{n-1}\partial_n(X) = \partial_n(Y)f_n$. Given two chain maps $f, g : X \to Y$, a *homotopy* $T : f \to g$ is a family $\{T_n \in \mathrm{Hom}_{\mathfrak{A}}(X_n, Y_{n+1})\}_{n\in\mathbb{Z}}$ of morphisms such that $f_n - g_n = \partial_{n+1}(Y)T_n + T_{n-1}\partial_n(X)$; we say that f and g are *homotopic*, and we write $f \sim g$, if there exists a homotopy $T : f \to g$. Given a chain complex X in $\mathfrak{A}$ and an integer k, put

$$X[k] := X_{n-k}, \quad \partial_n(X[k]) := (-1)^k \partial_{n-k}(X),$$

thereby defining the *twist* $X[k]$. Given a chain map $f : X \to Y$ of chain complexes in $\mathfrak{A}$, put

$$\operatorname{Cone}(f)_n := \begin{bmatrix} X_{n-1} \\ Y_n \end{bmatrix}, \quad \partial_n(\operatorname{Cone}(f)) := \begin{bmatrix} -\partial_{n-1}(X) & 0 \\ f_{n-1} & \partial_n(Y) \end{bmatrix},$$

thereby defining the *mapping cone* $\operatorname{Cone}(f)$, which fits into a natural exact sequence

$$0 \to Y \to \operatorname{Cone}(f) \to X[1] \to 0$$

of chain complexes in $\mathfrak{A}$.

PROPOSITION 2.2.1. *Let $f : X \to Y$ be a chain map of chain complexes in $\mathfrak{A}$. Let S be the set of integers n such that both f_{n-1} and f_n are isomorphisms. Then there exists a chain map $e : \operatorname{Cone}(f) \to \operatorname{Cone}(f)$ such that $e \sim 1$ and $e_n = 0$ for all $s \in S$.*

PROOF. For each n, let $\phi_n : Y_n \to X_n$ be f_n^{-1} or 0 according as f_n is or is not invertible. Then the family of morphisms

$$\left\{ \begin{bmatrix} 0 & \phi_n \\ 0 & 0 \end{bmatrix} : \operatorname{Cone}(f)_n \to \operatorname{Cone}(f)_{n+1} \right\}_{n \in \mathbb{Z}}$$

is a homotopy from the identity map to a map e such that $e_n = 0$ for $n \in S$, as one verifies by a brief matrix calculation. $\square$

PROPOSITION 2.2.2. *Let $g : X \to Z$ and $h : Y \to Z$ be chain maps of chain complexes in an abelian category $\mathfrak{A}$. Make either of the following assumptions.*

1. *$H_*(\operatorname{Hom}_{\mathfrak{A}}(X_n, \operatorname{Cone}(h))) = 0$ for all n and there exists a chain map $e : \operatorname{Cone}(h) \to \operatorname{Cone}(h)$ such that $e \sim 1$ and $e_n = 0$ for all $n \ll 0$.*
2. *$H^*(\operatorname{Hom}_{\mathfrak{A}}(X, Y_n)) = 0$ and $H^*(\operatorname{Hom}_{\mathfrak{A}}(X, Z_n)) = 0$ for all n, and there exists a chain map $e : \operatorname{Cone}(h) \to \operatorname{Cone}(h)$ such that $e \sim 1$ and $e_n = 0$ for all $n \gg 0$.*

Then there exists a chain map $f : X \to Y$ unique up to homotopy such that $g \sim hf$.

PROOF. Under either hypothesis 1 or hypothesis 2, every chain map $X[k] \to \operatorname{Cone}(h)$ is homotopic to the zero map. In particular, one has $ig \sim 0$, where $i : Z \to \operatorname{Cone}(h)$ is the evident map, whence follows the existence of f after a brief matrix calculation. Moreover, the difference of any two homotopies $ig \to 0$ defines a chain map $X[1] \to \operatorname{Cone}(h)$ homotopic to the zero map, whence follows the uniqueness of f up to homotopy after another brief matrix calculation. $\square$

2.3. Farrell-Tate homology. Let G be a group. We say that a (left) G-module M (we work exclusively with left modules) is *relatively projective* if M is a direct summand of a G-module of the form $\operatorname{Ind}_{\{1\}}^G N$ for some abelian group N. Here $\operatorname{Ind}_{\{1\}}^G$ is the functor left adjoint to the restriction functor $\operatorname{Res}_{\{1\}}^G$ associating to each G-module the underlying abelian group; more generally, given a subgroup $H \subseteq G$, the corresponding restriction functor is denoted by Res_H^G, and the function left (resp. right) adjoint to Res_H^G is denoted by Ind_H^G (resp. Coind_H^G).

PROPOSITION 2.3.1. *Let G be a group, $H \subseteq G$ a subgroup of finite index, M a relatively projective G-module, and X a chain complex of G-modules.*

1. *If $\mathrm{Res}^G_{\{1\}} X$ is contractible, then $H_*(\mathrm{Hom}_G(M, X)) = 0$.*
2. *If $\mathrm{Res}^G_H X$ is contractible, then $H^*(\mathrm{Hom}_G(X, M)) = 0$.*

PROOF. There is no loss of generality in assuming that $M = \mathrm{Ind}^G_{\{1\}} N$ for some abelian group N. One has $H_*(\mathrm{Hom}_G(M, X)) = H_*(\mathrm{Hom}(N, \mathrm{Res}^G_{\{1\}} X)) = 0$, and therefore assertion 1 holds. Because H is of finite index in G, the functors Ind^G_H and Coind^G_H are isomorphic, hence $H^*(\mathrm{Hom}_G(X, M)) = H^*(\mathrm{Hom}_H(\mathrm{Res}^G_H X, \mathrm{Ind}^H_{\{1\}} N)) = 0$, and therefore assertion 2 holds. □

PROPOSITION 2.3.2. *Let G be a group. Let $g : X \to Z$ and $h : Y \to Z$ be chain maps of chain complexes of G-modules. Assume that X, Y and Z are concentrated in nonnegative degree, $\mathrm{Res}^G_{\{1\}} \mathrm{Cone}(h)$ is contractible, and X_n is relatively projective for all n. Then there exists a chain map $f : X \to Y$ unique up to homotopy such that $g \sim hf$.*

PROOF. This boils down to a special case of Proposition 2.2.2. □

Given G-modules M and N, recall that the tensor product $M \otimes N$ is defined to be the tensor product of underlying abelian groups equipped with the diagonal G-action $g(m \otimes n) := (gm) \otimes (gn)$. More generally, given chain complexes X and Y of G-modules, the tensor product $X \otimes Y$ is defined to be the chain complex of G-modules given by the rules

$$(X \otimes Y)_n := \bigoplus_{p+q=n} X_p \otimes Y_q$$

and

$$\partial_{p+q}(X \otimes Y)(x \otimes y) := (\partial_p(X)x) \otimes y + (-1)^p x \otimes (\partial_q(Y)y)$$

for all $x \in X_p$ and $y \in Y_q$.

We say that a chain map $f : X \to Y$ of chain complexes of G-modules is a *resolution* if X and Y are concentrated in nonnegative degree, X_n is relatively projective for all n, and $\mathrm{Res}^G_{\{1\}} \mathrm{Cone}(f)$ is contractible. Abusing language, in a situation where the chain map f is understood, we also say that X is a resolution of Y. Proposition 2.3.2 specifies the sense in which resolutions are unique. Now by one's favorite method one can construct a resolution P of $\mathrm{Inf}^G_{\{1\}} \mathbb{Z}$ such that P_n is projective for all n; then, for any chain complex X of G-modules concentrated in nonnegative degree, the tensor product complex $X \otimes P$ is a resolution of X. In particular, every G-module M (viewed in this context as a chain complex of G-modules concentrated in degree 0) has a resolution. Now if G is a group of cohomological dimension r, then there exists a resolution P of $\mathrm{Inf}^G_{\{1\}} \mathbb{Z}$ such that P_n is projective for all n and $P_n = 0$ for $n > r$, and hence every G-module M has a resolution $M \otimes P$ concentrated in degree $\leq r$.

PROPOSITION 2.3.3. *Let G be a group of finite cohomological dimension. Let P be a chain complex of G-modules such that P_n is relatively projective for all n and $\mathrm{Res}^G_{\{1\}} P$ is contractible. Then P is contractible.*

PROOF. The complex P^+ obtained by replacing P_n by 0 for all $n < 0$ is a resolution of $\operatorname{coker} \partial_0(P) = \ker \partial_{-1}(P)$, and hence has the homotopy type of a complex concentrated in degree $\leq r$, where r is the cohomological dimension of G. It follows that $\ker \partial_n(P) = \operatorname{coker} \partial_{n+1}(P)$ is a direct summand of P_n for all $n > r$. An evident modification of the preceding argument proves that $\ker \partial_n(P) = \operatorname{coker} \partial_{n+1}(P)$ is a direct summand of P_n for all n. □

PROPOSITION 2.3.4. *Let G be a group. Let $g : X \to Z$ and $h : Y \to Z$ be chain maps of chain complexes of G-modules. Make the following assumptions:*

1. *G is of finite virtual cohomological dimension.*
2. *h_n is an isomorphism for all $n \gg 0$.*
3. *X_n, Y_n, and Z_n are relatively projective for all n, and $\operatorname{Res}^G_{\{1\}} X$ is contractible.*

Then there exists a chain map $f : X \to Y$ unique up to homotopy such that $g \sim hf$.

PROOF. By hypothesis 1 and Proposition 2.3.3, there exists a subgroup $H \subseteq G$ of finite index such that the chain complex $\operatorname{Res}^G_H X$ is contractible. By hypothesis 2 and Proposition 2.2.1 there exists a chain map $e : \operatorname{Cone}(h) \to \operatorname{Cone}(h)$ such that $e \sim 1$ and $e_n = 0$ for all $n \gg 0$. By hypothesis 3 and Proposition 2.3.1, one has $H^*(\operatorname{Hom}_G(X, Y_n)) = 0$ and $H^*(\operatorname{Hom}_G(X, Z_n)) = 0$ for all n. The result now follows by Proposition 2.2.2. □

We say that a chain map $\kappa : X \to P$ of chain complexes of G-modules is a *completion* if X_n and P_n are relatively projective for all n, $\operatorname{Res}^G_{\{1\}} X$ is contractible, and κ_n is an isomorphism for all $n \gg 0$. Proposition 2.3.4 specifies the sense in which completions are unique. Abusing language, in a situation where the chain map κ is understood, we also call X a completion of P. For any group G of finite virtual cohomological dimension r, Farrell [**6**] (see also Brown [**1**, Chap. X]) showed how to construct a resolution P of $\operatorname{Inf}^G_{\{1\}} \mathbb{Z}$ with P_n projective for all n, and a completion $F \xrightarrow{\kappa} P$ with F_n projective for all n and κ_n an isomorphism for all $n \geq r$; given a G-module M, the tensor product $M \otimes P$ is then a resolution of M, and the tensor product $M \otimes F$ a completion of $M \otimes P$.

Given a group G of finite virtual cohomological dimension and a G-module M, one defines

$$\hat{H}_*(G, M) := H_*(\operatorname{Coinv}^G_G X)$$

where X is any completion of a resolution of M, and Coinv^G_G is the functor left adjoint to the functor $\operatorname{Inf}^G_{\{1\}}$ equipping abelian groups with trivial G-action. We also introduce the abbreviated notation

$$\hat{H}_*(G) := \hat{H}_*(G, \operatorname{Inf}^G_{\{1\}} \mathbb{Z}).$$

The *Farrell-Tate homology theory* $\hat{H}_*$ extends to groups of finite virtual cohomological dimension the theory introduced by Tate for finite groups.

2.4. The Shapiro lemma and related results. Let G be a group of finite virtual cohomological dimension, and let H be a subgroup (necessarily also of finite virtual cohomological dimension). Let N be an H-module and let Y be a completion of a resolution of N. Then $\operatorname{Ind}^G_H Y$ is a completion of a resolution of $\operatorname{Ind}^G_H N$.

Further, the functors $\mathrm{Res}_H^G \circ \mathrm{Inf}_{\{1\}}^G$ and $\mathrm{Inf}_{\{1\}}^H$ are isomorphic, and hence so are their left adjoints $\mathrm{Coinv}_G^G \circ \mathrm{Ind}_H^G$ and Coinv_H^H. One thus obtains canonical isomorphisms

$$\begin{aligned}\hat{H}_*(G, \mathrm{Ind}_H^G N) &= H_*(\mathrm{Coinv}_G^G \mathrm{Ind}_H^G Y)) \\ &= H_*(\mathrm{Coinv}_H^H Y) \\ &= \hat{H}_*(H, N)\end{aligned}$$

of graded abelian groups. The assertion that there exists an isomorphism between the extreme terms in the relation above, functorial in H-modules N, is the *Shapiro lemma* for Farrell-Tate homology.

With G and H as in the preceding paragraph, let M be a G-module and let X be a completion of a resolution of M. Then $\mathrm{Res}_H^G X$ is a completion of a resolution of $\mathrm{Res}_H^G M$. Suppose now that H is a normal subgroup of G and put $Q := G/H$. Let Inf_Q^G be the inflation functor that equips each Q-module with a G-action via the quotient map $G \to Q$, and let Coinv_H^G be the functor left adjoint to Inf_Q^G. Now the functors $\mathrm{Coinv}_H^H \circ \mathrm{Res}_H^G$ and $\mathrm{Res}_{\{1\}}^Q \circ \mathrm{Coinv}_H^G$ are isomorphic. Moreover, the functor $\mathrm{Res}_{\{1\}}^Q$ is exact. One thus obtains canonical isomorphisms

$$\begin{aligned}\hat{H}_*(H, \mathrm{Res}_H^G M) &= H_*(\mathrm{Coinv}_H^H \mathrm{Res}_H^G X) \\ &= H_*(\mathrm{Res}_{\{1\}}^Q \mathrm{Coinv}_H^G X) \\ &= \mathrm{Res}_{\{1\}}^Q H_*(\mathrm{Coinv}_H^G X)\end{aligned}$$

of graded abelian groups. Thus $\hat{H}_*(H, \mathrm{Res}_H^G M)$ is canonically equipped with graded Q-module structure; in the sequel we identify $\hat{H}_*(H, \mathrm{Res}_H^G M)$ with $H_*(\mathrm{Coinv}_H^G X)$ rather than $H_*(\mathrm{Coinv}_H^H \mathrm{Res}_H^G X)$.

PROPOSITION 2.4.1. *Let Γ be a group of finite virtual cohomological dimension. Let G be a normal subgroup of Γ. Let Π be any subgroup of Γ. Put*

$$H := G \cap \Pi, \quad \bar{\Gamma} := \Gamma/G, \quad \bar{\Pi} := \Pi/H.$$

Let M be a Π-module. Then there exists an isomorphism

$$\hat{H}_*(G, \mathrm{Res}_G^\Gamma \mathrm{Ind}_\Pi^\Gamma M) = \mathrm{Ind}_{\bar{\Pi}}^{\bar{\Gamma}} \hat{H}_*(H, \mathrm{Res}_H^\Pi M)$$

of $\bar{\Gamma}$-modules functorial in M.

PROOF. Clearly the functors $\mathrm{Res}_\Pi^\Gamma \circ \mathrm{Inf}_{\bar{\Gamma}}^\Gamma$ and $\mathrm{Inf}_{\bar{\Pi}}^\Pi \circ \mathrm{Res}_{\bar{\Pi}}^{\bar{\Gamma}}$ are isomorphic, and hence so are their left adjoints $\mathrm{Coinv}_G^\Gamma \circ \mathrm{Ind}_\Pi^\Gamma$ and $\mathrm{Ind}_{\bar{\Pi}}^{\bar{\Gamma}} \circ \mathrm{Coinv}_H^\Pi$. Moreover, the functor $\mathrm{Ind}_{\bar{\Pi}}^{\bar{\Gamma}}$ is exact. Let X be a completion of a resolution of M. One has canonical isomorphisms

$$\begin{aligned}\hat{H}_*(G, \mathrm{Res}_G^\Gamma \mathrm{Ind}_\Pi^\Gamma M) &= H_*(\mathrm{Coinv}_G^\Gamma \mathrm{Ind}_\Pi^\Gamma X) \\ &= H_*(\mathrm{Ind}_{\bar{\Pi}}^{\bar{\Gamma}} \mathrm{Coinv}_H^\Pi X) \\ &= \mathrm{Ind}_{\bar{\Pi}}^{\bar{\Gamma}} H_*(\mathrm{Coinv}_H^\Pi X) \\ &= \mathrm{Ind}_{\bar{\Pi}}^{\bar{\Gamma}} \hat{H}_*(H, \mathrm{Res}_H^\Pi M)\end{aligned}$$

of graded $\bar{\Gamma}$-modules. $\square$

PROPOSITION 2.4.2. *Let G be a group of finite virtual cohomological dimension and let $H \subseteq G$ be a normal subgroup. Let σ be an element of the center of G. Let M be a G-module on which σ acts trivially. Let X be a completion of a resolution of M.*

Then the automorphism of X induced by σ is homotopic to the identity, and hence $\sigma H \in G/H$ induces the identity mapping in $\hat{H}_*(H, \operatorname{Res}_H^G M) = H_*(\operatorname{Coinv}_H^G X)$.

PROOF. This is a consequence of the uniqueness of completions of resolutions (Proposition 2.3.2 and Proposition 2.3.4). □

2.5. The double complex $\mathcal{KT}$. We give a construction exploited repeatedly in the paper. The input for the construction is as follows:

- A commutative ring R with unit.
- An R-module M.
- A linearly ordered set S.
- A family $\{f_s \in R\}_{s \in S}$.
- Elements $f^\pm$ of R such that $f^+ f^- = 0$.

The output of the construction is as follows:

- A double complex $\mathcal{KT}$ of R-modules, i. e., a bigraded R-module
$$\mathcal{KT} = \mathcal{KT}\left(M/R, \{f_s\}_{s\in S}, \left[\begin{array}{c} f^+ \\ f^- \end{array}\right]\right) = \bigoplus_m \bigoplus_n \mathcal{KT}_{mn}$$
equipped with R-linear maps
$$\partial, \delta : \mathcal{KT} \to \mathcal{KT}$$
of bidegree $(-1, 0)$ and $(0, -1)$, respectively, such that $\partial^2 = 0$, $\delta^2 = 0$, and $\partial\delta + \delta\partial = 0$.
- Chain complexes of R-modules
$$\begin{array}{rcl}
\mathcal{K} & = & \mathcal{K}\left(M/R, \{f_s\}_{s\in S}\right), \\
\overline{\mathcal{K}} & = & \overline{\mathcal{K}}\left(M/R, \{f_s\}_{s\in S}, \left[\begin{array}{c} f^+ \\ f^- \end{array}\right]\right), \\
\mathcal{T} & = & \mathcal{T}\left(M/R, \left[\begin{array}{c} f^+ \\ f^- \end{array}\right]\right), \\
\overline{\mathcal{T}} & = & \overline{\mathcal{T}}\left(M/R, \{f_s\}_{s\in S}, \left[\begin{array}{c} f^+ \\ f^- \end{array}\right]\right), \\
\mathcal{KT}^{\mathrm{tot}} & = & \mathcal{KT}^{\mathrm{tot}}\left(M/R, \{f_s\}_{s\in S}, \left[\begin{array}{c} f^+ \\ f^- \end{array}\right]\right), \\
\mathcal{KT}^{+} & = & \mathcal{KT}^{+}\left(M/R, \{f_s\}_{s\in S}, \left[\begin{array}{c} f^+ \\ f^- \end{array}\right]\right),
\end{array}$$
which we call the *companions* of the double complex $\mathcal{KT}$.

The notation $\mathcal{KT}$ is meant to call Koszul and Tate to mind.

Here is the construction. We define $\mathcal{S}$ to be the free abelian group on symbols of the form $[I, k]$ where $I \subseteq S$ is a finite subset and k is an integer, and we bigrade $\mathcal{S}$ by declaring the symbol $[I, k]$ to be of bidegree $(|I|, k)$. Put
$$\begin{array}{rcl}
\mathcal{KT} & := & M \otimes \mathcal{S} \\
\partial(m \otimes [I, k]) & := & \sum_{i \in I} (-1)^{|\{j \in I | j < i\}|} f_i m \otimes [I \setminus \{i\}, k] \\
\delta(m \otimes [I, k]) & := & (-1)^{|I|} \left\{ \begin{array}{ll} f^+ m \otimes [I, k-1] & \text{if } k \text{ is even} \\ f^- m \otimes [I, k-1] & \text{if } k \text{ is odd} \end{array} \right.
\end{array}$$
for all $m \in M$, finite subsets $I \subseteq S$ and integers k. Take $\mathcal{K}_n := \mathcal{KT}_{n0}$ and equip $\mathcal{K}$ with the differential induced by the operator ∂. Take $\mathcal{T}_n := \mathcal{KT}_{0n}$ and equip $\mathcal{T}$

with the differential induced by the operator δ. Put

$$\overline{\mathcal{K}} := \mathcal{K}\left(\frac{M}{f^- M}/R, \{f_s\}_{s\in S}\right), \quad \overline{\mathcal{T}} := \mathcal{T}\left(\frac{M}{\sum_{s\in S} f_s M}/R, \begin{bmatrix} f^+ \\ f^- \end{bmatrix}\right).$$

Let $\mathcal{KT}^{\text{tot}}$ be the *total complex* associated to the double complex $\mathcal{KT}$, i. e., a copy of $\mathcal{KT}$ graded by total degree and equipped with the differential induced by $\partial + \delta$. Let $\mathcal{KT}^-$ be the subcomplex of $\mathcal{KT}^{\text{tot}}$ spanned over R by elements of the form $m \otimes [I, k]$ with $m \in M$, $I \subseteq S$ finite, and $k < 0$. Finally, put $\mathcal{KT}^+ := \mathcal{KT}^{\text{tot}}/\mathcal{KT}^-$. Note that $\overline{\mathcal{T}}$ is naturally a quotient of $\mathcal{KT}^{\text{tot}}$ and $\overline{\mathcal{K}}$ naturally a quotient of $\mathcal{KT}^+$.

PROPOSITION 2.5.1. *Let R be a commutative ring with unit, M an R-module, $\{f_s\}_{s\in S}$ a family of elements of R indexed by a linearly ordered set S, $f^\pm$ elements of R such that $f^+ f^- = 0$. Consider the double complex*

$$\mathcal{KT}\left(M/R, \{f_s\}_{s\in S}, \begin{bmatrix} f^+ \\ f^- \end{bmatrix}\right)$$

and companion complexes $\mathcal{K}$, $\overline{\mathcal{K}}$, $\mathcal{T}$, $\overline{\mathcal{T}}$, $\mathcal{KT}^{\text{tot}}$ and $\mathcal{KT}^+$.

1. *If, for all finite subsets $I \subseteq S$, the sequence $\{f_i\}_{i\in I}$ is M-regular, then $\mathcal{K}$ is acyclic in positive degree.*
2. *If, for some $s \in S$, the element f_s operates invertibly on M, then $\mathcal{K}$ is acyclic.*
3. *If $\mathcal{K}$ is acyclic in positive degree, then the quotient map $\mathcal{KT}^{\text{tot}} \to \overline{\mathcal{T}}$ induces an isomorphism in homology.*
4. *If $\mathcal{T}$ is acyclic, then $\mathcal{KT}^{\text{tot}}$ is acyclic and the quotient map $\mathcal{KT}^+ \to \overline{\mathcal{K}}$ induces an isomorphism in homology.*

PROOF. Because homology commutes with direct limits, we may assume that S is a finite set. Then assertions 1 and 2 are standard facts about Koszul complexes; assertions 3 and 4 are proved by straightforward spectral sequence arguments. □

2.6. Almost free abelian groups. Finitely generated abelian groups are of finite virtual cohomological dimension and hence the Farrell-Tate theory applies to them. For each homomorphis $\phi : H \to G$ of groups, ϕ^* denotes the functor equipping each G-module with an H-action via ϕ.

PROPOSITION 2.6.1. *Let Γ be a finitely generated abelian group and let $G \subset \Gamma$ be a subgroup. Let $\Delta \subseteq G \times G$ be the diagonal subgroup. Let $p : \Gamma \times G \to \Gamma$ and $q : \Gamma \times G \to G$ be the first and second projections, respectively. Let $r : \Gamma \xrightarrow{\sim} (\Gamma \times G)/\Delta$ be the isomorphism inverse to that induced by $p - q$. Let F be a completion of a resolution P of $\operatorname{Inf}_{\{1\}}^G \mathbb{Z}$ such that F_n and P_n are projective for all n. Let M be a Γ-module. Put*

$$M' := r^* \operatorname{Coinv}_\Delta^{\Gamma\times G}(p^* M \otimes q^* F).$$

Then there exists an isomorphism

$$H_*(M') = \operatorname{Inf}_{\Gamma/G}^\Gamma \hat{H}_*(G, \operatorname{Res}_G^\Gamma M)$$

of graded Γ-modules functorial in M.

PROOF. Without loss of generality we may assume that $F = \operatorname{Res}_G^\Gamma \tilde{F}$, where $\tilde{F}$ is a completion of a resolution $\tilde{P}$ of $\operatorname{Inf}_{\{1\}}^\Gamma \mathbb{Z}$ such that $\tilde{P}_n$ and $\tilde{F}_n$ are projective for all n. Let

$$\left.\begin{array}{l} i := (\gamma \mapsto (\gamma, 1)) \\ d := (\gamma \mapsto (\gamma, \gamma)) \end{array}\right\} : \Gamma \to \Gamma \times \Gamma$$

and let $\tilde{q} : \Gamma \times \Gamma \to \Gamma$ be the second projection. Consider the complex

$$\tilde{M} := \mathrm{Inf}^{\Gamma\times\Gamma}_{(\Gamma\times\Gamma)/\Delta} \mathrm{Coinv}^{\Gamma\times\Gamma}_{\Delta}(p^* M \otimes \tilde{q}^* \tilde{F})$$

of $\Gamma \times \Gamma$-modules. Now $d^*(p^* M \otimes \tilde{q}^* \tilde{F}) = M \otimes \tilde{F}$ is a completion of a resolution of M and one has an isomorphism

$$d^* \mathrm{Inf}^{\Gamma\times\Gamma}_{(\Gamma\times\Gamma)/\Delta} \mathrm{Coinv}^{\Gamma\times\Gamma}_{\Delta} = \mathrm{Inf}^{\Gamma}_{\Gamma/G} \mathrm{Coinv}^{\Gamma}_{G} d^*$$

of functors; accordingly, we have an isomorphism

$$H_*(d^*\tilde{M}) = \mathrm{Inf}^{\Gamma}_{\Gamma/G} \hat{H}_*(G, \mathrm{Res}^{\Gamma}_{G} M)$$

of graded Γ-modules functorial in M. One has an isomorphism of functors

$$i^* \mathrm{Inf}^{\Gamma\times\Gamma}_{(\Gamma\times\Gamma)/\Delta} \mathrm{Coinv}^{\Gamma\times\Gamma}_{\Delta} = r^* \mathrm{Coinv}^{\Gamma\times G}_{\Delta} \mathrm{Res}^{\Gamma\times\Gamma}_{\Gamma\times G}$$

and thus we have an isomorphism

$$H_*(i^*\tilde{M}) = H_*(M')$$

of graded Γ-modules functorial in M. Finally, for all $\gamma \in \Gamma$, the action of γ on $\tilde{F}$ is homotopy trivial by Proposition 2.4.2, hence the elements $i(\gamma)$ and $d(\gamma)$ of $\Gamma \times \Gamma$ induce homotopic automorphisms of the complex $\tilde{M}$, and hence we have a canonical isomorphism

$$H_*(d^*\tilde{M}) = H_*(i^*\tilde{M})$$

of graded Γ-modules functorial in M. □

We say that an abelian group is *almost free* if the group can be factored as the product of a free abelian group and a finite cyclic group. The multiplicative group of a global field is almost free. Every subgroup of an almost free abelian group is again almost free.

PROPOSITION 2.6.2. *Let Γ be a finitely generated abelian group. Let $G \subseteq \Gamma$ be an almost free subgroup of rank r, and let m be the order of the torsion subgroup of G. Let $g_1, \ldots, g_r \in G$ be independent, and let $g_0 \in G$ generate the torsion subgroup of G. Let M be a Γ-module. Consider the chain complex*

$$M' := \mathcal{KT}^{\mathrm{tot}}\left(M/\mathbb{Z}[\Gamma], \{1-g_i\}_{i=1}^r, \begin{bmatrix} \sum_{i=0}^{m-1} g_0^i \\ 1-g_0 \end{bmatrix}\right).$$

of Γ-modules. Then there exists an isomorphism

$$H_*(M') = \mathrm{Inf}^{\Gamma}_{\Gamma/G} \hat{H}_*(G, \mathrm{Res}^{\Gamma}_{G} M)$$

of graded Γ-modules functorial in M.

PROOF. Consider the double complex

$$\mathcal{KT}\left(\mathbb{Z}[G]/\mathbb{Z}[G], \{1-g_i^{-1}\}_{i=1}^r, \begin{bmatrix} \sum_{i=0}^{m-1} g_0^{-i} \\ 1-g_0^{-1} \end{bmatrix}\right)$$

and its companions $P := \mathcal{KT}^+$ and $F := \mathcal{KT}^{\mathrm{tot}}$. Then P_n and F_n are projective for all n and moreover $F_n = P_n$ for all $n \geq r$; by Proposition 2.5.1, P is a resolution of $\mathrm{Inf}^{G}_{\{1\}} \mathbb{Z}$ and F a completion of P. The result now becomes a special case of Proposition 2.6.1. □

PROPOSITION 2.6.3. *Let G be an almost free abelian group of positive finite rank r and let m be the order of the torsion subgroup of G. Then $\hat{H}_n(G)$ is a free $(\mathbb{Z}/m\mathbb{Z})$-module of rank 2^{r-1} for all n.*

PROOF. By Proposition 2.6.2 we have an isomorphism

$$\hat{H}_n(G) \tilde{\to} H_n\left(\mathcal{KT}^{\mathrm{tot}}\left(\mathbb{Z}/\mathbb{Z}, \{0\}_{i=1}^r, \left[\begin{array}{c} m \\ 0 \end{array}\right]\right)\right),$$

whence the result after a brief computation with binomial coefficients. □

The following technical result is the key to our proof of Yin's conjecture.

PROPOSITION 2.6.4. *Let Γ be an abelian group (not necessarily finitely generated) and let $\Pi \subseteq \Gamma$ be a subgroup of finite index. Let $G \subseteq \Gamma$ be an almost free subgroup of finite rank r, let $\Pi G \subseteq \Gamma$ be the subgroup generated by Π and G, and let m be the order of the torsion subgroup of G. Let $g_1, \dots, g_r \in G$ be independent and let $g_0 \in G$ generate the torsion subgroup. Consider the chain complex*

$$K := \mathcal{KT}^{\mathrm{tot}}\left(\mathrm{Ind}_\Pi^\Gamma \mathrm{Inf}_{\{1\}}^\Pi \mathbb{Z}/\mathbb{Z}[\Gamma], \{1 - g_i\}_{i=1}^r, \left[\begin{array}{c} \sum_{i=0}^{m-1} g_0^i \\ 1 - g_0 \end{array}\right]\right)$$

of Γ-modules. Then one has an isomorphism

$$H_*(K) \tilde{\to} \mathrm{Ind}_{\Pi G}^\Gamma \mathrm{Inf}_{\{1\}}^{\Pi G} \hat{H}_*(\Pi \cap G)$$

of graded Γ-modules.

PROOF. Let $\Gamma' \subseteq \Gamma$ be a finitely generated subgroup such that $G \subseteq \Gamma'$ and $\Gamma'\Pi = \Gamma$. Replacing Γ with Γ', we may assume that Γ is finitely generated. We have at our disposal a canonical isomorphism

$$H_*(K) = \mathrm{Inf}_{\Gamma/G}^\Gamma \hat{H}_*(G, \mathrm{Res}_G^\Gamma \mathrm{Ind}_\Pi^\Gamma \mathrm{Inf}_{\{1\}}^\Pi \mathbb{Z})$$

provided by Proposition 2.6.2, a canonical isomorphism

$$\hat{H}_*(G, \mathrm{Res}_G^\Gamma \mathrm{Ind}_\Pi^\Gamma \mathrm{Inf}_{\{1\}}^\Pi \mathbb{Z}) = \mathrm{Ind}_{\Pi/(\Pi\cap G)}^{\Gamma/G} \hat{H}_*(\Pi \cap G, \mathrm{Res}_{\Pi\cap G}^\Pi \mathrm{Inf}_{\{1\}}^\Pi \mathbb{Z})$$

provided by Proposition 2.4.1, a canonical isomorphism

$$\hat{H}_*(\Pi \cap G, \mathrm{Res}_{\Pi\cap G}^\Pi \mathrm{Inf}_{\{1\}}^\Pi \mathbb{Z}) = \mathrm{Inf}_{\{1\}}^{\Pi/(\Pi\cap G)} \hat{H}_*(\Pi \cap G)$$

provided by Proposition 2.4.2, and an isomorphism

$$\mathrm{Inf}_{\Gamma/G}^\Gamma \mathrm{Ind}_{\Pi/(\Pi\cap G)}^{\Gamma/G} \mathrm{Inf}_{\{1\}}^{\Pi/(\Pi\cap G)} = \mathrm{Ind}_{\Pi G}^\Gamma \mathrm{Inf}_{\{1\}}^{\Pi G}$$

of functors, whence the result. □

3. The principal objects of study

3.1. The basic data $(\mathbb{K}, A, \mathrm{sgn})$**.** For the rest of the paper we fix the following items.

- A locally compact nondiscrete topological field $\mathbb{K}$ containing only finitely many roots of unity.
- A discrete cocompact integrally closed subring $A \subset \mathbb{K}$.
- A continuous homomorphism

$$\mathrm{sgn} : \mathbb{K}^\times \to (\text{the group of roots of unity in } \mathbb{K})$$

  the restriction of which to the group of roots of unity of $\mathbb{K}$ is the identity mapping.

We call sgn the *sign homomorphism*, and we say that $x \in \mathbb{K}^\times$ is *positive* if $\operatorname{sgn} x = 1$. We say that the basic data are *archimedean* aif $\mathbb{K}$ is archimedean. We denote the fraction field of A by k.

There is only one archimedean example $(\mathbb{K}, A, \operatorname{sgn})$ of basic data, namely the triple $(\mathbb{R}, \mathbb{Z}, x \mapsto x/|x|)$. In the archimedean case our usage of the term "positive" is just the ordinary usage.

The simplest example $(\mathbb{K}, A, \operatorname{sgn})$ of nonarchimedean basic data arises as follows. Let $\mathbb{F}_q$ be the field of q elements and let $\mathbb{F}_q(T)$ be the field of rational functions in a variable T with coefficients in $\mathbb{F}_q$. Take $\mathbb{K}$ to be the completion $\mathbb{F}_q((1/T))$ of $\mathbb{F}_q(T)$ at the infinite place. Take A to be the polynomial ring $\mathbb{F}_q[T]$. Decompose $\mathbb{F}_q((1/T))^\times$ as a direct product

$$\mathbb{F}_q^\times \cdot T^{\mathbb{Z}} \cdot (1 + (1/T)\mathbb{F}_q[[1/T]])$$

and take the sign homomorphism sgn to be projection to the first factor. In this example the positive elements of $\mathbb{F}_q[T]$ are the monic polynomials.

Every nonarchimedean example $(\mathbb{K}, A, \operatorname{sgn})$ of basic data arises in the following manner. Let X/k_0 be a smooth projective geometrically irreducible curve defined over a finite field k_0. Let ∞ be a closed point of X. Take $\mathbb{K}$ to be the completion of the function field of X at ∞. Take A to be the ring consisting of elements of the function field of X regular away from ∞. Choose an isomorphism of topological fields under which to identify $\mathbb{K}$ with $\mathbb{F}_q((1/T))$, where q is the cardinality of the residue field of ∞, and define the sign homomorphism as in the preceding example.

For archimedean and nonarchimedean basic data $(\mathbb{K}, A, \operatorname{sgn})$ alike, the ring A is a Dedekind domain the group of units of which is finite, the class group of which is finite, and every residue field of which is finite.

3.2. A-lattices. A *fractional A-ideal* is a finitely generated nonzero A-submodule of k. An *integral A-ideal* is a fractional A-ideal contained in A. When we speak of fractional or integral A-ideals we tacitly exclude the zero ideal of A from consideration. We say that a fractional A-ideal I is *principal* in the if $I = (a)$ for some $a \in k^\times$; we say that I is principal in the *narrow* sense if $I = (a)$ for some positive $a \in k^\times$. The quotient of the group of fractional A-ideals by the subgroup of ideals principal in the narrow sense is by definition the *narrow ideal class group.* The narrow ideal class group is finite.

An *A-lattice* is by definition a cocompact discrete A-submodule of $\mathbb{K}$. An A-lattice is without A-torsion and contains a copy of A as a subgroup of finite index, and therefore is projective over A of rank one. We say that two A-lattices W_1 and W_2 are *homothetic*, and we write $W_1 \sim W_2$, if there exists some positive $x \in \mathbb{K}$ such that $xW_1 = W_2$. The relation of homothety is an equivalence relation in the set of A-lattices.

Every fractional A-ideal is an A-lattice. Fractional A-ideals belong to the same narrow ideal class if and only if they are homothetic. Every homothety class of A-lattices contains a fractional A-ideal. The set of homothety classes of A-lattices thus corresponds bijectively with the narrow ideal class group and in particular is finite.

3.3. The set Ξ. Given $x \in \mathbb{K}$ and an A-lattice W, we say that

$$x + W := \{x + w \in \mathbb{K} \mid w \in W\}$$

is a *translate* of the A-lattice W, and we say that a subset of $\mathbb{K}$ is an *A-lattice translate* if of the form $x + W$. We always write A-lattice translates as a sum, the first symbol denoting an element of $\mathbb{K}$ and the second an A-lattice. We say that two A-lattice translates $x_1 + W_1$ and $x_2 + W_2$ are *homothetic*, and we write $x_1+W_1 \sim x_2+W_2$, if for some positive $y \in \mathbb{K}$ one has $yW_1 = W_2$ and $yx_1-x_2 \in W_2$. Homothety is an equivalence relation in the set of A-lattice translates. Note that for all A-lattices W and $x, y \in \mathbb{K}$, one has $x + W \sim y + W$ if and only if $x - y \in W$. Given an A-lattice translate $x + W$ and an integral A-ideal f, we say that $x + W$ is *annihilated by f*, or that $x + W$ is *f-torsion*, if $xf \subseteq W$; and we say that $x + W$ is of *order f* if $\{a \in A \mid ax \in W\} = f$. We say that an A-lattice translate is *torsion* if f-torsion for some integral A-ideal f.

We denote the homothety class of a torsion A-lattice translate $x+W$ by $[x+W]$. We denote the set of homothety classes of torsion A-lattice translates by Ξ. For each integral A-ideal f, let $\Xi(f)$ be the set of homothety classes of f-torsion A-lattice translates, and let $\Xi^\times(f)$ be the set of homothety classes of A-lattice translates of order f. Given a fractional A-ideal I and an A-lattice W let $I \cdot W$ be the A-submodule of $\mathbb{K}$ generated by all products of the form aw where $a \in I$ and $w \in W$; the A-submodule $I \cdot W$ is again an A-lattice.

PROPOSITION 3.3.1. *Let f be an integral A-ideal. There exists a unique map*

$$Y_f : \Xi \to \Xi$$

such that

$$Y_f[x + W] = [x + f^{-1} \cdot W]$$

for all torsion A-lattice translates $x+W$. Every fiber of the map Y_f is of cardinality $|A/f|$. One has

$$\begin{aligned}
Y_f \circ Y_g &= Y_{fg} \\
Y_f\Xi(g) &= \begin{cases} \Xi(g/f) & \text{if } f \text{ divides } g \\ \Xi(g) & \text{if } f \text{ is prime to } g \end{cases} \\
Y_f\Xi^\times(g) &= \begin{cases} \Xi^\times(g/f) & \text{if } f \text{ divides } g \\ \Xi^\times(g) & \text{if } f \text{ is prime to } g \end{cases} \\
Y_f^{-1}\Xi(g) &= \Xi(fg)
\end{aligned}$$

for all integral A-ideals g.

PROOF. The proof is quite straightforward and we omit it. □

3.4. The profinite group G. Given integral A-ideals f, I and J, we write $I \sim_f J$ if I and J are prime to f and there exist nonzero $a, b \in A$ prime to f such that b/a is positive, $a \equiv b \bmod f$ and $aI = bJ$. The relation $\sim_f$ is an equivalence relation in the set of integral A-ideals prime to f. For each integral A-ideal f, the quotient G_f of the monoid of integral A-ideals prime to f by the equivalence relation $\sim_f$ is a finite abelian group. The family of groups $\{G_f\}$ forms an inverse system indexed by the set of integral A-ideals directed by the divisibility relation. Put

$$G := \varprojlim G_f.$$

The transition maps of the inverse system $\{G_f\}$ are surjective and hence each group G_f is canonically a quotient of G.

Given an integral A-ideal f, let $\sqrt{f}$ be the product of the maximal A-ideals dividing f.

PROPOSITION 3.4.1. *For each integral A-ideal f, the natural map*

$$\prod_{p|f} \ker\left(G_f \to G_{f/p}\right) \to \ker\left(G_f \to G_{f/\sqrt{f}}\right)$$

is bijective, where the Cartesian product on the left is extended over the maximal A-ideals p dividing f.

PROOF. There exists a unique isomorphism

$$(A/f)^\times \xrightarrow{\sim} \ker\left(G_f \to G_1\right)$$

under which, for all positive $a \in A$ prime to f, the congruence class of a modulo f maps to the $\sim_f$-equivalence class of (a). This noted, the proposition reduces to the Chinese Remainder Theorem. □

PROPOSITION 3.4.2. *Let f be an integral A-ideal. Let $x + W$ be a torsion A-lattice translate of order f.*

1. *For all integral A-ideals I and J both prime to f, one has $I \sim_f J$ if and only if $x + I^{-1} \cdot W \sim x + J^{-1} \cdot W$.*
2. *For all torsion A-lattice translates $x' + W'$ of order f there exists an integral A-ideal I prime to f such that $x' + W' \sim x + I^{-1} \cdot W$.*

PROOF. 1($\Rightarrow$). By hypothesis there exist nonzero $a, b \in A$ prime to f such that b/a is positive, $a \equiv b \bmod f$ and $aI = bJ$. We have

$$ba^{-1}I^{-1} \cdot W = J^{-1} \cdot W, \quad ba^{-1}x - x \in a^{-1} \cdot W \cap J^{-1}f^{-1} \cdot W \subseteq J^{-1} \cdot W,$$

whence the result.

1($\Leftarrow$). By hypothesis there exists some positive $y \in \mathbb{K}$ such that

$$yI^{-1} \cdot W = J^{-1} \cdot W, \quad yx - x \in J^{-1} \cdot W.$$

Necessarily $yJ = I$, and moreover, because I and J are prime to f, we can write $y = b/a$ where $0 \neq a, b \in A$ are prime to f. We have

$$(b - a)x \in (I^{-1} + J^{-1}) \cdot W \cap f^{-1} \cdot W = W,$$

hence $a \equiv b \bmod f$, and the result follows.

2. Replacing $x' + W'$ by a homothetic torsion A-lattice translate, we may assume that $W' = J^{-1} \cdot W$ for some integral A-ideal J prime to f; replacing W by $J^{-1} \cdot W$, we may assume that $W = W'$. By hypothesis both $x + W$ and $x' + W$ generate the free rank one (A/f)-module $f^{-1} \cdot W/W$, and hence we can find positive $a \in A$ such that $ax \equiv x' \bmod W$. Necessarily a is prime to f. Then $x' + W = ax + W \sim x + a^{-1}W = x + (a^{-1}) \cdot W$. □

PROPOSITION 3.4.3. *There exists a unique (left) action of the group G on Ξ such that for all integral A-ideals f, integral A-ideals I prime to f, and A-lattice translates $x + W$ of order f,*

$$\sigma[x + W] = [x + I^{-1} \cdot W]$$

for all $\sigma \in G$ with image in G_f equal to the $\sim_f$-equivalence class of I. (Hereafter Ξ is considered to be equipped with the action of G so defined.)

PROOF. This follows in a straightforward way from Proposition 3.3.1 and Proposition 3.4.2. □

PROPOSITION 3.4.4. *Let f be an integral A-ideal. The map $Y_f : \Xi \to \Xi$ is G-equivariant. Moreover, for any A-lattice translate $x + W$ of order f, the map $\sigma \mapsto \sigma[x + W] : G \to \Xi^\times(f)$ induces a bijection $G_f \tilde{\to} \Xi^\times(f)$.*

PROOF. This follows in a straightforward way from Proposition 3.3.1 and Proposition 3.4.2. $\square$

REMARK 3.4.5. In class field theory the group G is identified with the Galois group of a certain infinite abelian extension of k. In the archimedean (resp. nonarchimedean) case, this extension can be obtained explicitly by adjoining to k all roots of unity (resp. all torsion points of all sign-normalized rank one elliptic A-modules). The set Ξ turns out to be G-equivariantly isomorphic in the archimedean (resp. nonarchimedean) case to the set of roots of unity (resp. the disjoint union, extended over the set of sign-normalized rank one elliptic A-modules ρ, of the set of torsion points of ρ). For an overview of the theory of sign-normalized rank one elliptic A-modules see Hayes [**9**]. For an overview of related function field arithmetic see Goss [**8**].

3.5. The sign group G_∞. For each integral A-ideal f, let D_f be the subgroup of G_f consisting of the $\sim_f$-equivalence classes of ideals of the form (a) for some $a \in A$ such that $a \equiv 1 \bmod f$. We define

$$G_\infty := \varprojlim D_f \subset G.$$

We call G_∞ the *sign group.*

REMARK 3.5.1. Identifying G with the Galois group of an abelian extension of k via class field theory, the subgroup G_∞ may be interpreted as the decomposition group of the valuation of k inherited from $\mathbb{K}$.

PROPOSITION 3.5.2. *There exists a unique homomorphism*

$$\mathrm{sgn} : G_\infty \to \mathbb{K}^\times$$

mapping G_∞ isomorphically to the group of roots of unity of $\mathbb{K}$ such that

$$\gamma[x + W] = [(\mathrm{sgn}\,\gamma)^{-1}(x + W)] \tag{1}$$

for all $\gamma \in G_\infty$ and torsion A-lattice translates $x + W$.

PROOF. For each integral A-ideal f, let E_f be the subgroup of $A^\times$ consisting of $a \in A^\times$ such that $a \equiv 1 \bmod f$. Then for all but finitely many integral A-ideals f, one has $E_f = \{1\}$. (In fact, if f is not the unit ideal and $E_f \neq \{1\}$, then $(\mathbb{K}, A, \mathrm{sgn}) = (\mathbb{R}, \mathbb{Z}, x \mapsto x/|x|)$ and $f = (2)$.) For all integral A-ideals f there exists a unique homomorphism $\phi_f : D_f \to \mathbb{K}^\times/E_f$ mapping D_f isomorphically to the group of roots of unity of $\mathbb{K}^\times$ modulo E_f under which an element of D_f represented by an ideal of the form (a) for some $a \in A$ such that $a \equiv 1 \bmod f$ maps to the E_f-coset containing $\mathrm{sgn}\, a$. The system $\{\phi_f\}$ is compatible and induces a homomorphism $\phi : G_\infty \to \mathbb{K}^\times$ mapping G_∞ isomorphically to the group of roots of unity of $\mathbb{K}$.

We claim that ϕ has property (1). Fix an integral A-ideal f, a torsion A-lattice translate $x + W$ of order f and an element $\gamma \in G_\infty$. Choose an integral A-ideal I prime to f belonging to the $\sim_f$-equivalence class to which γ gives rise in G_f. Then

$I = (a)$ for some $a \in A$ such that $a \equiv 1 \bmod f$, and

$$\begin{array}{rcl}\gamma[x+W] & = & [x + I^{-1} \cdot W] \\ & = & [(\operatorname{sgn} a)^{-1} a(x + I^{-1} \cdot W)] \\ & = & [(\operatorname{sgn} a)^{-1}(ax + W)] \\ & = & [(\operatorname{sgn} a)^{-1}(x + W)] = [\phi(\gamma)^{-1}(x+W)].\end{array}$$

The claim is proved. Thus we have established the existence of a homomorphism $G_\infty \to \mathbb{K}^\times$ with the desired properties; uniqueness follows by Proposition 3.4.4. $\square$

Fix a generator $\gamma_0 \in G_\infty$ arbitrarily and let m denote the order of G_∞. Given an abelian group M equipped with an action of G_∞ and an integer i, we define the i^{th} *sign-homology module* and the $(1-i)^{th}$ *sign-cohomology module* of M to be

$$H_i\left(\mathcal{T}\left(M/\mathbb{Z}[G_\infty], \left[\begin{array}{c} \sum_{i=0}^{m-1} \gamma_0^i \\ 1 - \gamma_0 \end{array}\right]\right)\right).$$

As explained in §2, the sign-(co)homology of M can be identified with the Tate (co)homology of G_∞ with coefficients in M.

3.6. The module $U^{(\nu)}$. Let R be a commutative ring with unit. Let $\mathcal{A}$ be the free R-module generated by Ξ, and let the action of G on Ξ be extended to $\mathcal{A}$ in R-linear fashion. Fix a family

$$\nu = \{\nu_f\}$$

of elements of R indexed by the integral A-ideals such that

$$\nu_1 = 1$$

and

$$\nu_{fg} = \nu_f \nu_g$$

for all integral A-ideals f and g. We are primarily interested in the case $R = \mathbb{Z}$ and $\nu = 1$, but we work at the higher level of generality because (i) it offers no additional difficulties and (ii) we anticipate applicability of the theory to the study of K-theoretic index questions.

The R-module $U^{(\nu)}$ is defined to be the quotient of $\mathcal{A}$ by the R-submodule generated by the family of elements of the form

$$\nu_p \xi - \sum_{\eta \in Y_p^{-1}(\xi)} \eta$$

where p is a maximal A-ideal, $\xi \in \Xi$, and the sum is extended over those $\eta \in \Xi$ such that $Y_p \eta = \xi$. By Proposition 3.4.4, $\ker\left(\mathcal{A} \to U^{(\nu)}\right)$ is G-stable, and hence the action of G on $\mathcal{A}$ descends to $U^{(\nu)}$. The multiplicativity of the system $\{\nu_f\}$, along with Proposition 3.4.4, implies that $\ker\left(\mathcal{A} \to U^{(\nu)}\right)$ contains every element of the form

$$\nu_f \xi - \sum_{\eta \in Y_p^{-1}(\xi)} \eta$$

where f is an integral A-ideal, $\xi \in \Xi$, and the sum is extended over those $\eta \in \Xi$ such that $Y_f \eta = \xi$.

Let f be an integral A-ideal. We define $\mathcal{A}(f)$ to be the R-submodule of $\mathcal{A}$ generated by $\Xi(f)$. The R-module $\mathcal{A}(f)$ is finitely generated and free, and clearly

$$\mathcal{A} = \bigcup_f \mathcal{A}(f).$$

By Proposition 3.4.4, the R-module $\mathcal{A}(f)$ is a G-stable R-submodule of $\mathcal{A}$, and moreover the action of G on $\mathcal{A}(f)$ factors through an action of G_f. We define $U^{(\nu)}(f)$ to be the quotient of $\mathcal{A}(f)$ by the R-submodule generated by all elements of the form

$$\nu_p\xi - \sum_{\eta\in Y_p^{-1}(\xi)} \eta$$

where p is an maximal A-ideal dividing f and $\xi \in \Xi(f/p)$. By Proposition 3.4.4, $\ker\left(\mathcal{A}(f) \to U^{(\nu)}(f)\right)$ is G-stable, and hence the action of G descends to $U^{(\nu)}(f)$. Note that the action of G on $U^{(\nu)}(f)$ factors through an action of G_f. Clearly

$$U^{(\nu)} = \varinjlim U^{(\nu)}(f).$$

The multiplicativity of the system $\{\nu_f\}$ implies that $\ker\left(\mathcal{A}(f) \to U^{(\nu)}(f)\right)$ contains all elements of the form

$$\nu_g\xi - \sum_{\eta\in Y_p^{-1}(\xi)} \eta$$

where g is any integral A-ideal dividing f and $\xi \in \Xi(f/g)$.

4. The structure of $U^{(\nu)}$ and its sign-homology

4.1. A partition of Ξ.

LEMMA 4.1.1. *Let f be an integral A-ideal. Let p be a maximal A-ideal dividing f. Write $f = cp^n$ where n is a positive integer and c is an integral A-ideal prime to f. Let $\phi \in G$ be an element projecting to the $\sim_c$-equivalence class of p in G_c. Let S be a set of elements of G mapping bijectively to* $\ker\left(G_f \to G_{f/p}\right)$ *under projection to G_f. Then*

$$(2)\qquad \sum_{\eta\in Y_p^{-1}(Y_p(\xi))} \eta = \left(\sum_{\sigma\in S}\sigma\xi\right) + \begin{cases} \phi^{-1}Y_p(\xi) & \textit{if } n=1 \\ 0 & \textit{if } n>1 \end{cases}$$

for each $\xi \in \Xi^\times(f)$.

PROOF. Let $x + W$ be an A-lattice translate of order f such that $\xi = [x + W]$. Let T be a set of positive elements of A prime to f mapping bijectively to $\ker\left((A/f)^\times \to (A/(f/p))^\times\right)$ under reduction modulo f. Let b be a positive element of A such that $b \equiv 0 \bmod p$ and $b \equiv 1 \bmod c$. Then the sum

$$(3)\qquad \left(\sum_{a\in T}[ax+W]\right) + \begin{cases} [bx+W] & \text{if } n=1 \\ 0 & \text{if } n>1 \end{cases}$$

equals the left side of (2). Put $J := p^{-1}(b)$. Then J is an integral A-ideal prime to c such that Jp is $\sim_c$-equivalent to the unit ideal, $\{(a) \mid a \in T\}$ is a set of integral A-ideals prime to f mapping bijectively to $\ker\left(G_f \to G_{f/p}\right)$, and

$$(4)\qquad \left(\sum_{a\in T}[x+(a)^{-1}\cdot W]\right) + \begin{cases} [x+J^{-1}p^{-1}\cdot W] & \text{if } n=1 \\ 0 & \text{if } n>1 \end{cases}$$

equals the right side of (2). But for each $a \in T$ one has

$$ax + W \sim x + a^{-1}W = x + (a)^{-1}\cdot W.$$

Further, in the case $n = 1$ one has

$$bx + w \sim x + b^{-1}W = x + J^{-1}p^{-1} \cdot W.$$

Thus the sums (3) and (4) are equal term by term. □

LEMMA 4.1.2. *There exists a partition*

$$\Xi = \coprod_{k=0}^{\infty} \Xi_k$$

with the following properties:

1. *For all integers $k > 0$, integral A-ideals f, and $\xi \in \Xi_k \cap \Xi^\times(f)$, there exists a maximal A-ideal p dividing f such that $Y_p^{-1}(Y_p(\xi)) \setminus \{\xi\} \subseteq \Xi_{k-1} \cup \Xi(f/p)$.*
2. *For all integral A-ideals f such that the map $G_\infty \to G_{f/\sqrt{f}}$ is injective, the group G_∞ stabilizes and acts freely upon the set $\Xi_0 \cap \Xi^\times(f)$.*
3. *For each integral A-ideal f, one has $|\Xi_0 \cap \Xi(f)| = |G_f|$.*

(Hereafter we will assume such a partition of Ξ to be fixed.)

PROOF. For each integral A-ideal f, we select a subset $S(f) \subseteq G$ with the following properties:

- $1 \in S(f)$.
- The natural map $S_f \to G_f$ is bijective.
- If the natural map $G_\infty \to G_f$ is injective, then the set $S(f)$ is a union of cosets of G_∞ in G.

By Proposition 3.4.1 and Proposition 3.4.4 it follows that for each integral A-ideal f and $\xi \in \Xi^\times(f)$, there exist unique

$$\sigma \in S(f/\sqrt{f})$$

and, for each maximal A-ideal p dividing f, unique

$$\tau_p \in S(f) \cap \ker\left(G \to G_{f/p}\right)$$

such that

$$\xi = \sigma \left(\prod_p \tau_p \right) [1 + f];$$

in this situation we declare $\xi \in \Xi_k$, where k is the number of maximal A-ideals p dividing f such that $\tau_p = 1$. Property 1 of the partition may be verified with the help of Lemma 4.1.1; property 2 of the partition follows by Proposition 3.4.4. For each integral A-ideal f, one has

$$|\Xi_0 \cap \Xi^\times(f)| = \left|G_{f/\sqrt{f}}\right| \cdot \prod_{p|f} \left(\left|\ker\left(G_f \to G_{f/p}\right)\right| - 1\right)$$

where the product is extended over the maximal A-ideals p dividing f, and hence property 3 of the partition holds by Möbius inversion. □

4.2. A Λ-basis for $\mathcal{A}$. Let Λ be the polynomial ring over R generated by a collection $\{X_p\}$ of independent variables indexed by the maximal A-ideals. For each integral A-ideal f put

$$X_f := \prod_i X_{p_i}^{n_i}$$

where

$$f = \prod_i p_i^{n_i}$$

is the prime factorization of f. Then the collection of monomials $\{X_f\}$ indexed by the integral A-ideals is an R-basis of Λ. We equip $\mathcal{A}$ with the unique structure of Λ-module extending the R-module structure in such a way that

$$X_f\xi = \sum_{\eta \in Y_f^{-1}(\xi)} \eta$$

for all $\xi \in \Xi$ and integral A-ideals f. By the G-equivariance of the map Y_f, the action of G on $\mathcal{A}$ is Λ-linear.

For each integral A-ideal f, put $\Xi(f^\infty) := \bigcup_{N=1}^\infty \Xi(f^N)$, let $\mathcal{A}(f^\infty)$ be the R-span of $\Xi(f^\infty)$, and let $R\left[\{X_p\}_{p|f}\right]$ be the R-subalgebra of Λ generated by the variables X_p where p is a maximal A-ideal dividing f. Note that $\mathcal{A}(f^\infty)$ is a G-stable $R\left[\{X_p\}_{p|f}\right]$-submodule of $\mathcal{A}$.

THEOREM 4.2.1. *Let f be an integral A-ideal.*

1. *The elements of $\mathcal{A}(f)$ of the form $X_g\xi$ with g an integral A-ideal dividing f and $\xi \in \Xi_0 \cap \Xi(f/g)$ constitute an R-basis.*
2. *The elements of $\mathcal{A}(f^\infty)$ of the form $X_g\xi$ with g a integral A-ideal such that $\sqrt{g}$ divides $\sqrt{f}$ and $\xi \in \Xi_0 \cap \Xi(f^\infty)$ constitute an R-basis.*
3. *As an $R\left[\{X_p\}_{p|f}\right]$-module $\mathcal{A}(f^\infty)$ is free and the set $\Xi_0 \cap \Xi(f^\infty)$ is a basis.*
4. *As a Λ-module $\mathcal{A}$ is free and the set Ξ_0 is a basis.*

PROOF. Clearly $1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 4$. It will be enough to prove assertion 1. In turn, it will be enough to show that the family of elements of $\mathcal{A}(f)$ in question spans $\mathcal{A}(f)$ over R, because that family has cardinality

$$\sum_{g|f} |G_g| = \sum_{g|f} |\Xi^\times(g)| = |\Xi(f)|$$

by property 3 of the partition $\Xi = \coprod_{k=0}^\infty \Xi_k$. In turn, it will be enough to prove that

$$\mathcal{A}_k \cap \mathcal{A}^\times(f) \subseteq \left(\mathcal{A}_{k-1} \cap \mathcal{A}^\times(f)\right) + \sum_{p|f} \mathcal{A}(f/p) + \sum_{p|f} X_p\mathcal{A}(f/p) \tag{5}$$

where k is a positive integer, $\mathcal{A}_k$ is the R-span of Ξ_k, $\mathcal{A}^\times(f)$ is the R-span of $\Xi^\times(f)$, and the sums are extended over the maximal A-ideals p dividing f. But for each $\xi \in \Xi^\times(f) \cap \Xi_k$ there exists by property 1 of the partition $\Xi = \coprod_{k=0}^\infty \Xi_k$ a maximal A-ideal p such that

$$\xi - X_pY_p(\xi) \in \mathcal{A}_{k-1} \cap \mathcal{A}^\times(f) + \mathcal{A}(f/p),$$

and hence (5) does indeed hold. □

4.3. An R-basis for $U^{(\nu)}$. For each integral A-ideal f, put

$$U^{(\nu)}(f^\infty) := \lim_{N\to\infty} U^{(\nu)}(f^N) = \frac{\mathcal{A}(f^\infty)}{\sum_{p|f}(X_p - \nu_p)\mathcal{A}(f^\infty)}.$$

THEOREM 4.3.1. *Let f be an integral A-ideal.*

1. *The R-module $U^{(\nu)}$ is free and the set Ξ_0 gives rise to an R-basis.*
2. *The R-module $U^{(\nu)}(f^\infty)$ is free and the set $\Xi_0 \cap \Xi(f^\infty)$ gives rise to an R-basis.*
3. *The R-module $U^{(\nu)}(f)$ is free and the set $\Xi_0 \cap \Xi(f)$ gives rise to an R-basis.*
4. *With the exception in the archimedean case of f exactly divisible by 2, the natural map $U^{(\nu)}(f) \to U^{(\nu)}(f^\infty)$ induces an isomorphism in sign-homology.*

PROOF. 1. Clearly

$$R = \frac{\Lambda}{\sum_p(X_p - \nu_p)\Lambda}, \quad U^{(\nu)} = \frac{\mathcal{A}}{\sum_p(X_p - \nu_p)\mathcal{A}}.$$

By Theorem 4.2.1, the set Ξ_0 is a Λ-basis of $\mathcal{A}$, and therefore gives rise to an R-basis of $U^{(\nu)}$.

2. An argument similar to the preceding one proves this.

3. Let $\mathcal{A}_0$ be the R-span of Ξ_0. It is enough to show that the natural map $\mathcal{A}_0 \cap \mathcal{A}(f) \to U^{(\nu)}(f)$ is bijective, and injectivity is clear by what we have proved so far. By Theorem 4.2.1 we have

$$\mathcal{A}(f) = (\mathcal{A}_0 \cap \mathcal{A}(f)) \bigoplus \left(\sum_{1\neq g|f} X_g(\mathcal{A}_0 \cap \mathcal{A}(f/g)) \right)$$

and hence

$$\mathcal{A}(f) = (\mathcal{A}_0 \cap \mathcal{A}(f)) \bigoplus \left(\sum_{1\neq g|f} (X_g - \nu_g)(\mathcal{A}_0 \cap \mathcal{A}(f/g)) \right),$$

whence follows the surjectivity of map in question.

4. By Lemma 4.1.2 and what we have already proved, the set $\Xi_0 \cap (\Xi(f^\infty) \setminus \Xi(f))$ gives rise to an R-basis for the quotient $U^{(\nu)}(f^\infty)/U^{(\nu)}(f)$ that is stabilized by G_∞ and on which G_∞ acts freely. Consequently the sign-homology of the quotient $U^{(\nu)}(f^\infty)/U^{(\nu)}(f)$ vanishes. □

4.4. The sign-homology of $U^{(\nu)}$. Let $\mathcal{A}'$ be the R-submodule of $\mathcal{A}$ generated by $\Xi \setminus \Xi(1)$. Let $\Lambda[G]$ be the group ring of G with coefficients in Λ. Note that $\mathcal{A}$ is a $\Lambda[G]$-module and that $\mathcal{A}'$ is a $\Lambda[G]$-submodule. Let $R[G] \subset \Lambda[G]$ be the R-subalgebra generated by G and let $R[G_\infty] \subseteq \Lambda[G]$ be the R-subalgebra generated by G_∞. Let $\Xi^\dagger \subset \Xi$ be the union of all G_∞-orbits of cardinality $|G_\infty|$. Let $\mathcal{A}^\dagger$ be the R-span of $\Xi^\dagger$. Then $\mathcal{A}^\dagger$ is a free $R[G_\infty]$-module. Note that $\mathcal{A}^\dagger$ is a $\Lambda[G]$-submodule of $\mathcal{A}$. Note that $\mathcal{A}'$ is a $\Lambda[G]$-submodule of $\mathcal{A}$ containing $\mathcal{A}^\dagger$. Of course the only case in which $\mathcal{A}' \neq \mathcal{A}^\dagger$ is the archimedean case.

PROPOSITION 4.4.1. *In the archimedean case, X_p annihilates $\mathcal{A}'/\mathcal{A}^\dagger$ for all primes p.*

PROOF. One has $X_2[1/2+\mathbb{Z}] = [1/4+\mathbb{Z}] + [3/4+\mathbb{Z}]$; the case of an odd prime p is similarly trivial. □

THEOREM 4.4.2. *Assume either that we are in the nonarchimedean case or that $\nu_f \in R^\times$ for all integral A-ideals f. Let m be the order of G_∞ and let $\gamma_0 \in G_\infty$ be a generator. Fix a linear ordering of the set of maximal A-ideals arbitrarily. Then the directed family of graded $R[G]$-modules underlying the directed family*

$$\left\{H_*\left(\mathcal{K}\mathcal{T}^{\mathrm{tot}}\left((\mathcal{A}/\mathcal{A}')/\Lambda[G],\{\nu_p - X_p\}_{p|f},\left[\begin{array}{c}\sum_{i=0}^{m-1}\gamma_0^i\\ 1-\gamma_0\end{array}\right]\right)\right)\right\} \tag{6}$$

of graded $\Lambda[G]$-modules indexed by squarefree integral A-ideals f is isomorphic to the directed family

$$\left\{H_*\left(\mathcal{T}\left(U^{(\nu)}(f^\infty)/R[G],\left[\begin{array}{c}\sum_{i=0}^{m-1}\gamma_0^i\\ 1-\gamma_0\end{array}\right]\right)\right)\right\} \tag{7}$$

of graded $R[G]$-modules indexed by squarefree integral A-ideals f. (An explicit isomorphism is given in the proof.)

PROOF. Let f be a squarefree integral A-ideal. Let $\Lambda(f)[G]$ be the group ring of G with coefficients in the R-subalgebra $\Lambda(f) \subseteq \Lambda$ generated by the variables X_p for p ranging over maximal A-ideals dividing f. Consider the following chain complexes of $\Lambda(f)[G]$-modules.

$$\mathcal{K}\mathcal{T}^{\mathrm{tot}}\left((\mathcal{A}/\mathcal{A}')/\Lambda(f)[G],\{\nu_p - X_p\}_{p|f},\left[\begin{array}{c}\sum_{i=0}^{m-1}\gamma_0^i\\ 1-\gamma_0\end{array}\right]\right) \tag{8}$$

$$\mathcal{K}\mathcal{T}^{\mathrm{tot}}\left(\mathcal{A}(f^\infty)/\Lambda(f)[G],\{\nu_p - X_p\}_{p|f},\left[\begin{array}{c}\sum_{i=0}^{m-1}\gamma_0^i\\ 1-\gamma_0\end{array}\right]\right) \tag{9}$$

$$\overline{\mathcal{T}}\left(\mathcal{A}(f^\infty)/\Lambda(f)[G],\{\nu_p - X_p\}_{p|f},\left[\begin{array}{c}\sum_{i=0}^{m-1}\gamma_0^i\\ 1-\gamma_0\end{array}\right]\right) \tag{10}$$

The chain complex (8) is naturally a quotient of (9) because

$$\mathcal{A}/\mathcal{A}' = \mathcal{A}(f^\infty)/(\mathcal{A}(f^\infty)\cap\mathcal{A}').$$

The chain complex (10) is naturally a quotient of (9) because they are companions of the double complex

$$\mathcal{K}\mathcal{T}\left(\mathcal{A}(f^\infty)/\Lambda(f)[G],\{\nu_p - X_p\}_{p|f},\left[\begin{array}{c}\sum_{i=0}^{m-1}\gamma_0^i\\ 1-\gamma_0\end{array}\right]\right). \tag{11}$$

We claim that both quotient maps induce homology isomorphisms; the claim granted, the isomorphism from the homology of (8) to the homology of (10) provided by the claim induces (for variable f) the desired isomorphism from the directed family of graded $R[G]$-modules underlying (6) to the directed family (7).

We turn to the proof of the claim. Clearly the chain complex

$$\mathcal{T}\left(\mathcal{A}(f^\infty)\cap\mathcal{A}^\dagger/\Lambda(f)[G],\left[\begin{array}{c}\sum_{i=0}^{m-1}\gamma_0^i\\ 1-\gamma_0\end{array}\right]\right)$$

is acyclic, and hence by Proposition 2.5.1 the chain complex

$$\mathcal{K}\mathcal{T}^{\mathrm{tot}}\left(\mathcal{A}(f^\infty)\cap\mathcal{A}^\dagger/\Lambda(f)[G],\{\nu_p - X_p\}_{p|f},\left[\begin{array}{c}\sum_{i=0}^{m-1}\gamma_0^i\\ 1-\gamma_0\end{array}\right]\right) \tag{12}$$

is acyclic. The chain complex

$$\mathcal{K}\left(\left(\frac{\mathcal{A}(f^\infty)\cap\mathcal{A}'}{\mathcal{A}(f^\infty)\cap\mathcal{A}^\dagger}\right)/\Lambda(f)[G],\{\nu_p - X_p\}_{p|f}\right)$$

vanishes in the nonarchimedean case and is acyclic in the archimedean case by Proposition 2.5.1 and Proposition 4.4.1. Therefore the chain complex

$$\mathcal{K}\mathcal{T}^{\mathrm{tot}}\left(\left(\frac{\mathcal{A}(f^\infty)\cap\mathcal{A}'}{\mathcal{A}(f^\infty)\cap\mathcal{A}^\dagger}\right)/\Lambda(f)[G],\{\nu_p - X_p\}_{p|f},\left[\begin{array}{c}\sum_{i=0}^{m-1}\gamma_0^i\\ 1-\gamma_0\end{array}\right]\right) \tag{13}$$

is acyclic by Proposition 2.5.1. The acyclicity of the chain complexes (12) and (13) implies that the quotient map from (9) to (8) is a homology isomorphism. Now $\mathcal{A}(f^\infty)$ is by Theorem 4.2.1 a free $\Lambda(f)[G]$-module. It follows by Proposition 2.5.1 that the complex

$$\mathcal{K}\left(\mathcal{A}(f^\infty)/\Lambda(f)[G],\{\nu_p - X_p\}_{p|f}\right)$$

is acyclic in positive degree, and hence by Proposition 2.5.1 the quotient map from (9) to (10) is indeed a homology isomorphism. The claim is proved. $\square$

5. The universal ordinary distribution

For the remainder of the paper we specialize the preceding theory as follows. We take the coefficient ring R to be $\mathbb{Z}$ and we take $\nu_f = 1$ for all integral A-ideals f. Then $\mathcal{A}$ becomes the free abelian group generated by the set Ξ and U becomes the quotient of $\mathcal{A}$ by the subgroup generated by all elements of the form $\xi - \sum_{\eta\in Y_p^{-1}(\xi)}\eta$ with $\xi \in \Xi$ and p a maximal A-ideal. We now write simply U instead of $U^{(\nu)}$ and $U(f)$ instead of $U^{(\nu)}(f)$. We call U the *universal ordinary distribution.*

5.1. Comparison of $U(f)$ and $U'(f)$. For each locally constant homomorphism $\chi : G \to \mathbb{C}^\times$, there exists a unique integral A-ideal c such that for all integral A-ideals f, the homomorphism χ factors through G_f if and only if c divides f; the integral A-ideal c is called the *conductor* of χ. Given a locally constant homomorphism $\chi : G \to \mathbb{C}^\times$ of conductor c and a maximal A-ideal p, if p does not divide c, let $\chi(p)$ denote the value of χ at any $\sigma \in G$ projecting to the $\sim_c$-equivalence class of p in G_c, and otherwise, if p does divide c, put $\chi(p) := 0$.

LEMMA 5.1.1. *There exists a unique homomorphism $u : \mathcal{A} \to \mathbb{Q}$ such that for all integral A-ideals f and locally constant homomorphisms $\chi : G \to \mathbb{C}^\times$ of conductor dividing f one has*

$$\int_G u(\gamma[1+f])\chi(\gamma)d\mu(\gamma) := \frac{1}{|G_f|}\prod_{p|f}(1-\chi(p))$$

where μ is Haar probability measure on G and the product is extended over the maximal A-ideals p dividing f. Necessarily u factors through the universal ordinary distribution U.

PROOF. Existence and uniqueness of u are clear in view of Proposition 3.4.4. Fix a maximal A-ideal p and consider the unique homomorphism $v : \mathcal{A} \to \mathbb{Q}$ such that $v(\xi) = u(X_p\xi)$ for all $\xi \in \Xi$. It will be enough to prove that $u = v$. Let f be any integral A-ideal divisible by p. Write $f = cp^n$ with $n \geq 1$ and c prime to p. Select a subset $S \subset G$ mapping bijectively to $\ker\left(G_f \to G_{f/p}\right)$, and select $\phi \in G$ such that ϕ and p have a common image in the generalized ideal class group G_c. For all locally constant homomorphisms $\chi : G \to \mathbb{C}^\times$ of conductor dividing f/p, by

Lemma 4.1.1 and the definition of u, one has

$$\begin{aligned}
&\int_G v(\gamma[1+f/p])\chi(\gamma)d\mu(\gamma)\\
=\ &\int_G \left(\sum_{\sigma\in S} u(\sigma\gamma[1+f]) + \begin{cases} u(\phi^{-1}\gamma[1+f/p]) & \text{if } n=1\\ 0 & \text{if } n>1\end{cases}\right)\chi(\gamma)d\mu(\gamma)\\
=\ &\frac{1}{|G_{f/p}|}\prod_{q|(f/p)}(1-\chi(q))
\end{aligned}$$

where the product is extended over the maximal A-ideals q dividing f. Therefore $u = v$, and we are done. □

For each integral A-ideal f, let $U'(f)$ be the $\mathbb{Z}[G_f]$-submodule of $\mathbb{Q}[G_f]$ generated by elements of the form

$$\sum_{\gamma\in G_f} u(\tilde{\gamma}[1+g])\gamma^{-1} \in \mathbb{Q}[G_f]$$

where g is any integral A-ideal dividing f and $\tilde{\gamma}\in G$ is any lifting of $\gamma\in G_f$. It is easy to check that $U'(f)$ is a free abelian group of rank $|G_f|$. In the archimedean case $U'(f)$ coincides with the module denoted by U in Sinnott's paper [**16**], and in the nonarchimedean case with the module denoted by U in Yin's paper [**17**]. We remark that Yin worked under the additional hypothesis (not made in this paper) that the infinite valuation of k is of degree 1 over the constant field of k; in that case every principal ideal is automatically principal in the narrow sense. In all cases, because the homomorphism u factors through the universal ordinary distribution U, it follows formally that $\operatorname{Inf}_{G_f}^G U'(f)$ is G-equivariantly a quotient of $U(f)$ and hence G-equivariantly isomorphic to $U(f)$ because the underlying abelian groups are free of the same rank, namely $|G_f|$.

5.2. Proof of Yin's conjecture. Assume now that we are in the nonarchimedean case. Let $\tilde{\Lambda}$ be the ring obtained from Λ by inverting the variables X_p for p ranging over maximal A-ideals, and let $\Gamma\subset\tilde{\Lambda}^\times$ be the subgroup generated by those variables. Then $\tilde{\Lambda}$ is the integral group ring of Γ, and Γ is a free abelian group for which the family of elements of the form X_p for p a maximal A-ideal constitute a basis. Note that the group Γ is a copy of the group of fractional A-ideals. Let $\tilde{\Lambda}[G]$ be the group ring of G with coefficients in $\tilde{\Lambda}$, and let $\Gamma G\subset\tilde{\Lambda}[G]^\times$ be the subgroup generated by Γ and G. Then the natural map $\Gamma\times G\to\Gamma G$ is an isomorphism and $\tilde{\Lambda}[G]$ may be viewed as the integral group ring of ΓG. Let $\Pi\subseteq\Gamma G$ be the kernel of the unique homomorphism $\Gamma G\to G_1$ under which each $\gamma\in G$ maps to its image in G_1, and each variable X_p with p a maximal A-ideal maps to its narrow ideal class. Note that the group $\Gamma G/\Pi$ is a copy of G_1. Recall that $\mathcal{A}'$ is the subgroup of $\mathcal{A}$ generated by $\Xi\setminus\Xi(1)$.

LEMMA 5.2.1. *For every maximal A-ideal p, the action of X_p on $\mathcal{A}/\mathcal{A}'$ is invertible, and hence $\mathcal{A}/\mathcal{A}'$ can be viewed as a ΓG-module; as such, $\mathcal{A}/\mathcal{A}'$ is isomorphic to* $\operatorname{Ind}_\Pi^{\Gamma G}\operatorname{Inf}_{\{1\}}^\Pi\mathbb{Z}$.

PROOF. For any A-lattice W, maximal A-ideals p and q, and $\gamma \in G$ such that γ and q have a common image in G_1, one has

$$\begin{aligned}\gamma X_p[W] &= [q^{-1}p\cdot W] + \sum_{0\neq y\in q^{-1}p\cdot W/p\cdot W}[y+p\cdot W]\\ &\equiv [q^{-1}p\cdot W] \bmod \mathcal{A}'.\end{aligned}$$

The result follows straightforwardly from this identity. □

For each integral A-ideal f, let $\Gamma(f)$ be the subgroup of Γ generated by the variables of the form X_p for some maximal A-ideal p dividing f.

LEMMA 5.2.2. *Let f be an integral A-ideal. Then the group $\Gamma(f)G_\infty \cap \Pi$ is isomorphic to the subgroup of $k^\times$ consisting of elements that are units at all maximal A-ideals not dividing f. In particular, $\Gamma(f)G_\infty \cap \Pi$ is almost free of rank r with torsion subgroup of order w, where r is the number of distinct maximal A-ideals dividing f, and w is the number of roots of unity in k.*

PROOF. For each $a \in k^\times$, there exists unique $\gamma(a) \in G_\infty$ such that

$$\operatorname{sgn}\gamma(a)\operatorname{sgn}a = 1,$$

where $\operatorname{sgn}\gamma$ is as defined in Proposition 3.5.2. One can check that the map

$$a \mapsto X_{(a)}\gamma(a) : k^\times \to \Gamma G$$

induces an isomorphism $k^\times \tilde{\to} \Gamma G_\infty \cap \Pi$, whence the result via the Dirichlet unit theorem. □

The following was conjectured L. S. Yin [**17**, p. 64] in the case that the infinite valuation of k is of degree 1 over the constant field of k.

THEOREM 5.2.3. *Let f be a nonunit integral A-ideal and identify G_∞ with a subgroup of G_f under the natural map. Let H_f be the subgroup of the narrow ideal class group G_1 generated by the narrow ideal classes of the maximal A-ideals dividing f and the fractional A-ideals principal in the wide sense. Then the sign-homology of $U'(f)$ is in each degree G_f-equivariantly isomorphic to*

$$\operatorname{Inf}_{G_1}^{G_f}\operatorname{Ind}_{H_f}^{G_1}\operatorname{Inf}_{\{1\}}^{H_f}(\mathbb{Z}/w\mathbb{Z})^{2^{r-1}},$$

where r is the number of distinct maximal A-ideals dividing f, and w is the number of roots of unity of k.

PROOF. We work with the G-module $U(f)$ instead of the G_f-module $U'(f)$. By Theorem 4.3.1 it will be enough to show that the sign-homology of $U(f^\infty)$ is in each degree G-equivariantly isomorphic to

$$\operatorname{Inf}_{G_1}^{G}\operatorname{Ind}_{H_f}^{G_1}\operatorname{Inf}_{\{1\}}^{H_f}(\mathbb{Z}/w\mathbb{Z})^{2^{r-1}} = \operatorname{Res}_G^{\Gamma G}\operatorname{Ind}_{\Pi\Gamma(f)G_\infty}^{\Gamma G}\operatorname{Inf}_{\{1\}}^{\Pi\Gamma(f)G_\infty}(\mathbb{Z}/w\mathbb{Z})^{2^{r-1}}.$$

Now by Theorem 4.4.2, the sign-homology of $U(f^\infty)$ is isomorphic as a graded G-module to the graded G-module underlying the homology of the chain complex

$$\mathcal{KT}^{\mathrm{tot}}\left((\mathcal{A}/\mathcal{A}')/\Lambda[G], \{1-X_p\}_{p|f}, \left[\begin{array}{c}\sum_{i=0}^{m-1}\gamma_0\\ 1-\gamma_0\end{array}\right]\right),$$

where $\gamma_0 \in G_\infty$ is a generator. In turn, by Lemma 5.2.1, we can identify the homology of the latter complex with the graded $\Lambda[G]$-module underlying the homology of the chain complex

$$\mathcal{KT}^{\mathrm{tot}}\left(\mathrm{Ind}_{\Pi}^{\Gamma G}\mathrm{Inf}_{\{1\}}^{\Pi}\mathbb{Z}/\mathbb{Z}[\Gamma G], \{1-X_p\}_{p|f}, \begin{bmatrix} \sum_{i=0}^{m-1}\gamma_0 \\ 1-\gamma_0 \end{bmatrix}\right).$$

By Proposition 2.6.4 the homology of the latter complex is isomorphic as a graded ΓG-module to

$$\mathrm{Ind}_{\Pi\Gamma(f)G_\infty}^{\Gamma G}\mathrm{Inf}_{\{1\}}^{\Pi\Gamma(f)G_\infty}\hat{H}_*(\Gamma(f)G_\infty \cap \Pi).$$

Finally, by Proposition 2.6.3 and Lemma 5.2.2, the Farrell-Tate homology group $\hat{H}_*((\Gamma(f)G_\infty)\cap\Pi)$ is in each degree a free $(\mathbb{Z}/w\mathbb{Z})$-module of rank 2^{r-1}. The proof of Yin's conjecture is complete. □

5.3. The archimedean case: the double complex $\mathcal{SK}$. We narrow the focus to the archimedean case. We are going to explain how the general theory developed above specializes to the classical situation originally contemplated by Iwasawa, Sinnott and Kubert. We speak now of positive integers and prime numbers rather than integral and maximal A-ideals. We identify $\mathcal{A}$ with the free abelian group on symbols of the form $[a]$ with $a \in \mathbb{Q}/\mathbb{Z}$, and thus identify U with the universal ordinary distribution as defined by Kubert. Fix a positive integer $f > 1$ such that $f \not\equiv 2 \bmod 4$. We identify $U(f)$ with Kubert's universal level f ordinary distribution. We also write $U(f^\infty) := \lim_{n\to\infty} U(f^n)$, and we put $\frac{1}{f^\infty}\mathbb{Z}/\mathbb{Z} := \bigcup_{n=1}^\infty \frac{1}{f^n}\mathbb{Z}/\mathbb{Z}$.

By Theorem 4.3.1, we have at our disposal a subset $X_0 \subset \mathbb{Q}/\mathbb{Z}$ giving rise to a basis of U such that the set $X_0 \cap \frac{1}{f}\mathbb{Z}/\mathbb{Z}$ is of cardinality $|G_f|$ and gives rise to a basis of $U(f)$. Thus we recover Kubert's result to the effect that the natural map $U(f) \to U$ is a split monomorphism with source a free abelian group of rank $|G_f|$. From Theorem 4.3.1 we also get a little more, namely that the map $U(f) \to U(f^\infty)$ induces an isomorphism in sign-(co)homology.

Consider the free abelian group $\mathcal{SK}$ generated by symbols of the form $[a, g, n]$ where $a \in \mathbb{Q}/\mathbb{Z}$, g is a squarefree positive integer and n is an integer. (The notation $\mathcal{SK}$ is meant to call Sinnott and Kubert to mind.) Let G operate on $\mathcal{SK}$ by the rule $\sigma[a, g, n] := [ta, g, n]$, where t is any integer such that for any root of unity ζ of order equal to the denominator of a, one has $\sigma\zeta = \zeta^t$. Equip $\mathcal{SK}$ with a G-stable bigrading $\mathcal{SK} = \bigoplus_m \bigoplus_n \mathcal{SK}_{mn}$ by declaring the symbol $[a, g, n]$ to be of bidegree (m, n), where m is the number of prime factors of g. Equip $\mathcal{SK}$ with a G-equivariant differential of bidegree $(0, -1)$ by the rule

$$\delta[a, g, n] := (-1)^m([a, g, n-1] + (-1)^n[-a, g, n-1])$$

and a G-equivariant differential ∂ of bidegree $(-1, 0)$ by the rule

$$\partial[a, g, n] := \sum_{i=1}^m (-1)^{i-1}\left([a, g/p_i, n] - \sum_{p_i b = a}[b, g/p_i, n]\right)$$

where $p_1 < \cdots < p_m$ are the primes dividing g. Let $\mathcal{SK}' \subset \mathcal{SK}$ be the subgroup generated by symbols $[a, g, n]$ with $a \neq 0$. Let $\mathcal{SK}(f) \subset \mathcal{SK}$ be the subgroup generated by symbols $[a, g, n]$ where $a \in \frac{1}{f}\mathbb{Z}/\mathbb{Z}$ and put $\mathcal{SK}(f^\infty) := \bigcup_{n=1}^\infty \mathcal{SK}(f^n)$. Finally, let $\mathcal{N}$ be the subgroup generated by all symbols of the form $[a, g, n]$ with

$g \neq 1$, and by all elements of the form $\partial[a, g, n]$ where g is prime. Note that $\mathcal{SK}'$, $\mathcal{SK}(f^\infty)$, and $\mathcal{N}$ are bigraded, G-, ∂- and δ-stable subgroups of $\mathcal{SK}$.

Now on the one hand, the total complex associated to the double complex

$$\frac{\mathcal{SK}(f^\infty)}{\mathcal{SK}(f^\infty) \cap \mathcal{N}}$$

in an obvious way computes the sign-homology of $U(f^\infty)$. But the double complex (11) figuring in the proof of Theorem 4.4.2 can (as a double complex of G-modules) be identified with $\mathcal{SK}(f^\infty)$, and what the proof of the theorem says in the present context is that the quotient maps

$$\begin{array}{ccc} \mathcal{SK}(f^\infty) & \rightarrow & \dfrac{\mathcal{SK}(f^\infty)}{\mathcal{SK}(f^\infty) \cap \mathcal{SK}'} \\ \downarrow & & \\ \dfrac{\mathcal{SK}(f^\infty)}{\mathcal{SK}(f^\infty) \cap \mathcal{N}} & & \end{array}$$

induce isomorphisms in homology of associated total complexes. In particular, the double complex

$$\frac{\mathcal{SK}(f^\infty)}{\mathcal{SK}(f^\infty) \cap \mathcal{SK}'}$$

also computes the sign-homology of $U(f^\infty)$. But the latter double complex has an extremely simple structure: it is a copy of the double complex

$$\mathcal{KT}\left(\mathbb{Z}/\mathbb{Z}, \{0\}_{p|f}, \begin{bmatrix} 2 \\ 0 \end{bmatrix}\right)$$

which, if employed as in the proof of Proposition 2.6.3, computes the Farrell-Tate homology of the subgroup of $\mathbb{Q}^\times$ generated by -1 and the primes p dividing f. Thus, in confirmation of Sinnott's result, we find that the sign-(co)homology of $U(f^\infty)$ (and therefore also that of $U(f)$) is in each degree a vector space over $\mathbb{F}_2$ of rank 2^{r-1}, where r is the number of prime divisors of f.

Passing to the limit over f, we can identify the sign-homology of U with the homology of the total complex associated to the double complex $\mathcal{SK}/\mathcal{SK}'$. It is easy to see that the natural map

$$\frac{\mathcal{SK}(f^\infty)}{\mathcal{SK}(f^\infty) \cap \mathcal{SK}'} \rightarrow \frac{\mathcal{SK}}{\mathcal{SK}'}$$

of double complexes is isomorphic to the natural map

$$\mathcal{KT}\left(\mathbb{Z}/\mathbb{Z}, \{0\}_{p|f}, \begin{bmatrix} 2 \\ 0 \end{bmatrix}\right) \rightarrow \mathcal{KT}\left(\mathbb{Z}/\mathbb{Z}, \{0\}_{p:\text{any prime}}, \begin{bmatrix} 2 \\ 0 \end{bmatrix}\right)$$

of double complexes. Thus, in confirmation of Kubert's result, we find that the natural map $U(f^\infty) \rightarrow U$ induces a monomorphism in sign-homology. Finally, it is clear that G acts trivially on $\mathcal{SK}/\mathcal{SK}'$, and in confirmation of Sinnott's result, we find that G acts trivially on the sign-(co)homology U and *a fortiori* on the sign-homology of $U(f)$.

6. Acknowledgements

I thank W. Sinnott for correspondence about topics related to his work. I thank M. Feshbach for providing me with a reference (namely [**1**]). I thank G. Mislin for correspondence about his work. I thank the organizers of the conference on Recent Progress in Algebra at the Korea Advanced Institute of Science and Technology for inviting me and for producing a well run and enjoyable conference. I am especially grateful to my students S. Sinha and P. Das for teaching me a lot about the topics discussed in this paper.

References

[1] K. S. Brown, *Cohomology of Groups*, Graduate Texts in Mathematics **87**, Springer-Verlag, New York, 1982

[2] P. Das, *Double coverings of cyclotomic fields arising from algebraic* Γ*-monomials*, PhD thesis, University of Minnesota, June 1997.

[3] P. Das, *Algebraic Gamma monomials and double coverings of cyclotomic fields*, TAMS (to appear)

[4] P. Deligne, *Valeurs de fonctions L et périodes d'intégrales*, Proc. of Symp. in Pure Math. **33(2)**(1979)313-346.

[5] P. Deligne, J. S. Milne, A. Ogus, K.-Y. Shih, *Hodge Cycles, Motives, and Shimura Varieties*, Lecture Notes in Math. **900**, Springer Verlag, New York 1982.

[6] F. T. Farrell, *An extension of Tate cohomology to a class of infinite groups*, J. Pure Appl. Algebra **10**(1977)153-161.

[7] S. Galovich and M. Rosen, *Units and class groups in cyclotomic function fields*, J. Number Theory **14**(1982)156-184.

[8] D. Goss, *Basic Structures of Function Field Arithmetic*, Ergeb. der Math. und ihrer Grenzgebiete, 3. Folge, Vol. 35, Springer Verlag, Berlin Heidelberg 1996.

[9] D. Hayes, *Analytic class number formulas in function fields*, Invent. Math. **65**(1981)49-69.

[10] D. Hayes, *A brief introduction to Drinfeld modules*, in: *The arithmetic of function fields*, D. Goss, D. Hayes, M. Rosen, eds., pp. 1-32, W. de Gruyter, Berlin New York 1992.

[11] D. S. Kubert, *The universal ordinary distribution*, Bull. Soc. Math. France **107**(1979)179-202.

[12] D. S. Kubert, *The* $\mathbb{Z}/2\mathbb{Z}$*-cohomology of the universal ordinary distribution*, Bull. Soc. Math. France **107**(1979)203-224.

[13] S. Lang, *Cyclotomic Fields I and II*, Graduate Texts in Mathematics **121**, Springer-Verlag, New York 1990.

[14] G. Mislin, *Tate cohomology for arbitrary groups via satellites*, Topology and its Applications **56**(1994)293-300.

[15] S. K. Sinha, *Deligne's reciprocity for function fields*, J. Number Theory **63**(1997)65-88.

[16] W. Sinnott, *On the Stickelberger ideal and the circular units of a cyclotomic field*, Ann. Math. **108**(1978)107-134.

[17] L. S. Yin, *Index-class number formulas over global function fields*, Compositio Math. **107**(1997)49-66.

School of Mathematics, University of Minnesota, Minneapolis, MN 55455
E-mail address: `gwanders@math.umn.edu`

This page intentionally left blank

http://dx.doi.org/10.1090/conm/224/03190

Contemporary Mathematics
Volume **224**, 1999

Down-up Algebras and Witten's Deformations of the Universal Enveloping Algebra of $\mathfrak{sl}_2$

Georgia Benkart

ABSTRACT. Down-up algebras originated in the study of differential posets. In this paper we explain their relationship to Witten's 7-parameter family of deformations of the universal enveloping algebra $U(\mathfrak{sl}_2)$ of the Lie algebra $\mathfrak{sl}_2$ and to the subfamily of conformal $\mathfrak{sl}_2$ algebras singled out by Le Bruyn. Down-up algebras exhibit many of the important features of $U(\mathfrak{sl}_2)$ including a Poincaré-Birkhoff-Witt type basis and a well-behaved representation theory. We describe Verma modules for down-up algebras and results on category $\mathcal{O}$ modules for them.

§1. Down-up algebras and their combinatorial origins

Differential posets.

Assume P is a partially ordered set (poset), and let $\mathbf{C}P$ denote the complex vector space whose basis is the set P. For many posets there are two well-defined transformations on $\mathbf{C}P$, the down and up operators, which come from the order relation on P and are defined by

$$d(y) = \sum_{x \prec y} x \qquad \text{and} \qquad u(y) = \sum_{y \prec z} z.$$

Thus, $d(y)$ is the sum of all the elements x of P that y covers, and $u(y)$ is the sum of all the elements z of P that cover y.

The characterizing property of an r-differential poset is that the down and up operators satisfy $du - ud = rI$ for some positive integer r, where I is the

1991 *Mathematics Subject Classification.* Primary 16S15, 16S30, 17B35, 17B10 Secondary 81R50, 06A07.

Support from National Science Foundation Grant #DMS–9622447 is gratefully acknowledged. A lecture based on this article was presented at the *Recent Progress in Algebra Conference*, Taejon, Korea, August 1997. We express sincere thanks to KAIST for its hospitality during this meeting. Section 2 of this paper contains new results not discussed at the conference. We realized the connections with Witten's deformation algebras after receiving a copy of Kulkarni's paper [K]. We thank Kaiming Zhao for his comments on an earlier version of this paper.

identity transformation (see [St]). Thus, the space $\mathbf{C}P$ affords a representation of the Weyl algebra, (the associative algebra with generators y, x subject to the relation $yx - xy = 1$), via the mapping $y \mapsto d/r$, and $x \mapsto u$. Since the Weyl algebra also can be realized as differential operators $y \mapsto d/dx$ and $x \mapsto x$ (multiplication by x) on $\mathbf{C}[x]$, Stanley referred to the posets satisfying $du - ud = rI$ as r-differential. Fomin [F] studied essentially the same class of posets (when $r = 1$), calling them "Y-graphs". This terminology comes from the fact that Young's lattice of all partitions of all nonnegative integers provides an important example.

A partition μ of an integer m can be regarded as a descending sequence $\mu = (\mu_1 \geq \mu_2 \geq \dots)$ of parts whose sum $|\mu| = \sum_i \mu_i$ equals m. If $\nu = (\nu_1 \geq \nu_2 \geq \dots)$ is a second partition, then $\mu \leq \nu$ when $\mu_i \leq \nu_i$ for all i. The partition ν covers μ (written $\mu \prec \nu$) if $\mu \leq \nu$ and $|\nu| = 1 + |\mu|$. Thus, $\mu \prec \nu$ if the partition μ is obtained from ν by subtracting 1 from exactly one of the parts of ν, and $d(\nu)$ is the sum of all such μ. Analogously, $u(\nu)$ is the sum of all partitions π obtained from ν by adding 1 to one part of ν. Many interesting enumerative and combinatorial properties of Young's lattice can be deduced from fact that it is a 1-differential poset (see [St] and [F]).

The down and up operators on the partition poset also have a representation theoretic significance. The simple modules of the symmetric group S_n are indexed by the partitions ν of n. Upon restriction to S_{n-1} the representation labelled by ν decomposes into a direct sum of simple S_{n-1}-modules indexed by the partitions $\mu \prec \nu$, so it is given by $d(\nu)$. When the simple module labelled by ν is induced to a representation of S_{n+1}, it decomposes into a sum of simple S_{n+1}-modules indexed by partitions π of $n+1$ such that $\nu \prec \pi$, which is just $u(\nu)$.

In his study of *uniform posets* [T], Terwilliger considered finite ranked posets P whose down and up operators satisfy the following relation

$$d_i d_{i+1} u_i = \alpha_i d_i u_{i-1} d_i + \beta_i u_{i-2} d_{i-1} d_i + \gamma_i d_i,$$

where d_i and u_i denote the restriction of d and u to the elements of rank i. (There is an analogous second relation,

$$d_{i+1} u_i u_{i-1} = \alpha_i u_{i-1} d_i u_{i-1} + \beta_i u_{i-1} u_{i-2} d_{i-1} + \gamma_i u_{i-1},$$

which holds automatically in this case because d_{i+1} and u_i are adjoint operators relative to a certain bilinear form.) In many instances the constants in these relations do not depend on the rank i. In those examples, the down and up operators satisfy

$$\begin{aligned} d^2 u &= q(q+1) dud - q^3 ud^2 + rd \\ du^2 &= q(q+1) udu - q^3 u^2 d + ru \end{aligned}$$

where q and r are fixed complex numbers. Such a poset is said to be "(q, r)-differential," and many interesting examples of (q, r)-differential posets are constructed in [T] from certain subspaces of a vector space over a finite field.

1. Assume W is an n-dimensional vector space over $GF(q)$, the field of q elements, and consider the set of pairs $P = \{(U, f) \mid U$ is a subspace of W and f is an alternating bilinear form on $U\}$ with the ordering: $(U, f) \leq (V, g)$ if

U is a subspace of V and $g|_U = f$. Then P is a (q, r)-differential poset with $r = -q^n(q+1)$.

2. In Example 1 replace "an alternating bilinear form" with "a quadratic form". The resulting poset P is $(q, -q^{n+1}(q+1))$-differential.

3. In this example assume W is an n-dimensional space over $GF(q^2)$ and the bilinear forms are Hermitian. The poset P is $(q^2, -q^{2n+1}(q^2+1))$-differential in this case.

Down-up algebras.

To study the algebra generated by the down and up operators of a poset and its action on the poset, we introduced the notion of a down-up algebra in our joint work with Roby (see [BR]). Although the initial motivation for our investigations came from posets, we made no assumptions about the existence of posets whose down and up operators satisfy our relations. However, when such a poset exists, it affords a representation of the down-up algebra, and so our primary focus in [BR] was on determining explicit information about the representations of down-up algebras. Proofs of the results stated in this paper and more detailed explanations can be found in [BR].

DEFINITION 1.1. Let α, β, γ be fixed but arbitrary complex numbers. The unital associative algebra $A(\alpha, \beta, \gamma)$ over $\mathbf{C}$ with generators d, u and defining relations

(R1) $d^2u = \alpha dud + \beta ud^2 + \gamma d$,

(R2) $du^2 = \alpha udu + \beta u^2d + \gamma u$,

is a *down-up algebra.*

It is easy to see that when $\gamma \neq 0$ the down-up algebra $A(\alpha, \beta, \gamma)$ is isomorphic to $A(\alpha, \beta, 1)$ by the map, $d \mapsto d'$, $u \mapsto \gamma u'$. Therefore, it would suffice to treat just two cases $\gamma = 0, 1$, but to avoid dividing considerations into these two cases, we retain the notation γ.

Examples of down-up algebras.

If B is the associative algebra generated by the down and up operators d, u of a (q, r)-differential poset P, then relations (R1) and (R2) hold with $\alpha = q(q+1)$, $\beta = -q^3$, and $\gamma = r$. Thus, B is a homomorphic image of the algebra $A(\alpha, \beta, \gamma)$ with these parameters, and the action of B on $\mathbf{C}P$ gives a representation of $A(\alpha, \beta, \gamma)$.

The relation $du - ud = rI$ of an r-differential poset, can be multiplied on the left by d and on the right by d and the resulting equations can be added to get the relation $d^2u - ud^2 = 2rd$ of a $(-1, 2r)$-differential poset. Thus, the Weyl algebra is a homomorphic image (by the ideal generated by $du - ud - r1$) of the algebra $A(0, 1, 2r)$. The q-Weyl algebra is a homomorphic image of the algebra $A(0, q^2, q+1)$ by the ideal generated by $du - qud - 1$. The skew polynomial algebra $\mathbf{C}_q[d, u]$, or quantum plane (see [M]), is the associative algebra with generators d, u which satisfy the relation $du = qud$. Therefore, $\mathbf{C}_q[d, u]$ is a homomorphic image (by the ideal generated by $du - qud$) of the algebra $A(2q, -q^2, 0)$.

Suppose $\mathfrak{g}$ is a 3-dimensional Lie algebra over $\mathbf{C}$ with basis $x, y, [x, y]$ such that $[x[x, y]] = \gamma x$ and $[[x, y], y] = \gamma y$. In the universal enveloping algebra $U(\mathfrak{g})$ of $\mathfrak{g}$, the relations above become

$$x^2y - 2xyx + yx^2 = \gamma x$$
$$xy^2 - 2yxy + y^2x = \gamma y.$$

Thus, $U(\mathfrak{g})$ is a homomorphic image of the down-up algebra $A(2, -1, \gamma)$ via the mapping $\phi : A(2, -1, \gamma) \to U(\mathfrak{g})$ with $\phi : d \mapsto x$, $\phi : u \mapsto y$. The mapping $\psi : \mathfrak{g} \to A(2, -1, \gamma)$ with $\psi : x \mapsto d$, $\psi : y \mapsto u$, and $\psi : [x, y] \mapsto du - ud$ extends, by the universal property of $U(\mathfrak{g})$, to an algebra homomorphism $\psi : U(\mathfrak{g}) \to A(2, -1, \gamma)$ which is the inverse of ϕ. Consequently, $U(\mathfrak{g})$ is isomorphic to $A(2, -1, \gamma)$.

The Lie algebra $\mathfrak{sl}_2$ of 2×2 complex matrices of trace zero has a standard basis e, f, h, which satisfies $[e, f] = h$, $[h, e] = 2e$, and $[h, f] = -2f$. From this we see that $U(\mathfrak{sl}_2) \cong A(2, -1, -2)$. The Heisenberg Lie algebra $\mathfrak{H}$ has a basis x, y, z where $[x, y] = z$, and $[z, \mathfrak{H}] = 0$. Thus, $U(\mathfrak{H}) \cong A(2, -1, 0)$.

S.P. Smith [Sm] investigated a class of associative algebras having a presentation by generators a, b, h and relations $[h, a] = a$, $[h, b] = -b$ and $ab - ba = f(h)$, where $f(h)$ is a polynomial in h. In the special situation that $\deg(f) \leq 1$, such an algebra is a homomorphic image of a down-up algebra $A(2, -1, \gamma)$ for some γ.

The 2×2 complex matrices $y = \begin{pmatrix} y_1 & y_2 \\ y_3 & y_4 \end{pmatrix}$ with supertrace $y_1 - y_4 = 0$ is the special linear Lie superalgebra $L = \mathfrak{sl}(1, 1) = L_{\overline{0}} \oplus L_{\overline{1}}$ under the supercommutator $[x, y] = xy - (-1)^{ab}yx$ for $x \in L_{\overline{a}}$, $y \in L_{\overline{b}}$. It has a presentation by generators e, f (which belong to $L_{\overline{1}}$ and can be identified with the matrix units $e = e_{1,2}$, $f = e_{2,1}$) and relations $[e, [e, f]] = 0$, $[[e, f], f] = 0$, $[e, e] = 0$, $[f, f] = 0$. The universal enveloping algebra $U(\mathfrak{sl}(1, 1))$ of $\mathfrak{sl}(1, 1)$ has generators e, f and relations $e^2f - fe^2 = 0$, $ef^2 - f^2e = 0$, $e^2 = 0$, $f^2 = 0$. Thus, $U(\mathfrak{sl}(1, 1))$ is a homomorphic image of the down-up algebra $A(0, 1, 0)$ by the ideal generated by the elements e^2 and f^2, which are central in $A(0, 1, 0)$.

Consider the field $\mathbf{C}(q)$ of rational functions in the indeterminate q over the complex numbers, and let $U_q(\mathfrak{g})$ be the quantized enveloping algebra (quantum group) of a finite-dimensional simple complex Lie algebra $\mathfrak{g}$ corresponding to the Cartan matrix $\mathfrak{A} = (a_{i,j})_{i,j=1}^n$. There are relatively prime integers ℓ_i so that the matrix $(\ell_i a_{i,j})$ is symmetric. Let

$$q_i = q^{\ell_i}, \qquad \text{and} \qquad [m]_i = \frac{q_i^m - q_i^{-m}}{q_i - q_i^{-1}}$$

for all $m \in \mathbf{Z}_{\geq 0}$. When $m \geq 1$, let

$$[m]_i! = \prod_{j=1}^{m} [j]_i.$$

Set $[0]_i! = 1$ and define

$$\begin{bmatrix} m \\ n \end{bmatrix}_i = \frac{[m]_i!}{[n]_i![m-n]_i!}.$$

Then $U = U_q(\mathfrak{g})$ is the unital associative algebra over $\mathbf{C}(q)$ with generators E_i, F_i, K_i, K_i^{-1} $(i = 1, \dots, n)$ subject to the relations

(Q1) $K_iK_i^{-1} = K_i^{-1}K_i, \qquad K_iK_j = K_jK_i$

(Q2) $K_iE_jK_i^{-1} = q_i^{a_{i,j}}E_j$

(Q3) $K_iF_jK_i^{-1} = q_i^{-a_{i,j}}F_j$

(Q4) $E_iF_j - F_jE_i = \delta_{i,j}\dfrac{K_i - K_i^{-1}}{q_i - q_i^{-1}}$

(Q5) $\displaystyle\sum_{k=0}^{1-a_{i,j}} (-1)^k \begin{bmatrix} 1-a_{i,j} \\ k \end{bmatrix}_i E_i^{1-a_{i,j}-k}E_jE_i^k = 0 \qquad \text{for} \quad i \neq j$

(Q6) $\displaystyle\sum_{k=0}^{1-a_{i,j}} (-1)^k \begin{bmatrix} 1-a_{i,j} \\ k \end{bmatrix}_i F_i^{1-a_{i,j}-k}F_jF_i^k = 0 \qquad \text{for} \quad i \neq j.$

Suppose $a_{i,j} = -1 = a_{j,i}$ for some $i \neq j$, and consider the subalgebra $U_{i,j}$ generated by E_i, E_j. In this special case, the quantum Serre relation (Q5) reduces to

$$\begin{aligned} &E_i^2E_j - [2]_iE_iE_jE_i + E_jE_i^2 = 0 \qquad \text{and} \\ &E_j^2E_i - [2]_jE_jE_iE_j + E_iE_j^2 = 0. \end{aligned}$$

Since $-\ell_i = \ell_ia_{i,j} = \ell_ja_{j,i} = -\ell_j$, the coefficients $[2]_i$ and $[2]_j$ are equal. The algebra $U_{i,j}$ (with q is specialized to a complex number which is not a root of unity) is isomorphic to $A([2]_i, -1, 0)$ by the mapping $E_i \mapsto d$, $E_j \mapsto u$. The same result is true if the corresponding F's are used in place of the E's. In particular, when $\mathfrak{g} = \mathfrak{sl}_3$, the algebra $U_{i,j}$ is just the subalgebra of $U_q(\mathfrak{sl}_3)$ generated by the E's.

§2. Witten's Deformations of $U(\mathfrak{sl}_2)$

To provide an explanation of the existence of quantum groups, Witten ([W1], [W2]) introduced a 7-parameter deformation of the universal enveloping algebra $U(\mathfrak{sl}_2)$. Witten's deformation is a unital associative algebra over a field $\mathbf{K}$ (which is algebraically closed of characteristic zero and which could be assumed to be $\mathbf{C}$) and depends on a 7-tuple $\underline{\xi} = (\xi_1, \dots, \xi_7)$ of elements of $\mathbf{K}$. It has a presentation by generators x, y, z and defining relations

$$xz - \xi_1 zx = \xi_2 x \tag{2.1}$$

$$zy - \xi_3 yz = \xi_4 y \tag{2.2}$$

$$yx - \xi_5 xy = \xi_6 z^2 + \xi_7 z. \tag{2.3}$$

We denote the resulting algebra by $\mathfrak{W}(\underline{\xi})$.

Let us assume $\xi_6 = 0$ and $\xi_7 \neq 0$. Then substituting expression (2.3) into (2.1) and (2.2) and rearranging we have

$$
\begin{aligned}
&-\xi_5 x^2 y + (1+\xi_1\xi_5)xyx - \xi_1 yx^2 = \xi_2\xi_7 x \\
&-\xi_5 xy^2 + (1+\xi_3\xi_5)yxy - \xi_3 y^2 x = \xi_4\xi_7 y.
\end{aligned} \tag{2.4}
$$

In particular, when $\xi_5 \neq 0$, $\xi_1 = \xi_3$, and $\xi_2 = \xi_4$ we obtain

$$
\begin{aligned}
x^2y &= \frac{1+\xi_1\xi_5}{\xi_5}xyx - \frac{\xi_1}{\xi_5}yx^2 - \frac{\xi_2\xi_7}{\xi_5}x \\
xy^2 &= \frac{1+\xi_1\xi_5}{\xi_5}yxy - \frac{\xi_1}{\xi_5}y^2x - \frac{\xi_2\xi_7}{\xi_5}y.
\end{aligned}
$$

From this it is easy to see that a Witten deformation algebra $\mathfrak{W}(\underline{\xi})$ with $\xi_6 = 0$, $\xi_5\xi_7 \neq 0$, $\xi_1 = \xi_3$, and $\xi_2 = \xi_4$ is a homomorphic image of the down-up algebra $A(\alpha, \beta, \gamma)$ with

$$
\alpha = \frac{1+\xi_1\xi_5}{\xi_5}, \qquad \beta = -\frac{\xi_1}{\xi_5}, \qquad \gamma = -\frac{\xi_2\xi_7}{\xi_5}. \tag{2.5}
$$

This is the initial step of the proof of the following result.

THEOREM 2.6. *A Witten deformation algebra $\mathfrak{W}(\underline{\xi})$ with*

$$
\xi_6 = 0, \ \ \xi_5\xi_7 \neq 0, \ \xi_1 = \xi_3, \ \ \textit{and} \ \ \xi_2 = \xi_4 \tag{2.7}
$$

is isomorphic to the down-up algebra $A(\alpha, \beta, \gamma)$ with α, β, γ given by (2.5). Conversely, any down-up algebra $A(\alpha, \beta, \gamma)$ with not both α and β equal to 0 is isomorphic to a Witten deformation algebra $\mathfrak{W}(\underline{\xi})$ whose parameters satisfy (2.7).

PROOF. Observe first that any deformation algebra $\mathfrak{W}(\underline{\xi})$ with $\xi_6 = 0$ and $\xi_7 \neq 0$ is isomorphic to the algebra $\mathfrak{W}'(\underline{\xi})$, which has generators x, y and defining relations

$$
\begin{aligned}
&-\xi_5 x^2 y + (1+\xi_1\xi_5)xyx - \xi_1 yx^2 = \xi_2\xi_7 x \\
&-\xi_5 xy^2 + (1+\xi_3\xi_5)yxy - \xi_3 y^2 x = \xi_4\xi_7 y.
\end{aligned} \tag{2.8}
$$

When $\xi_6 = 0$ and $\xi_7 \neq 0$ we will identify these two algebras.

We have argued above that a deformation algebra $\mathfrak{W}(\underline{\xi})$ whose parameters satisfy (2.7) is a homomorphic image of $A(\alpha, \beta, \gamma)$ for α, β, γ given by (2.5) via the map that sends d to x and u to y. Now consider the map $\mathbf{K}\langle x, y\rangle \to A(\alpha, \beta, \gamma)$ from the free associative algebra $\mathbf{K}\langle x, y\rangle$ generated by x, y to the down-up algebra $A(\alpha, \beta, \gamma)$ (with α, β, γ as in (2.5)) given by $x \mapsto d$ and $y \mapsto u$. By (2.8), the elements

$$
\begin{aligned}
x^2y &- \frac{1+\xi_1\xi_5}{\xi_5}xyx + \frac{\xi_1}{\xi_5}yx^2 + \frac{\xi_2\xi_7}{\xi_5}x \\
xy^2 &- \frac{1+\xi_1\xi_5}{\xi_5}yxy + \frac{\xi_1}{\xi_5}y^2x + \frac{\xi_2\xi_7}{\xi_5}y
\end{aligned}
$$

are in the kernel, and so there is an induced homomorphism $\mathfrak{W}(\underline{\xi}) \to A(\alpha, \beta, \gamma)$. Thus, the two algebras can be seen to be isomorphic. Observe that $\xi_1 \neq 0$ if and only if $\beta \neq 0$. If $\xi_1 = 0$ then $\alpha = \xi_5^{-1} \neq 0$, so either α or β is nonzero for the down-up algebras that are obtained.

Conversely, consider an arbitrary down-up algebra $A(\alpha, \beta, \gamma)$ with not both α and β equal to 0. Suppose first $\beta \neq 0$, and let ξ_1 be a solution to $\xi_1^2 - \alpha\xi_1 - \beta = 0$. Set

$$\begin{gathered} \xi_3 = \xi_1, \quad \xi_6 = 0, \quad 0 \neq \xi_7 \in \mathbf{K} \quad \text{(arbitrary)} \\ \xi_5 = \frac{1}{\alpha - \xi_1}, \quad \xi_2 = \xi_4 = -\frac{\gamma\xi_5}{\xi_7}. \end{gathered} \tag{2.9}$$

(Note that $\beta \neq 0$ implies $\alpha \neq \xi_1$.) The relations in (2.9) imply the ones in (2.5). Consequently, if $\underline{\xi} = (\xi_1, \dots, \xi_7)$ where the parameters satisfy (2.9), then $\mathfrak{W}(\underline{\xi}) \cong A(\alpha, \beta, \gamma)$ where α, β, γ are as in (2.5).

Finally suppose for the down-up algebra $A(\alpha, \beta, \gamma)$ that $\beta = 0$ and $\alpha \neq 0$. Set $\xi_1 = \xi_3 = 0$, and define the remainder of the parameters in $\underline{\xi} = (\xi_1, \dots, \xi_7)$ as in (2.9). The corresponding deformation algebra $\mathfrak{W}(\underline{\xi})$ is isomorphic to $A(\alpha, 0, \gamma)$. $\square$

A deformation algebra $\mathfrak{W}(\underline{\xi})$ has a filtration, and Le Bruyn ([L1], [L2]) investigated the algebras $\mathfrak{W}(\underline{\xi})$ whose associated graded algebras are Auslander regular. They determine a 3-parameter family of deformation algebras which are called *conformal $\mathfrak{sl}_2$ algebras* and whose defining relations are

$$\begin{aligned} xz - azx &= x \\ zy - ayz &= y \\ yx - cxy &= bz^2 + z \end{aligned} \tag{2.10}$$

When $c \neq 0$ and $b = 0$, the conformal $\mathfrak{sl}_2$ algebra with defining relations given by (2.10) is isomorphic to the down-up algebra $A(\alpha, \beta, \gamma)$ with $\alpha = c^{-1}(1 + ac), \beta = -ac^{-1}$ and $\gamma = -c^{-1}$. If $c = b = 0$ and $a \neq 0$, then the conformal $\mathfrak{sl}_2$ algebra is isomorphic to the down-up algebra $A(\alpha, \beta, \gamma)$ with $\alpha = a^{-1}$, $\beta = 0$ and $\gamma = -a^{-1}$.

In a recent paper Kulkarni [K] has shown that under certain assumptions on the parameters, a Witten deformation algebra is isomorphic to a conformal $\mathfrak{sl}_2$ algebra or to a double skew polynomial extension. The precise statement of the result is

THEOREM 2.11. *([K, Thm. 3.0.3]) If $\xi_1\xi_3\xi_5\xi_2 \neq 0$ or $\xi_1\xi_3\xi_5\xi_4 \neq 0$, then $\mathfrak{W}(\underline{\xi})$ is isomorphic to one of the following algebras:*

(a) *A conformal $\mathfrak{sl}_2$ algebra with generators x, y, z and relations given by (2.10) for some $a, b, c \in \mathbf{K}$.*

(b) *A double skew polynomial extension (that is, a skew polynomial extension of a skew polynomial ring) whose generators satisfy*

(i) $xz - zx = x, \quad zy - yz = \zeta y, \quad yx - \eta xy = 0$ *or*

(ii) $xw = \theta wx, \quad wy = \kappa yw, \quad yx = \lambda xy$
for parameters $\zeta, \eta, \theta, \kappa, \lambda \in \mathbf{K}$.

Kulkarni studies the simple representations of the conformal sl_2 algebras and of the skew polynomial algebras in (b). Essential to the investigations in [K] is the observation that the conformal $\mathfrak{sl}_2$ algebra of (2.10) can be realized as a *hyperbolic ring* $R\{\phi, \tau\}$, where R is the polynomial ring $\mathbf{K}[z, \tau]$ and ϕ is the automorphism of R sending $f(z,\tau)$ to $f(az+1, c^{-1}(\tau - t(az+1)))$, where $t = bz^2 + z$. Kulkarni then applies results of Rosenberg [R] to describe the left ideals in the left spectrum of $R\{\phi,\tau\}$ and to determine the maximal left ideals for the conformal sl_2 algebras. Further applications of results of [R] give the left spectrum of the double skew polynomial extensions in (b) of Theorem 2.11.

§3. Representations of down-up algebras

Down-up algebras have a rich representation theory. In this section we construct highest weight modules for $A(\alpha,\beta,\gamma)$ and discuss more general weight modules. Further details of the results can be found in [BR, Sec. 2].

Highest weight modules.

A module V for $A = A(\alpha,\beta,\gamma)$ is said to be a *highest weight module of weight* λ if V has a vector y_0 such that $d \cdot y_0 = 0$, $(du)\cdot y_0 = \lambda y_0$, and $V = Ay_0$. The vector y_0 is a *maximal vector* or *highest weight vector* of V.

PROPOSITION 3.1. *(See [BR, Sec. 2]) Set $\lambda_{-1} = 0$ and let $\lambda_0 = \lambda \in \mathbf{C}$ be arbitrary. For $n \geq 1$, define λ_n inductively by the recurrence relation,*

$$\lambda_n = \alpha\lambda_{n-1} + \beta\lambda_{n-2} + \gamma. \tag{3.2}$$

The $\mathbf{C}$-vector space $V(\lambda)$ with basis $\{v_n \mid n = 0,1,2,\dots\}$ and with $A(\alpha,\beta,\gamma)$-action given by

$$\begin{aligned} d \cdot v_n &= \lambda_{n-1}v_{n-1}, \quad n \geq 1, \quad \text{and} \quad d\cdot v_0 = 0 \\ u \cdot v_n &= v_{n+1}. \end{aligned} \tag{3.3}$$

is a highest weight module for $A(\alpha,\beta,\gamma)$. Every $A(\alpha,\beta,\gamma)$-module of highest weight λ is a homomorphic image of $V(\lambda)$.

Because it shares the same universal property and many of the same features as Verma modules for finite-dimensional semisimple complex Lie algebras, the module $V(\lambda)$ is said to be the *Verma module* for $A(\alpha,\beta,\gamma)$.

PROPOSITION 3.4.

(a) *$V(\lambda)$ is simple if and only if $\lambda_n \neq 0$ for any n.*

(b) *If m is minimal with the property that $\lambda_m = 0$, then $M(\lambda) = \mathrm{span}_{\mathbf{C}}\{v_j \mid j \geq m+1\}$ is a maximal submodule of $V(\lambda)$.*

(c) *Suppose N is a submodule of $V(\lambda)$ such that $N \subseteq \mathrm{span}_{\mathbf{C}}\{v_j \mid j \geq 1\}$. Then $N \subseteq M(\lambda)$.*

When $V(\lambda)$ is simple, we set $M(\lambda) = (0)$.

Weight modules.

If we multiply the relation $d^2u - \alpha dud - \beta ud^2 = \gamma d$ on the left by u and the relation $du^2 - \alpha udu - \beta u^2 d = \gamma u$ on the right by d and subtract the second from the first, the resulting equation is

$$0 = ud^2u - du^2d \qquad \text{or} \qquad (du)(ud) = (ud)(du). \tag{3.5}$$

Therefore, the elements du and ud commute in $A = A(\alpha, \beta, \gamma)$. For any basis element $v_n \in V(\lambda)$, we have $du \cdot v_n = \lambda_n v_n$ and $ud \cdot v_n = \lambda_{n-1} v_n$. Using that with $n = 0$ and $\lambda \neq 0$, it is easy to see that du and ud are linearly independent. Let $\mathfrak{h} = \mathbf{C}du \oplus \mathbf{C}ud$.

We say an A-module V is a *weight module* if $V = \sum_{\nu \in \mathfrak{h}^*} V_\nu$, where $V_\nu = \{v \in V \mid h \cdot v = \nu(h)v \text{ for all } h \in \mathfrak{h}\}$, and the sum is over elements in the dual space $\mathfrak{h}^*$ of $\mathfrak{h}$ (necessarily the sum is direct). Any submodule of a weight module is a weight module. If $V_\nu \neq (0)$, then ν is a *weight* and V_ν is the corresponding *weight space.* Each weight ν is determined by the pair (ν', ν'') of complex numbers, $\nu' = \nu(du)$ and $\nu'' = \nu(ud)$, and often it is convenient to identify ν with (ν', ν''). In particular, highest weight modules are weight modules in this sense. The basis vector v_n of $V(\lambda)$ is a weight vector whose weight is given by the pair $(\lambda_n, \lambda_{n-1})$. Finding these weights explicitly involves solving the linear recurrence relation in (3.3), which can be done by standard methods as in [Br, Chap.7] for example.

PROPOSITION 3.6. *Assume $\lambda_{-1} = 0$, $\lambda_0 = \lambda$, and λ_n for $n \geq 1$ is given by the recurrence relation $\lambda_n - \alpha\lambda_{n-1} - \beta\lambda_{n-2} = \gamma$. Fix $t \in \mathbf{C}$ such that*

$$t^2 = \frac{\alpha^2 + 4\beta}{4}.$$

(i) *If $\alpha^2 + 4\beta \neq 0$, then*

$$\lambda_n = c_1 r_1^n + c_2 r_2^n + x_n,$$

where

$$r_1 = \frac{\alpha}{2} + t, \qquad r_2 = \frac{\alpha}{2} - t,$$
$$x_n = \begin{cases} (1-\alpha-\beta)^{-1}\gamma & \text{if} \quad \alpha+\beta \neq 1 \\ (2-\alpha)^{-1}\gamma n & \text{if} \quad \alpha+\beta = 1 \quad (\text{necessarily} \quad \alpha \neq 2), \end{cases}$$
$$\text{and} \qquad \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \frac{1}{r_2 - r_1} \begin{pmatrix} r_2 & -1 \\ -r_1 & 1 \end{pmatrix} \begin{pmatrix} \lambda - x_0 \\ \alpha\lambda + \gamma - x_1 \end{pmatrix}.$$

(ii) *If $\alpha^2 + 4\beta = 0$ and $\alpha \neq 0$, then*

$$\lambda_n = c_1 s^n + c_2 n s^n + x_n \quad \text{where}$$

$$s = \frac{\alpha}{2}$$

$$x_n = \begin{cases} (1-\alpha-\beta)^{-1}\gamma & \textit{if} \quad \alpha+\beta \neq 1 \\ 2^{-1}n^2\gamma & \textit{if} \quad \alpha+\beta = 1 \quad \textit{i.e.} \quad \textit{if} \quad \alpha = 2,\ \beta = -1, \end{cases}$$

and $$\begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -1 & 2\alpha^{-1} \end{pmatrix} \begin{pmatrix} \lambda - x_0 \\ \alpha\lambda + \gamma - x_1 \end{pmatrix}.$$

(iii) *If* $\alpha^2 + 4\beta = 0$ *and* $\alpha = 0$, *then* $\beta = 0$ *and* $\lambda_n = \gamma$ *for all* $n \geq 1$.

If α, β are real, then it is natural to take $t = \dfrac{\sqrt{\alpha^2+4\beta}}{2}$ in the above calculations.

Let us consider several special cases.

EXAMPLE (I). Recall that the universal enveloping algebra $U(\mathfrak{sl}_2)$ of $\mathfrak{sl}_2$ is isomorphic to the algebra $A(2,-1,-2)$, and the universal enveloping algebra $U(\mathfrak{H})$ of the Heisenberg Lie algebra $\mathfrak{H}$ is isomorphic to $A(2,-1,0)$. For any algebra $A(2,-1,\gamma)$, applying (ii) with $s = \alpha/2 = 1$ and $x_n = n^2\gamma/2$ we have that

$$\lambda_n = c_1 + c_2 n + \frac{n^2\gamma}{2}, \qquad \text{where}$$

$$\begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} \lambda \\ 2\lambda + \frac{\gamma}{2} \end{pmatrix} = \begin{pmatrix} \lambda \\ \lambda + \frac{\gamma}{2} \end{pmatrix}.$$

Therefore

$$\begin{aligned} \lambda_n &= \lambda + (\lambda + \frac{\gamma}{2})n + \frac{\gamma n^2}{2} \\ &= (n+1)(\lambda + \frac{\gamma n}{2}). \end{aligned}$$

In the $\mathfrak{sl}_2$-case, the operator $h = du - ud$ is used rather than du. The eigenvalues of h are $\lambda_n - \lambda_{n-1} = \lambda + n\gamma = \lambda - 2n$, $n = 0, 1, \ldots,$ (as is customary in the representation theory of $\mathfrak{sl}_2$), and $V(\lambda)$ is simple if and only if $\lambda \notin \mathbf{Z}_{\geq 0}$. The analogous computation in the Heisenberg Lie algebra shows that the central element $z = du - ud$ has constant eigenvalue $\lambda_n = \lambda$.

EXAMPLE (II). Recall that the quantum case discussed in Sec. 1 involves the down-up algebra $A([2]_i, -1, 0)$. To compute the values of λ_n in this case, we adopt the shorthand

$$p = q_i,$$

and note that $\alpha = [2]_i = \dfrac{p^2 - p^{-2}}{p - p^{-1}} = p + p^{-1}$, $\beta = -1$, and $\gamma = 0$ so that

$$\alpha^2 + 4\beta = p^2 + 2 + p^{-2} - 4 = (p - p^{-1})^2.$$

Thus

$$r_1 = \frac{p+p^{-1}+p-p^{-1}}{2} = p$$
$$r_2 = \frac{p+p^{-1}-(p-p^{-1})}{2} = p^{-1},$$
$$\begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \frac{1}{p^{-1}-p}\begin{pmatrix} p^{-1} & -1 \\ -p & 1 \end{pmatrix}\begin{pmatrix} \lambda \\ (p+p^{-1})\lambda \end{pmatrix}$$
$$= \frac{1}{p^{-1}-p}\begin{pmatrix} -p\lambda \\ p^{-1}\lambda \end{pmatrix} = \frac{1}{p-p^{-1}}\begin{pmatrix} p\lambda \\ -p^{-1}\lambda \end{pmatrix}.$$

Therefore

$$\begin{aligned}\lambda_n &= \frac{p\lambda}{p-p^{-1}}p^n - \frac{p^{-1}\lambda}{p-p^{-1}}p^{-n} \\ &= \Big(\frac{p^{n+1}-p^{-(n+1)}}{p-p^{-1}}\Big)\lambda \\ &= [n+1]_i\lambda.\end{aligned}$$

In the particular case of $U_q(\mathfrak{sl}_3)$, the subalgebra generated by the E_i's is isomorphic to $A([2],-1,0)$ where $[2] = \dfrac{q^2-q^{-2}}{q-q^{-1}}$, and $\lambda_n = [n+1]\lambda = \Big(\dfrac{q^{n+1}-q^{-(n+1)}}{q-q^{-1}}\Big)\lambda$ in that case.

Example (iii). For the algebra $A(1,1,0)$, the solutions to the associated linear recurrence $\lambda_n = \lambda_{n-1}+\lambda_{n-2}$, $\lambda_0 = \lambda$, $\lambda_{-1} = 0$, (hence the eigenvalues of du and ud on $V(\lambda)$) are given by the Fibonacci sequence $\lambda_0 = \lambda$, $\lambda_1 = \lambda$, $\lambda_2 = 2\lambda$, $\lambda_3 = 3\lambda$, $\lambda_4 = 5\lambda$, ... In this case, the equations in Proposition 3.6 reduce to

$$\lambda_n = \lambda\frac{\sqrt{5}}{5}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}\right).$$

Example (iv). When $\beta = 0$, we may assume $t = \alpha/2$ so that $r_1 = \alpha$ and $r_2 = 0$. Solving for λ_n from Proposition 3.6 we obtain

$$\lambda_n = \begin{cases} \Big(\lambda - \dfrac{\gamma}{1-\alpha}\Big)\alpha^n + \dfrac{\gamma}{1-\alpha} & \text{if} \quad \alpha \neq 1 \\ \lambda + \gamma n \quad \text{if} \quad \alpha = 1. \end{cases}$$

Weights and submodules.

In [BR] we investigated in detail the weight space and submodule structure of the Verma module $V(\lambda)$. Roots of unity play a critical role in determining the dimension of a weight space. For example if $\beta = 0$, it is easy to see from the expressions in Example (iv) that weight spaces are either 1-dimensional or infinite-dimensional. (The latter occurs when $\alpha \neq 1$ and $\lambda = \gamma/(1-\alpha)$ or α is a root of unity, or when $\alpha = 1$ and $\gamma = 0$). This dichotomy is a general phenomenon. We briefly summarize some of the main results.

PROPOSITION 3.7.

(a) *In* $V(\lambda)$ *each weight space is either one-dimensional or infinite-dimensional. If an infinite-dimensional weight space occurs, there are only finitely many weights.*

(b) *If each weight space of* $V(\lambda)$ *is one-dimensional, then the proper submodules of* $V(\lambda)$ *have the form* $N = span_{\mathbf{C}}\{v_j \mid j \geq n\}$ *for some* $n > 0$ *with* $\lambda_{n-1} = 0$*, and hence they are contained in* $M(\lambda)$*.*

(c) *If* $\gamma = 0 = \lambda$*, then* $V(\lambda)$ *has infinitely many maximal proper submodules, each of the form* $N^{(\tau)} = span_{\mathbf{C}}\{v_n - \tau v_{n-1} \mid n = 1, 2, \dots\}$ *for some* $\tau \in \mathbf{C}$*, and infinitely many one-dimensional simple quotients,* $L(0, \tau) = V(0)/N^{(\tau)}$*. In all other cases,* $M(\lambda)$ *is the unique maximal submodule of* $V(\lambda)$*, and there is a unique simple highest weight module,* $L(\lambda) = V(\lambda)/M(\lambda)$*, of weight* λ *up to isomorphism.*

In a weight module the weight spaces are translated by the operators d and u. If $m \in M$ is a vector of weight $\nu = (\nu', \nu'')$, where $\nu' = \nu(du)$ and $\nu'' = \nu(ud)$, in an $A(\alpha, \beta, \gamma)$-module M, then

(i) $u \cdot m$ has weight

$$\begin{aligned} &\mu(\nu) = (\mu(\nu)', \mu(\nu)'') \qquad \text{where} \\ &\mu(\nu)' = \alpha\nu' + \beta\nu'' + \gamma \qquad \text{and} \qquad \mu(\nu)'' = \nu', \quad \text{and} \end{aligned} \tag{3.8}$$

(ii) when $\beta \neq 0$, $d \cdot m$ has weight

$$\begin{aligned} &\delta(\nu) = (\delta(\nu)', \delta(\nu)'') \qquad \text{where} \\ &\delta(\nu)' = \nu'' \qquad \text{and} \qquad \delta(\nu)'' = \beta^{-1}(\nu' - \alpha\nu'' - \gamma), \end{aligned} \tag{3.9}$$

An easy direct computation shows that $\delta(\mu(\nu)) = \nu$ and $\mu(\delta(\nu)) = \nu$.

Starting with $\nu_0 = (\lambda, 0)$ for $\lambda \in \mathbf{C}$, and defining ν_n inductively by $\nu_n = \mu(\nu_{n-1}) = \mu^n(\nu_0)$, we have $\nu_n = (\lambda_n, \lambda_{n-1})$, where λ_n is as in (3.2). Thus the set $\{\nu_0, \nu_1, \dots\}$ is just the set of weights of the Verma module $V(\lambda)$.

Lowest weight modules.

Lowest weight modules W for $A = A(\alpha, \beta, \gamma)$ can be created by reversing the roles of d and u. Thus, there is a vector w_0 such that $u \cdot w_0 = 0$, $ud \cdot w_0 = \kappa w_0$, and $W = Aw_0$. When $\beta \neq 0$, the eigenvalues of du are given by the sequence which has $\kappa_{-1} = 0$, $\kappa_0 = \kappa$, an arbitrary complex number, and

$$\begin{aligned} &\beta\kappa_n + \alpha\kappa_{n-1} - \kappa_{n-2} = -\gamma, \quad \text{or equivalently} \\ &\kappa_n = \beta^{-1}\big(- \alpha\kappa_{n-1} + \kappa_{n-2} - \gamma\big) \end{aligned} \tag{3.10}$$

for all $n \geq 1$.

PROPOSITION 3.11. *Let $W(\kappa)$ be the* $\mathbf{C}$*-vector space having basis* $\{w_n \mid n = 0, 1, 2, \dots\}$.

(a) *Assume $\beta \neq 0$, $\kappa_{-1} = 0$, and $\kappa_0 = \kappa$, an arbitrary element of* $\mathbf{C}$. *Suppose κ_n for $n \geq 1$ is as in (3.10), and define*

$$\begin{aligned} u \cdot w_n &= \kappa_{n-1} w_{n-1}, \quad n \geq 1, \quad \textit{and} \quad u \cdot w_0 = 0 \\ d \cdot w_n &= w_{n+1}. \end{aligned} \tag{3.12}$$

Then this action gives $W(\kappa)$ the structure of a lowest weight $A(\alpha, \beta, \gamma)$-module.

(b) *When $\beta = 0$ and $\alpha \neq 0$, set*

$$\kappa_n = -\gamma \sum_{j=1}^{n+1} \alpha^{-j}$$

for all $n \geq 0$. Then $W(-\gamma\alpha^{-1})$ with the action given by (3.12) is a lowest weight $A(\alpha, \beta, \gamma)$-module.

(c) *When $\gamma \neq 0$, the only lowest weight $A(0, 0, \gamma)$-module is the 1-dimensional module $W = \mathbf{C}w_0$ with $d \cdot w_0 = 0 = u \cdot w_0$. When $\gamma = 0$, set $\kappa_n = 0$ for all n. Then $W(0)$ with the action given by (3.12) is a lowest weight $A(0, 0, 0)$-module.*

When $\beta \neq 0$, the set of weights of the lowest weight module $W(\kappa)$ is just $\{\delta^n(\omega) \mid n = 0, 1, \dots\}$, where $\omega = (0, \kappa)$.

Category $\mathcal{O}$ modules.

Bernstein, Gelfand, and Gelfand [BGG] introduced an important category of weight modules for finite-dimensional complex semisimple Lie algebras, the so-called category $\mathcal{O}$ modules. There is analogous category that can be defined for a down-up algebra $A = A(\alpha, \beta, \gamma)$.

(3.13) The category $\mathcal{O}$ consists of all A-modules M satisfying the following conditions:

(a) M is a weight module relative to $\mathfrak{h} = \mathrm{span}_{\mathbf{C}}\{du, ud\}$, i.e. $M = \sum_\nu M_\nu$ where $M_\nu = \{m \in M \mid h \cdot m = \nu(h)m \text{ for all } h \in \mathfrak{h}\}$;

(b) d acts locally nilpotently on M, so that for each $m \in M$, $d^n m = 0$ for some n.

(c) M is a finitely generated A-module.

The category $\mathcal{O}$ is closed under taking submodules and quotients. It contains all the Verma modules $V(\lambda)$ and their simple quotient modules $L(\lambda) = V(\lambda)/M(\lambda)$ (and in the case that $\gamma = 0$ and $\lambda = 0$, the one-dimensional quotients $L(0, \tau) = V(0)/N^{(\tau)}$).

PROPOSITION 3.14. *Suppose $\beta \neq 0$. If M is an simple object in the category $\mathcal{O}$, then either $M \cong L(\lambda)$ for some λ, or else $\gamma = 0$ and $M \cong V(0)/N^{(\tau)} = L(0,\tau)$ for some $\tau \in \mathbf{C}$.*

There is more general category of modules that can be defined for the down-up algebra $A = A(\alpha,\beta,\gamma)$. *Here we require that $\beta \neq 0$.*

(3.15) The category $\mathcal{O}'$ consists of all A-modules M satisfying the following conditions:

(a) M is a weight module relative to $\mathfrak{h} = \mathrm{span}_{\mathbf{C}}\{du, ud\}$.
(b) $\mathbf{C}[d]m$ is finite-dimensional for each $m \in M$.
(c) M is a finitely generated A-module.

The modules in $\mathcal{O}$ clearly belong to $\mathcal{O}'$, but $\mathcal{O}'$ is larger than $\mathcal{O}$ which can be seen from examining the simple modules in $\mathcal{O}'$.

PROPOSITION 3.16. *Suppose F is a set of weights such that $\delta(\omega)$, $\mu(\omega) \in F$ whenever $\omega \in F$. Suppose $\rho \in \mathbf{C}$ is nonzero, and let $N(F,\rho)$ be the $\mathbf{C}$-vector space with basis $\{v_\omega \mid \omega \in F\}$.*

(a) *Define*

$$\begin{aligned} d \cdot v_\omega &= \rho v_{\delta(\omega)} \\ u \cdot v_\omega &= \rho^{-1}\mu(\omega)'' v_{\mu(\omega)}. \end{aligned}$$

Then this action extends to give an $A(\alpha,\beta,\gamma)$-module action on $N(F,\rho)$.

(b) *If F is generated by any weight $\nu = (\nu', \nu'') \in F$ under the action of δ, and if $\nu' \neq 0$ for any $\nu \in F$, then $N(F,\rho)$ is a simple $A(\alpha,\beta,\gamma)$-module.*

THEOREM 3.17. *Assume M is a simple module in the category $\mathcal{O}'$. Then there are three possibilities:*

(a) *M is a highest weight module, that is, M is isomorphic to $L(\lambda)$ for some λ or to $L(0,\tau)$ for some $\tau \in \mathbf{C}$ (when $\gamma = 0$).*

(b) *M is a finite-dimensional lowest weight module with weights $\nu, \delta(\nu), \ldots, \delta^{n-1}(\nu)$ such that $\delta^n(\nu) = \nu$ for some $n \geq 1$.*

(c) *M is isomorphic to $N(F,\rho)$ for some $\rho \neq 0$ and some finite set $F = \{\nu, \delta(\nu), \ldots, \delta^{n-1}(\nu)\}$ such that $\delta^n(\nu) = \nu$ for some $n \geq 1$.*

§4. The structure of down-up algebras

It is apparent from the defining relations that the monomials $u^i(du)^j d^k$, $i,j,k = 0,1,\ldots$ in a down-up algebra $A = A(\alpha,\beta,\gamma)$ determine a spanning set. In [BR, Thm. 3.1] we apply the Diamond Lemma (see [Be]) to prove a Poincaré-Birkhoff-Witt type result for down-up algebras. There is one essential ambiguity, $(d^2u)u = d(du^2)$, and the result of resolving the ambiguity in the two possible ways is the same. Arguing in this manner we prove

THEOREM 4.1. *(Poincaré-Birkhoff-Witt Theorem) Assume $A = A(\alpha, \beta, \gamma)$ is a down-up algebra over* $\mathbf{C}$. *Then $\{u^i(du)^j d^k \mid i, j, k = 0, 1, \dots\}$ is a basis of A.*

The Gelfand-Kirillov dimension is a natural dimension to assign to an algebra A, and many cases (such as when A is a domain), it provides important structural information (see for example, [AS]). Theorem 4.1 enables us to compute the GK-dimension of any down-up algebra $A = A(\alpha, \beta, \gamma)$. The spaces $A^{(n)} = \mathrm{span}_{\mathbf{C}}\{u^i(du)^j d^k \mid i + 2j + k \leq n\}$ afford a filtration $(0) \subset A^{(0)} \subset A^{(1)} \subset \cdots \subset \cup_n A^{(n)} = A(\alpha, \beta, \gamma)$ of the down-up algebra, and $A^{(m)}A^{(n)} \subseteq A^{(m+n)}$ since the defining relations replace the words d^2u and du^2 by words of the same or lower total degree. The number of monomials $u^i(du)^j d^k$ with $i+2j+k = \ell$ is $(m+1)(m+1)$ if $\ell = 2m$ and is $(m+1)(m+2)$ if $\ell = 2m+1$. Thus, $\dim A^{(n)}$ is a polynomial in n with positive coefficients of degree 3, and the Gelfand-Kirillov dimension is given by

$$
\begin{aligned}
\mathrm{GKdim}\big(A(\alpha, \beta, \gamma)\big) &= \limsup_{n\to\infty} \log_n(\dim A^{(n)}) \\
&= \lim_{n\to\infty} \frac{\ln\left(\dim A^{(n)}\right)}{\ln n} \qquad (4.2)\\
&= 3.
\end{aligned}
$$

In [BR, Sec. 3] we show

PROPOSITION 4.3. *If $A(\alpha, \beta, \gamma)$ has infinitely many simple Verma modules $V(\lambda)$, then the intersection of the annihilators of the simple Verma modules is zero.*

As an immediate consequence, for such a down-up algebra $A(\alpha, \beta, \gamma)$ the Jacobson radical, which is the intersection of the annihilators of all the simple modules, is zero.

Conditions for $A(\alpha, \beta, \gamma)$ to have infinitely many simple Verma modules are (4.4)

(1) $\alpha^2 + 4\beta \neq 0$ and $\alpha^2 \neq -4\beta\cos^2(\theta/2)$ where $e^{i\theta}$ is a root of unity, or

(2) $\alpha^2 + 4\beta = 0$ and $\alpha \neq 0$ or

(3) $\alpha = 0 = \beta$ and $\gamma \neq 0$.

Gradation and the center.

The free associative algebra over $\mathbf{C}$ generated by d and u can be graded by assigning $\deg(d) = -1$ and $\deg(u) = 1$ and extending this by using $\deg(ab) = \deg(a) + \deg(b)$. The relations $d^2u = \alpha dud + \beta ud^2 + \gamma d$ and $du^2 = \alpha udu + \beta u^2 d + \gamma u$ are homogeneous, so the down-up algebra $A = A(\alpha, \beta, \gamma)$ inherits the grading and decomposes into homogeneous components $A = \bigoplus_{n\in\mathbf{Z}} A_n$. In [BR, Sec. 3] we show that the subalgebra $A_0 = \mathrm{span}_{\mathbf{C}}\{u^i(du)^j d^i \mid i, j = 0, 1, \dots\}$ is commutative.

PROPOSITION 4.5. *Assume A has infinitely many simple Verma modules. Let $A = \bigoplus_{j\in\mathbf{Z}} A_j$ be the $\mathbf{Z}$-grading of $A = A(\alpha,\beta,\gamma)$. Then:*

(a) *The center $Z(A)$ of A is contained in $A_0 = span_{\mathbf{C}}\{u^i(du)^j d^i \mid i,j = 0,1,\ldots\}$.*

(b) *Suppose $z \in Z(A)$ and $V(\lambda)$ is any Verma module of A. Then z acts as a scalar, say $\chi_\lambda(z)$, on $V(\lambda)$. The mapping $\chi_\lambda : Z(A) \to \mathbf{C}$ is an algebra homomorphism.*

(c) *A scalar $\pi \in \mathbf{C}$ is* **linked** *to λ if $\pi = \lambda_{n+1}$ for some $n \geq 0$ with $\lambda_n = 0$, where the sequence $\lambda_1, \lambda_2, \ldots$ is constructed using the recurrence relation in (3.2) starting with $\lambda_{-1} = 0$ and $\lambda_0 = \lambda$. If π is linked to λ, then $\chi_\pi = \chi_\lambda$.*

Open Problems.* We conclude by mentioning several open questions concerning down-up algebras.

(a) The down-up algebras $A(2,-1,\gamma)$ are Noetherian because they are universal enveloping algebras of finite-dimensional Lie algebras. Determine when $A(\alpha,\beta,\gamma)$ is Noetherian.

(b) Determine conditions on α,β,γ for $A(\alpha,\beta,\gamma)$ to be a domain. When $\beta = 0$, then $d(du - \alpha ud - \gamma 1) = 0$ so that $A(\alpha,\beta,\gamma)$ has zero divisors for any choice of $\alpha,\gamma \in \mathbf{C}$. The universal enveloping algebra examples $A(2,-1,\gamma)$, as well as the quantum examples $A([2]_i,-1,0)$, show that some down-up algebras are domains.

(c) What is the center of $A(\alpha,\beta,\gamma)$? The center can be nontrivial as the enveloping algebra examples $A(2,-1,\gamma)$ show. The down-up algebra $A(0,1,0)$ has the elements d^2 and u^2 in its center.

(d) When is $A(\alpha,\beta,\gamma)$ a Hopf algebra?

(e) Relate Kulkarni's presentation of the maximal left ideals in conformal $\mathfrak{sl}_2$ algebras to the simple modules in category $\mathcal{O}$ and category $\mathcal{O}'$. The approach in [K] using noncommutative algebraic geometry is quite different from the one in [BR] and so is the description of the simple modules.

(f) Study the homogenization $A[t]$ of the down-up algebra $A = A(\alpha,\beta,\gamma)$, which is the graded algebra generated by d,u,t subject to the relations

$$d^2u = \alpha dud + \beta ud^2 + \gamma dt^2, \quad du^2 = \alpha udu + \beta u^2d + \gamma ut^2,$$
$$dt = td, \quad ut = tu.$$

Homogenized $\mathfrak{sl}_2$ is a positively graded Noetherian domain and a maximal order, which is Auslander-regular of dimension 4 and satisfies the Cohen-Macaulay property. Le Bruyn and Smith [LS] have determined the point, line, and plane modules of homogenized $\mathfrak{sl}_2$ and shown the line modules are homogenizations of the Verma modules.

References

[AS] M. Artin and J.T. Stafford, *Noncommutative graded domains with quadratic growth*, Invent. Math. **122** (1995), 231–276.

[BR] G. Benkart and T. Roby, *Down-up algebras* (to appear).

[Be] G.M. Bergman, *The diamond lemma for ring theory*, Adv. in Math. **29** (1978), 178–218.

[BGG] J. Bernstein, I.M. Gelfand, and S.I. Gelfand, *A category of $\mathfrak{g}$-modules*, Func. Anal. Appl. **10** (1976), 87–92.

[Br] R.A. Brualdi, *Introductory Combinatorics*, Second Edition, North Holland, New York, 1992.

[F] S.V. Fomin, *Duality of graded graphs*, J. Alg. Comb. **3** (1994), 357–404.

[K] R. Kulkarni, *Irreducible representations of Witten's deformations of $U(sl_2)$* (to appear).

[L1] L. Le Bruyn, *Two remarks on Witten's quantum enveloping algebra*, Comm. Algebra **22** (1994), 865–876.

[L2] L. Le Bruyn, *Conformal $\mathfrak{sl}_2$ enveloping algebras*, Comm. Algebra **23** (1995), 1325–1362.

[LS] L. Le Bruyn and S.P. Smith, *Homogenized $\mathfrak{sl}_2$*, Proc. Amer. Math. Soc. **118** (1993), 725–730.

[M] Yu. Manin, *Some remarks on Koszul algebras and quantum groups*, Ann. Inst. Fourier **37** (1987), 191–205.

[R] A.L. Rosenberg, *Noncommutative Algebraic Geometry and Representations of Quantized Algebras*, Kluwer, 1995.

[Sm] S.P. Smith, *A class of algebras similar to the enveloping algebra of $sl(2)$*, Trans. Amer. Math. Soc. **322** (1990), 285–314.

[St] R.P. Stanley, *Differential posets*, J. of Amer. Math. Soc. **4** (1988), 919–961.

[T] P. Terwilliger, *The incidence algebra of a uniform poset*, 193-212; *Coding Theory and Design Theory, Part I*, D. Ray-Chaudhuri, ed., IMA Series, vol. 20, Springer-Verlag, New York, 1990.

[W1] E. Witten, *Gauge theories, vertex models, and quantum groups*, Nuclear Phys. B **330** (1990), 285–346.

[W2] E. Witten, *Quantization of Chern-Simons gauge theory with complex gauge group*, Comm. Math. Phys. **137** (1991), 29–66.

$*$ Since this paper was submitted, Kirkman, Musson, and Passman have shown in recent work that a down-up algebra is left and right Noetherian if and only if it is a domain if and only if $\beta \neq 0$. Their approach is to relate down-up algebras satisfying $\beta \neq 0$ to generalized Weyl algebras. It has been proved independently by Kulkarni (using methods from hyperbolic rings) that $\beta \neq 0$ is a necessary and sufficient condition for $A(\alpha, \beta, \gamma)$ to be a domain. The problem of determining the center of a down-up algebra has been solved in a very recent preprint of Zhao. This result was also announced by Kulkarni.

Department of Mathematics, University of Wisconsin, Madison, Wisconsin 53706 USA

E-mail address: `benkart@math.wisc.edu`

This page intentionally left blank

http://dx.doi.org/10.1090/conm/224/03194

Contemporary Mathematics
Volume **224**, 1999

Localizations of Grothendieck Groups and Galois Structure

Ted Chinburg, Boas Erez, Georgios Pappas, and Martin Taylor

ABSTRACT. In this paper we describe how the theory of ordinary and modular characters may be localized at the prime ideals of certain commutative rings acting on the representation ring of a finite group over a field. This localized character theory, and a Lefschetz Riemann Roch Theorem, are applied to study the Galois module structure of the cohomology of the structure sheaves of semi-stable curves over rings of algebraic integers.

1. Introduction

Two basic techniques in studying modules for a finite group are character theory and localization. The first part of this paper concerns how character theory may itself be localized, in the following sense. Suppose T is a subgroup of a finite group G, and that F is a field. The Grothendieck group $G_0^{\mathbf{Z}}(\mathbf{Z}G)$ of all finitely generated $\mathbf{Z}G$-lattices becomes a commutative ring via the tensor product of lattices over $\mathbf{Z}$. Via the restriction of operators from G to T and the tensor product of T-modules over $\mathbf{Z}$, $G_0^{\mathbf{Z}}(\mathbf{Z}G)$ acts on the Grothendieck group $G_0(FT)$ of all finitely generated FT-modules. Brauer (c.f. §2) determined the prime ideals ρ of $G_0^{\mathbf{Z}}(\mathbf{Z}G)$, while the theory of ordinary and modular characters (c.f. §3) provides a description of $G_0(FT)$ by means of functions on T. Our main result concerning $G_0(FT)$ is a character theoretic description (c.f. Theorem 3.8) of the localization $G_0(FT)_\rho$ by means of functions on a subset $T^{\ell,\rho}$ of T, where ℓ is the characteristic of F. This description allows one to readily compute the rank of $G_0(FT)_\rho$ as a finitely generated module over the localization $\mathbf{Z}_{\mathbf{q}}$ of $\mathbf{Z}$ at the ideal $\mathbf{q}$ generated by the residue characteristic of ρ. Theorem 3.8 is also useful in analyzing the ring structure on $G_0(FT)_\rho$ resulting from the tensor product of FT-modules over F. We illustrate some applications of Theorem 3.8 in §4.

The above localization of character theory can be used to study the coherent Galois module structure of schemes. Suppose X is a projective scheme over the ring of integers $\mathcal{O}_N$ of a number field N, with a right action of a finite group G

1991 *Mathematics Subject Classification.* Primary 20C15, 20C20, 19E20; Secondary 14C40, 14H25, 14F40.

The first author was supported in part by NSF Grant #DMS-9701411.
The second author was supported in part by the E. P. S. R. C..
The third author was supported in part by NSF grant #DMS-9623269.
The fourth author was supported in part by the E. P. S. R. C..

over $\mathcal{O}_N$. Let $G_0(G,X)$ be the Grothendieck group of all coherent $\mathcal{O}_X$-modules $\mathcal{F}$ having an action of G compatible with the action of G on $\mathcal{O}_X$. If $f : X \to \mathrm{Spec}(\mathcal{O}_N)$ is the structure morphism, one has an Euler characteristic map $f_* : G_0(G,X) \to G_0(\mathcal{O}_N G)$. This map, and a more refined Euler characteristic for tame G-actions, are recalled in §5; in the following discussion we identify $G_0(\mathcal{O}_N G)$ with the Grothendieck group $G_0^{\mathcal{O}_N}(\mathcal{O}_N G)$ of $\mathcal{O}_N G$-lattices. Coherent Galois structure theory has to do with methods for determining $f_*(\mathcal{F})$, and with connections between such Euler characteristics and other invariants of the G action on X. For a survey of some results in this subject, see [**6**].

The ring $G_0^{\mathbf{Z}}(\mathbf{Z}G)$ acts on $G_0(G,X)$ and $G_0(\mathcal{O}_N G)$ via the tensor product over $\mathbf{Z}$. In §5 we recall a Lefschetz Riemann Roch Theorem from [**2**] concerning the image $f_*(\mathcal{F})_\rho$ of $f_*(\mathcal{F})$ in the localization of $G_0(\mathcal{O}_N G)$ at a prime ideal ρ of $G_0^{\mathbf{Z}}(\mathbf{Z}G)$. (If the action of G is tame one may prove a more refined result.) The interest of this theorem is that it provides a way of determining $f_*(\mathcal{F})_\rho$ from calculations of Euler characteristics on a G-stable closed subset $X^{\rho,\mathrm{red}}$ of X which may be much smaller than X. The localized character theory developed in §3 is useful in carrying out these calculations.

To illustrate the results of §3 - §5, we consider in §6 the following situation. Let $G = T$ be a group of prime order r acting on a curve X over $\mathcal{O}_N$. Let $\mathcal{H}(\mathcal{O}_N, G)$ be the subgroup of $G_0(\mathcal{O}_N G)$ generated by r-torsion classes and classes induced up to G from the trivial subgroup. We will suppose the fixed point set X^G is zero-dimensional, and that the fibers of X over $\mathcal{O}_N$ are reduced with at most ordinary double points having tangent directions defined over $\mathcal{O}_N$. Under these conditions, we show in Theorem 6.3 a formula for the image of $f_*(\mathcal{O}_X)$ in $G_0(\mathcal{O}_N G)/\mathcal{H}$ in terms of the action of G on the tangent spaces of the points of X^G which do not lie over r. The first and second Stickelberger elements Θ and Θ_2 of $\mathbf{Z}[\mathrm{Aut}(G)]$ enter into this formula. From it one may deduce (c.f. Corollary 6.5) that $f_*(\mathcal{O}_X)$ lies in the subgroup of $G_0(\mathcal{O}_N G)$ generated by $\mathcal{H}(\mathcal{O}_N, G)$ and the images of Θ and Θ_2 acting on $G_0(\mathcal{O}_N G)$. This provides an upper bound for the set of classes in $G_0(\mathcal{O}_N G)$ which are of the form $f_*(\mathcal{O}_X)$ for some X as above. One can view Corollary 6.5 as a step towards a counterpart for two-dimensional schemes of McCulloh's results in [**10**] and [**11**] concerning classes coming from the Galois structure of rings of integers. When the action of G on X is tame, we prove analogous results concerning a refined Euler characteristic $f_*^{CT}(\mathcal{O}_X)$ in $K_0(\mathcal{O}_N G)$. If instead of assuming X^G is zero-dimensional, one assumes X^G is empty or purely 1-dimensional, a more precise result which completely determines $f_*(\mathcal{O}_X)$ in $G_0(\mathcal{O}_N G)$ can be obtained by a different method [**8**].

In §3 we have allowed T to be a proper subgroup of G. This case arises from studying coherent Galois structure on G-schemes X for which the inertia group T of a point $x \in X$ is strictly between G and the identity subgroup. In later papers we plan to return to this topic in greater generality by studying both lower and upper bounds on the set of classes in $G_0(\mathcal{O}_N G)$ or $K_0(\mathcal{O}_N G)$ which are of the form $f_*(\mathcal{O}_X)$ or $f_*^{CT}(\mathcal{O}_X)$ for G-schemes X over $\mathcal{O}_N$ of various kinds.

2. Prime ideals of $G_0^{\mathbf{Z}}(\mathbf{Z}G)$

Let G be a finite group. Define $G_0^{\mathbf{Z}}(\mathbf{Z}G)$ to be the Grothendieck group of all finitely generated $\mathbf{Z}G$-lattices. Then $G_0^{\mathbf{Z}}(\mathbf{Z}G)$ is a commutative ring via the tensor product of lattices over $\mathbf{Z}$. By [**5**, Th. 39.12] and [**4**, Th. 24.1], $G_0^{\mathbf{Z}}(\mathbf{Z}G)$ is finite over $\mathbf{Z}$. In this section we recall a description of the prime ideals of $G_0^{\mathbf{Z}}(\mathbf{Z}G)$ due to Brauer.

PROPOSITION 2.1. *Tensoring $\mathbf{Z}G$-lattices with $\mathbf{Q}$ over $\mathbf{Z}$ induces a surjective ring homomorphism $G_0^{\mathbf{Z}}(\mathbf{Z}G) \to G_0(\mathbf{Q}G)$ having nilpotent kernel. As a consequence, the prime ideals of $G_0^{\mathbf{Z}}(\mathbf{Z}G)$ correspond bijectively to those of $G_0(\mathbf{Q}G)$.*

PROOF. This is [**5**, Thm. 39.16]. $\square$

Let ζ be a root of unity in an algebraic closure $\overline{\mathbf{Q}}$ of $\mathbf{Q}$ which has order divisible by the order of each element of G. We define an action of $\Gamma_{\mathbf{Q}} = Gal(\overline{\mathbf{Q}}/\mathbf{Q})$ on G by letting $\sigma \in \Gamma_{\mathbf{Q}}$ send $g \in G$ to $\sigma(g) = g^t$, where t is any integer such that $\sigma(\zeta) = \zeta^t$. Two elements $g, g' \in G$ are said to be $\Gamma_{\mathbf{Q}}$-conjugate if g' is conjugate to $\sigma(g)$ for some $\sigma \in \Gamma_{\mathbf{Q}}$.

PROPOSITION 2.2. *Let χ_c be the character of $c \in G_0(\mathbf{Q}G)$. The map $c \to \chi_c$ identifies $G_0(\mathbf{Q}G)$ with the ring $R_{\mathbf{Q}}(G)$ of characters of representations of G which are realizable over $\mathbf{Q}$.*

a. *Let ℓ be a prime ideal of $\mathbf{Z}$. Suppose g is an ℓ-regular element of G, i.e. an element of order prime to ℓ. The kernel $Q_{\ell,g}$ of the homomorphism $R_{\mathbf{Q}}(G) \to \mathbf{Z}/\ell$ defined by $\chi \to \chi(g)$ mod ℓ is a prime ideal of $R_{\mathbf{Q}}(G)$, and all primes of $R_{\mathbf{Q}}(G)$ arise in this way.*
b. *Suppose $g' \in G$ is ℓ'-regular for some prime ideal ℓ' of $\mathbf{Z}$. One has $Q_{\ell',g'} = Q_{\ell,g}$ if and only if $\ell' = \ell$ and g is $\Gamma_{\mathbf{Q}}$-conjugate to g'.*
c. *For g' and ℓ' as above, one has $Q_{\ell',g'} \subset Q_{\ell,g}$ if and only if $\ell' \subset \ell$ and $g' = g'' \cdot h$ for some $g'', h \in G$ having the following properties:*
   (i) *g'' is $\Gamma_{\mathbf{Q}}$-conjugate to g and commutes with h;*
   (ii) *h is the identity if $\ell = \{0\}$;*
   (iii) *h has order a power of the residue characteristic of ℓ if $\ell \neq \{0\}$.*

PROOF. Define $A = \mathbf{Z}[\zeta]$. Since $A \otimes_{\mathbf{Z}} R_K(G)$ is finite over $R_K(G)$, the map which identifies a prime of $R_K(G)$ with the set of primes over it in $A \otimes_{\mathbf{Z}} R_K(G)$ defines a bijection. From [**12**, Ex. 12.7, p. 101] one finds that the prime ideals of $A \otimes_{\mathbf{Z}} R_K(G)$ may be described in the the following way. Let $\mathbf{q}$ be a prime ideal of A, and let g be a $\mathbf{q}$-regular element of G. The kernel $P_{\mathbf{q},g}$ of the homomorphism $A \otimes_{\mathbf{Z}} R_{\mathbf{Q}}(G) \to A/\mathbf{q}$ defined by $a \otimes \chi \to a\chi(g)$ *mod* $\mathbf{q}$ is a prime ideal of $A \otimes_{\mathbf{Z}} R_{\mathbf{Q}}(G)$, and each prime ideal of this ring arises in this way. One has $P_{\mathbf{q}',g'} \subset P_{\mathbf{q},g}$ if and only if $\mathbf{q}' \subset \mathbf{q}$ and $g' = g'' \cdot h$ where g'' is $\Gamma_{\mathbf{Q}}$-conjugate to g and commutes with h, h is the identity if $\mathbf{q} = \{0\}$, and h has order a power of the residue characteristic of $\mathbf{q}$ if $\mathbf{q} \neq 0$. One has $P_{\mathbf{q}',g'} = P_{\mathbf{q},g}$ and only if $\mathbf{q}' = \mathbf{q}$ and g is conjugate to g'.

For $h \in H = Gal(\mathbf{Q}(\zeta)/\mathbf{Q})$ one sees that h sends $P_{\mathbf{q},g}$ to $P_{h(\mathbf{q}),g}$, since H acts trivially on $R_{\mathbf{Q}}(G)$. Since $R_{\mathbf{Q}}(G)$ is flat over $\mathbf{Z}$ we have $(A \otimes_{\mathbf{Z}} R_{\mathbf{Q}}(G))^H = A^H \otimes_{\mathbf{Z}} R_{\mathbf{Q}}(G) = R_{\mathbf{Q}}(G)$. Therefore H permutes transitively the primes of $A \otimes_{\mathbf{Z}} R_{\mathbf{Q}}(G)$ over a given prime of $R_{\mathbf{Q}}(G)$. From the definition of $P_{\mathbf{q},g}$ we see that $P_{\mathbf{q},g} \cap R_{\mathbf{Q}}(G) = Q_{\ell,g}$ if $\mathbf{q} \cap \mathbf{Z} = \ell$. Thus the primes over $Q_{\ell,g}$ in $A \otimes_{\mathbf{Z}} R_{\mathbf{Q}}(G)$ are exactly those of the form $P_{\mathbf{q}',g}$ for $\mathbf{q}'$ a prime of A over ℓ. The description of the primes of $R_{\mathbf{Q}}(G)$ given in Proposition 2.2 now follows from the above description of the primes of $A \otimes_{\mathbf{Z}} R_{\mathbf{Q}}(G)$. $\square$

DEFINITION 2.3. *Suppose ℓ is a prime of $\mathbf{Z}$ and g is an ℓ-regular element of G. Let $\rho_{\ell,g}$ be the prime ideal of $G_0^{\mathbf{Z}}(\mathbf{Z}G)$ corresponding to the the prime $Q_{\ell,g}$ of*

Proposition 2.2(a) under the bijection $\mathrm{Spec}(R_{\mathbf{Q}}(G)) \leftrightarrow \mathrm{Spec}(G_0^{\mathbf{Z}}(\mathbf{Z}G))$ *of Proposition 2.1.*

3. Localized character theory

In this section we will use character theory to find explicit expressions for the localizations of certain Grothendieck groups. We begin with a general result which will clarify the structure of modules for $G_0^{\mathbf{Z}}(\mathbf{Z}G)$.

PROPOSITION 3.1. *Suppose $\mathcal{R}$ is a commutative ring finite over $\mathbf{Z}$ such that the algebra $\mathbf{Q} \otimes_{\mathbf{Z}} \mathcal{R}$ is the direct sum of a finite number of copies of $\mathbf{Q}$. Let M be an $\mathcal{R}$-module. Suppose $\mathbf{q}$ (resp. ρ) is a prime ideal of $\mathbf{Z}$ (resp. $\mathcal{R}$). Let $M_{\mathbf{q}}$ (resp. M_ρ) be the localization of M at $\mathbf{q}$ (resp. ρ). Define $P(\mathbf{q})$ to be the set of primes of $\mathcal{R}$ over $\mathbf{q}$. Then the natural $\mathcal{R}_{\mathbf{q}}$-module homomorphism*

$$M_{\mathbf{q}} \to \bigoplus_{\rho \in P(\mathbf{q})} M_\rho \tag{3.1}$$

is an isomorphism. Here $M_{\mathbf{q}} = \mathbf{Z}_{\mathbf{q}} \otimes_{\mathbf{Z}} M = \mathcal{R}_{\mathbf{q}} \otimes_{\mathcal{R}} M$ and $M_\rho = \mathcal{R}_\rho \otimes_{\mathcal{R}} M$.

PROOF. Consider the natural $\mathcal{R}_{\mathbf{q}}$-algebra homomorphism

$$h : \mathcal{R}_{\mathbf{q}} \to \bigoplus_{\rho \in P(\mathbf{q})} \mathcal{R}_\rho. \tag{3.2}$$

By the definition of localization and tensor products, one has $M_{\mathbf{q}} = \mathbf{Z}_{\mathbf{q}} \otimes_{\mathbf{Z}} M = \mathcal{R}_{\mathbf{q}} \otimes_{\mathcal{R}} M$ and $M_\rho = \mathcal{R}_\rho \otimes_{\mathcal{R}} M$. Thus the desired direct decomposition (3.1) will follow from h being an isomorphism. If $\mathbf{q} = 0$, we have assumed that $\mathcal{R}_{\mathbf{q}} = \mathbf{Q} \otimes_{\mathbf{Z}} \mathcal{R}$ is isomorphic as a $\mathbf{Q}$-algebra to the direct sum of copies of $\mathbf{Q}$; therefore h defines such an isomorphism. Hence for the rest of the proof we may assume that $\mathbf{q}$ is a maximal ideal of $\mathbf{Z}$. Then h is the natural homomorphism from the ring $\mathcal{R}_{\mathbf{q}}$ into the (finite) product of its localizations at the maximal ideals of $\mathcal{R}_{\mathbf{q}}$, so h is injective. It will thus suffice to show h is surjective.

Let $\mathcal{R}'$ be the normalization of the image of $\mathcal{R}$ in $\mathcal{R} \otimes_{\mathbf{Z}} \mathbf{Q}$. Since $\mathcal{R}$ is finite over $\mathbf{Z}$, the natural ring homomorphism $\mathcal{R} \to \mathcal{R}'$ has finite kernel and cokernel. Since $\mathcal{R} \otimes_{\mathbf{Z}} \mathbf{Q}$ is algebra isomorphic a direct sum of copies of $\mathbf{Q}$, $\mathcal{R}'$ must be isomorphic to a direct sum of copies of $\mathbf{Z}$. Consider now the diagram of morphisms

$$\begin{array}{ccccc} \mathcal{R}_{\mathbf{q}} & \xrightarrow{h} & \bigoplus_{\rho \in P(\mathbf{q})} \mathcal{R}_\rho & & \\ \downarrow & & \downarrow & & \\ \mathcal{R}'_{\mathbf{q}} & \xrightarrow[\alpha]{} & \bigoplus_{\rho \in P(\mathbf{q})} \mathcal{R}'_\rho & \xrightarrow[\beta]{} & \bigoplus_{\rho' \in P'(\mathbf{q})} \mathcal{R}'_{\rho'} \end{array} \tag{3.3}$$

Here $\mathcal{R}'_\rho$ is the localization of $\mathcal{R}'$ at ρ when one considers $\mathcal{R}'$ as an $\mathcal{R}$-module. The set $P'(\mathbf{q})$ is the set of prime ideals ρ' of $\mathcal{R}'$ over $\mathbf{q}$. The injective homomorphism α in the second row of (3.3) comes from viewing $\mathcal{R}'$ as an $\mathcal{R}$-module. The injective homomorphism β comes from the natural map $\mathcal{R}'_\rho \to \bigoplus_{\rho' | \rho} \mathcal{R}'_{\rho'}$, where the direct sum is over the primes ρ' over ρ in $\mathcal{R}'$. The composition $\beta \circ \alpha$ is the natural map $\mathcal{R}'_{\mathbf{q}} \to \bigoplus_{\rho' \in P'(\mathbf{q})} \mathcal{R}'_{\rho'}$, which is an isomorphism since $\mathcal{R}'$ is the algebra direct sum of a finite number of copies of $\mathbf{Z}$. Thus α and β are isomorphisms. Now because $\mathcal{R} \to \mathcal{R}'$ has finite kernel and cokernel, the vertical homomorphisms in diagram (3.3) also have finite kernel and cokernel because localization is exact. It follows that h must have finite cokernel, and we have already shown the kernel of h is $\{0\}$.

Since $\mathbf{q}$ is a maximal ideal of $\mathbf{Z}$, the finiteness of $coker(h)$ implies

$$\bigoplus_{\rho \in P(\mathbf{q})} \mathbf{q}^t \mathcal{R}_\rho \subset h(\mathcal{R}_\mathbf{q}) \tag{3.4}$$

for some integer $t \geq 0$. On localizing the surjection $\mathcal{R} \to \mathcal{R}/\mathbf{q}^t\mathcal{R}$ at ρ we obtain an isomorphism $\mathcal{R}_\rho/\mathbf{q}^t\mathcal{R}_\rho \to (\mathcal{R}/\mathbf{q}^t\mathcal{R})_\rho$. Now $\mathcal{R}/\mathbf{q}^t\mathcal{R}$ is a finite $\mathcal{R}$-module since $\mathcal{R}$ is finite over $\mathbf{Z}$, so this module is supported on finitely many prime ideals of $\mathcal{R}$. It follows from the structure theorem for commutative Artinian rings [**9**, Thm. VI.9.7] that the natural map

$$\mathcal{R}/\mathbf{q}^t\mathcal{R} \to \bigoplus_{\rho \in P(\mathbf{q})} \mathcal{R}_\rho/\mathbf{q}^t\mathcal{R}_\rho \tag{3.5}$$

is an isomorphism. Combining (3.4) and (3.5), we see h is surjective, and by what has already been shown this completes the proof. □

DEFINITION 3.2. *Let F be a field of characteristic $l \geq 0$ and let T be a subgroup of a finite group G which acts trivially on F. The Grothendieck group $G_0(FT)$ is a $G_0^{\mathbf{Z}}(\mathbf{Z}T)$-module via the tensor product over $\mathbf{Z}$ of $\mathbf{Z}T$-lattices. We may regard $G_0(FT)$ as a $G_0^{\mathbf{Z}}(\mathbf{Z}G)$-module via the ring homomorphism $G_0^{\mathbf{Z}}(\mathbf{Z}G) \to G_0^{\mathbf{Z}}(\mathbf{Z}T)$ induced by the restriction of operators from G to T.*

COROLLARY 3.3. *When $\mathcal{R} = G_0^{\mathbf{Z}}(\mathbf{Z}G)$ the hypothesis of Proposition 3.1 is satisfied. Thus in particular,*

$$\mathbf{Z}_\mathbf{q} \otimes_\mathbf{Z} G_0(FT) = G_0(FT)_\mathbf{q} = \bigoplus_{\rho \in P(\mathbf{q})} G_0(FT)_\rho \tag{3.6}$$

for all fields F and subgroups $T \subset G$. Since $G_0(FG)$ is a free finitely generated $\mathbf{Z}$-module on the classes of simple FT-modules, each of the modules appearing in (3.6) is a free finitely generated $\mathbf{Z}_\mathbf{q}$-module.

We now recall how $G_0(FT)$ may be described by character theory.

DEFINITION 3.4. *Let $l = char(F)$. If $l = 0$, let $W(F) = F$ and let $T^l = T$. If $l > 0$, let $W(F)$ be the ring of Witt vectors over F, and let T^l be the set of l-regular elements of T. Define $K(F)$ to be the fraction field of $W(F)$. Let n be the exponent of T. Define n_l be the part of n which is prime to l, so that $n = l^a n_l$ for some integer $a \geq 0$. Let $\bar{\zeta}_{n_l}$ be a primitive n_l-th root of unity in a fixed separable closure F^{sep} of F. Then $L = F(\bar{\zeta}_{n_l})$ is a finite seperable extension of F, and there is a unique root of unity $\zeta_{n_l} \in W(L)$ which reduces to $\bar{\zeta}_{n_l}$ modulo the maximal ideal of $W(L)$. Let A' be the subring $\mathbf{Z}[\zeta_{n_l}]$ of $W(L)$. The action of the Galois group $Gal(L/F)$ on L extends in a unique way to an action on $W(L)$, and we let A be the subring of A' fixed by $Gal(L/F)$*

Note that $K(L)/K(F)$ is an unramified Galois extension of fields, with Galois group $Gal(L/F)$. We have an injective homomorphism $Gal(L/F) \to (\mathbf{Z}/n_l)^*$ defined by $\sigma \to t$ if $\sigma(\bar{\zeta}_{n_l}) = (\bar{\zeta}_{n_l})^t$. Let $I_{n_l}(F)$ be the image of $Gal(L/F)$ under this homomorphism. We will say two elements $x, y \in T^l$ are F-conjugate in T if x is conjugate in T to y^t for some $t \in I_{n_l}(F)$.

DEFINITION 3.5. *Suppose T' is a union of conjugacy classes in T^l and that $\mathcal{R}$ is a commutative ring. Define $\mathrm{Hom}_{cl}^F(T', \mathcal{R})$ to be the set of functions $f : T' \to \mathcal{R}$ such that $f(t) = f(t')$ if $t, t' \in T'$ are F-conjugate in T. Then $\mathrm{Hom}_{cl}^F(T', \mathcal{R})$ becomes* *a ring via the ring operations of* $\mathcal{R}$. *We define a* $G_0^{\mathbf{Z}}(\mathbf{Z}G)$*-module structure on* $\mathrm{Hom}_{cl}^F(T',\mathcal{R})$ *in the following way. Suppose* $\alpha \in G_0^{\mathbf{Z}}(\mathbf{Z}G)$ *and* $f \in \mathrm{Hom}_{cl}^F(T',\mathcal{R})$. *The restriction of the character* χ_α *of* α *to* T' *is an element of* $\mathrm{Hom}_{cl}^{\mathbf{Q}}(T',\mathbf{Z}) \subset \mathrm{Hom}_{cl}^F(T',\mathbf{Z})$. *We let* $\alpha \cdot f$ *be* $\chi_\alpha \cdot f$.

Suppose $s \in T^l$ and that M is an FT-module of dimension m. Since s has order prime to $l = char(F)$, the action of s on $F^{sep} \otimes_F M$ is diagonalizable. The eigenvalues $\{\bar{\mu}_1, \dots, \bar{\mu}_m\}$ of s are roots of unity in $L \subset \overline{F}$ of order dividing the l-primary part n_l of the exponent n of T. Let $\mu_i \in A' \subset W(L)$ be the unique root of unity of order equal to that of $\bar{\mu}_i$ which has image $\bar{\mu}_i$ in L. Define the (Brauer) character of M to be the function $\chi_M : T^l \to A'$ defined by

$$\chi_M(s) = \sum_{i=1}^{m} \mu_i.$$

Since M is an FT-module, the action of an automorphism of $Gal(L/F)$ must permute the eigenvalues $\{\bar{\mu}_1, \dots, \bar{\mu}_m\}$. Recall that elements of $Gal(L/F)$ extend in a unique way to automorphisms of $W(L)$ over $W(F)$. It follows that χ_M takes values in $A = A'^{Gal(L/F)} \subset W(F) = W(F^{sep})^{Gal(F^{sep}/F)}$. Suppose $\sigma \in Gal(L/F)$ has image $t \in I_{n_l}(F)$ and that $x = s^t$ in T. Then the action of σ takes the eigenvalues of s on M to those for $x = s^t$, so by what we have already shown, these sets of eigenvalues are permutations of one another. It follows that χ_M is an element of $\mathrm{Hom}_{cl}^F(T^l, A)$.

THEOREM 3.6. ([**4**, p. 508 - 511 and Thm. 21.25]) *The function* $M \to \chi_M$ *extends additively to an injective* $G_0^{\mathbf{Z}}(\mathbf{Z}G)$*-algebra homomorphism* $\chi : G_0(FT) \to \mathrm{Hom}_{cl}^F(T^l, A)$. *This homomorphism and the inclusion of* A *into* $K(F)$ *induce an isomorphism of* $K(F)$*-vector spaces*

$$\chi \otimes 1 : G_0(FT) \otimes_{\mathbf{Z}} K(F) \to \mathrm{Hom}_{cl}^F(T^l, K(F))$$

where $G_0(FT)$ *is a free finitely generated abelian group. It follows that the rank of* $G_0(FT)$ *as a free abelian group equals the dimension of* $\mathrm{Hom}_{cl}^F(T^l, K(F))$ *over* $K(F)$, *which is the number of distinct* F*-conjugacy classes in* T^l.

We now state our main result concerning localizations of $G_0(FT)$ at prime ideals of $G_0^{\mathbf{Z}}(\mathbf{Z}G)$.

DEFINITION 3.7. *Let* $\mathbf{q}$ *be a prime ideal of* $\mathbf{Z}$, *and suppose* $g \in G$ *is* $\mathbf{q}$*-regular.*

a. *For* $c \in G_0^{\mathbf{Z}}(\mathbf{Z}G)$, *the character* χ_c *takes values in* $\mathbf{Z}$. *Let* $\rho = \rho_{\mathbf{q},g}$ *be the prime ideal of all* $c \in G_0^{\mathbf{Z}}(\mathbf{Z}G)$ *such that* $\chi_c(g) \equiv 0$ *mod* $\mathbf{q}$. *By Propositions 2.2 and 2.1, all prime ideals of* $G_0^{\mathbf{Z}}(\mathbf{Z}G)$ *have this form for some* $\mathbf{q}$ *and* g.
b. *If* $\mathbf{q} = \{0\}$, *let* $T^{l,\rho}$ *be the set of* $t \in T^l$ *which are conjugate in* G *to a generator of* $< g >$. *Suppose now that* $\mathbf{q} = p\mathbf{Z}$ *for some rational prime number* p. *Let* $T^{l,\rho}$ *be the set of* $t \in T^l$ *which are conjugate in* G *to a product of the form* $g' \cdot g''$, *where* g' *is a generator of* $< g >$, g'' *is of* p*-power order, and* g' *and* g'' *commute.*

THEOREM 3.8. . *With the notations of Definitions 3.4, 3.5 and 3.7, let* $\rho = \rho_{\mathbf{q},g}$ *be a prime ideal of* $G_0^{\mathbf{Z}}(\mathbf{Z}G)$ *over* $\mathbf{q}$.

a. *If* $\alpha \in G_0^{\mathbf{Z}}(\mathbf{Z}G) - \rho$, *then* $\chi_\alpha(g) \in \mathbf{Z} - \mathbf{q}$. *Let* $A_{\mathbf{q}}$ *(resp.* $\mathbf{Z}_{\mathbf{q}}$ *) be the localization of* $A = \mathbf{Z}[\zeta]$ *(resp.* $\mathbf{Z}$ *) at the multiplicative set* $\mathbf{Z} - \mathbf{q}$. *We then have an* *isomorphism of $G_0^{\mathbf{Z}}(\mathbf{Z}G)_\rho$ algebras*

$$z : \mathrm{Hom}_{cl}^F(T^l, A)_\rho \to \mathrm{Hom}_{cl}^F(T^{l,\rho}, A_{\mathbf{q}})$$

induced by $\alpha^{-1} \cdot f \to h$, where $h(t) = \chi_\alpha(t)^{-1} \cdot f(t)$ for $t \in T^{l,\rho}$.

b. *The character map in Theorem 3.6 together with the isomorphism in (a) induces an injection of $G_0^{\mathbf{Z}}(\mathbf{Z}G)_\rho$-algebras*

$$\chi_\rho : G_0(FT)_\rho \to \mathrm{Hom}_{cl}^F(T^{l,\rho}, A_{\mathbf{q}}).$$

c. *On viewing $\mathbf{Z_q}$ and $A_{\mathbf{q}}$ as subrings of $K(F)$, the homomorphism χ_ρ induces an isomorphism $K(F)$-vector spaces*

$$\chi_\rho \otimes 1 : G_0(FT)_\rho \otimes_{\mathbf{Z_q}} K(F) \to \mathrm{Hom}_{cl}^F(T^{l,\rho}, K(F)).$$

Thus $r = rank_{\mathbf{Z_q}}(G_0(FT)_\rho) = \dim_{K(F)}\mathrm{Hom}_{cl}^F(T^{l,\rho}, K(F))$ is the number of F-conjugacy classes in $T^{l,\rho}$, where conjugation is taken with respect to elements of T.

d. *Via χ_ρ, the algebra $\mathrm{Hom}_{cl}^F(T^{l,\rho}, A_{\mathbf{q}})$ is finite over the ring $G_0(FT)_\rho$. An element $\beta \in G_0(FT)_\rho$ is a unit if and only if $\chi_\rho(\beta) \in \mathrm{Hom}_{cl}^F(T^{l,\rho}, A_{\mathbf{q}}^*)$, where $A_{\mathbf{q}}^*$ is the unit group of $A_{\mathbf{q}}$.*

PROOF. Suppose, as in (a), that $\rho = \rho_{\mathbf{q},g}$ and $\alpha \in G_0^{\mathbf{Z}}(\mathbf{Z}G) - \rho$. Let t be an element of $T^{l,\rho}$. By definition, t is conjugate to $g' \cdot g''$ in G, where $< g' >=< g >$, g'' is the identity if $\mathbf{q} = \{0\}$, and g'' is an element of p-power order which commutes with g' if $\mathbf{q} = p\mathbf{Z} \neq 0$. The character χ_α is the character of a rational representation of G. Hence χ_α takes values in $\mathbf{Z}$. As in [**4**, Lemma 21.12] we have

$$\begin{aligned} \chi_\alpha(t) &= \chi_\alpha(g' \cdot g'') \\ &\equiv \chi_\alpha(g') \mod \mathbf{q} \\ &= \chi_\alpha(g) \end{aligned} \tag{3.7}$$

Since $\alpha \notin \rho$, we have $\chi_\alpha(g) \not\equiv 0 \bmod \mathbf{q}$. Therefore $\chi_\alpha(t) \in \mathbf{Z} - \mathbf{q}$, as claimed. We see from this that the map z in (a) is well defined. The fact that z is a $G_0^{\mathbf{Z}}(\mathbf{Z}G)_\rho$-algebra map follows from the definitions of the algebra structures on the domain and range. The map

$$\mathrm{Hom}_{cl}^F(T^l, A) \to \mathrm{Hom}_{cl}^F(T^{l,\rho}, A)$$

induced by restriction of functions from T^l to $T^{l,\rho}$ is surjective. Since $\mathbf{Z_q}$ injects into $G_0^{\mathbf{Z}}(\mathbf{Z}G)_\rho$ and $A_{\mathbf{q}} = \mathbf{Z_q} \cdot A$, we deduce from this that z is surjective. To show that z is injective, it will suffice to show that if $f \in \mathrm{Hom}_{cl}^F(T^l, A)$ and f has trivial image in $\mathrm{Hom}_{cl}^F(T^{l,\rho}, A_{\mathbf{q}})$, then there is an $\alpha \in G_0^{\mathbf{Z}}(\mathbf{Z}G) - \rho$ such that $\alpha \cdot f = 0$. Since A injects into $A_{\mathbf{q}}$, we know that f vanishes on the elements of $T^{l,\rho}$. Suppose $t \in T^l - T^{l,\rho}$. Let ρ' be the prime ideal of $\rho_{\{0\},t}$ of $G_0^{\mathbf{Z}}(\mathbf{Z}G)$. Thus ρ' is the ideal of all $\beta \in G_0^{\mathbf{Z}}(\mathbf{Z}G)$ such that $\chi_\beta(t) = 0$. In view of Definition 3.4 and Proposition 2.2, the assumption that $t \notin T^{l,\rho}$ implies $\rho = \rho_{\mathbf{q},g}$ does not contain ρ'. Thus there is an element $\alpha_t \in \rho'$ which is not in ρ. The product

$$\alpha = \prod_{t \in T^l - T^{l,\rho}} \alpha_t$$

does not lie in ρ, and $\chi_\alpha(t) = 0$ for all $t \in T^l - T^{l,\rho}$. Thus $\alpha \cdot f$ vanishes on all elements of T^l since f vanishes on the elements of $T^{l,\rho}$. This proves z is injective.

The existence of the injective character map χ_ρ in part (b) now follows from (a) on localizing at ρ the injection $\chi : G_0(FT) \to \mathrm{Hom}^F_{cl}(T^l, A)$ of Theorem 3.6.

To prove (c), recall from Corollary 3.3 that we have a direct sum decomposition

$$G_0(FT) \otimes_{\mathbf{Z}} \mathbf{Z}_{\mathbf{q}} = \bigoplus_\rho G_0(FT)_\rho$$

where the summands on the right are finitely generated free $\mathbf{Z}_{\mathbf{q}}$-modules. On tensoring with $K(F)$ over $\mathbf{Z}_{\mathbf{q}}$ we get an isomorphism

$$G_0(FT) \otimes_{\mathbf{Z}} K(F) \to \bigoplus_\rho G_0(FT)_\rho \otimes_{\mathbf{Z}_{\mathbf{q}}} K(F). \tag{3.8}$$

Consider now the homomorphism

$$\chi_\rho \otimes 1 : G_0(FT)_\rho \otimes_{\mathbf{Z}_{\mathbf{q}}} K(F) \to \mathrm{Hom}^F_{cl}(T^{l,\rho}, K(F)) \tag{3.9}$$

which results from χ_ρ and the embedding of $A_{\mathbf{q}}$ into $K(F)$. Taking the direct sum of these maps over the summands on the right hand side of (3.8) gives a homomorphism

$$G_0(FT) \otimes_{\mathbf{Z}} K(F) \to \bigoplus_\rho \mathrm{Hom}^F_{cl}(T^{l,\rho}, K(F)) = \mathrm{Hom}^F_{cl}(T^l, K(F))$$

in which the second equality follows from

$$T^l = \sqcup_\rho T^{l,\rho}.$$

This is exactly the isomorphism appearing in Theorem 3.6. Since (3) is an isomorphism, we conclude that each of the homomorphisms in (3.9) must be as well, which proves (c).

We finally prove (d). By (b), (c) and Corollary 3.3, χ_ρ induces an injection $\mathcal{R} = G_0(FT)_\rho \hookrightarrow \mathcal{R}' = \mathrm{Hom}^F_{cl}(T^{l,\rho}, A_{\mathbf{q}})$ of $\mathbf{Z}_{\mathbf{q}}$-algebras. These algebras are finite and flat over $\mathbf{Z}_{\mathbf{q}}$ because $A_{\mathbf{q}}$ is finite and flat over $\mathbf{Z}_{\mathbf{q}}$, so $\mathcal{R}'$ is finite over $\mathcal{R}$. The unit group $\mathcal{R}'^*$ is $\mathrm{Hom}^F_{cl}(T^{l,\rho}, A^*_{\mathbf{q}})$. Thus to show the last assertion in (d), it will suffice to show $\mathcal{R}^* = \mathcal{R} \cap \mathcal{R}'^*$. Clearly $\mathcal{R}^* \subset \mathcal{R} \cap \mathcal{R}'^*$. Suppose $\alpha \in \mathcal{R} \cap \mathcal{R}'^*$. Since $\mathcal{R}'$ is a finite flat $\mathbf{Z}_{\mathbf{q}}$-module, the characteristic polynomial over $\mathbf{Z}_{\mathbf{q}}$ of multiplication by α on $\mathcal{R}'$ has unit constant coefficient. Since α is a root of this polynomial, it follows that $\alpha \in \mathcal{R}^*$, which completes the proof. $\square$

4. Inverses of classes in $G_0(FT)_\rho$

In this section we assume the notations of Theorem 3.8. We illustrate how this result can be used to calculate inverses of certain classes in $G_0(FT)_\rho$ which arise in the study of coherent Euler characteristics (c.f. §5 and §6).

Let M be an FT-module of dimension $d \geq 0$ over F. For $i \geq 0$, the i-th lambda operator on $G_0(FT)$ is defined by the i^{th} exterior power $\lambda^i(M) = \Lambda^i M$ over F. Define

$$\lambda_{-1}(M) = \sum_{i=0}^{d} (-1)^i \Lambda^i M \tag{4.1}$$

in $G_0(FT)$. Suppose $\bar{\mu}_1(h), \ldots, \bar{\mu}_d(h)$ are the eigenvalues in $\overline{F}$ of an l-regular element h of T acting on M. The value of the virtual character of $\lambda_{-1}(M)$ on h is then

$$\chi_{\lambda_{-1}(M)}(h) = \prod_{i=1}^{d}(1 - \mu_i(h)) \tag{4.2}$$

where $\mu_i(h)$ is the unique root of unity in $W(\overline{F})$ of the same order as $\bar{\mu}_i(h)$ which has image $\bar{\mu}_i(h)$ in F.

As in Theorem 3.8, let G be a group containing T. Let $\mathbf{q}$ be a prime ideal of $\mathbf{Z}$ and suppose g is a $\mathbf{q}$-regular element of G. Let $\rho = \rho_{\mathbf{q},g}$ be the prime ideal of $G_0^{\mathbf{Z}}(\mathbf{Z}G)$ specified in Definition 3.7(a).

PROPOSITION 4.1. *The class $\lambda_{-1}(M)$ is invertible in $G_0(FT)_\rho$ if and only if $\overline{\mu}_i(h) \neq 1$ for all $h \in T^{l,\rho}$ and all $i = 1, \dots, d$. If $\mathbf{q} = p\mathbf{Z}$ for some rational prime p, this implies $\overline{\mu}_i(h)$ is not a p-power root of unity.*

PROOF. With the notations of Definition 3.4, we have an inclusion of finite flat $\mathbf{Z}_\mathbf{q}$ algebras $A_\mathbf{q} \subset A'_\mathbf{q}$. Furthermore, $\mu_i(h) \in A'_\mathbf{q}$ for $h \in T^{l,\rho}$, and $\chi_{\lambda_{-1}(M)}(h) \in A_\mathbf{q}$. By (4.2) and the argument at the end of the proof of Theorem 3.8, one sees that $\chi_{\lambda_{-1}(M)}(h) \in A^*_\mathbf{q}$ if and only if the element $1 - \mu_i(h)$ is a unit in the algebra $\mathbf{Z}[\mu_i(h)]_\mathbf{q} \subset A'_\mathbf{q}$ for all i. Hence by Theorem 3.8(d), it will suffice to show that $1 - \mu_i(h)$ is a unit for all $h \in T^{l,\rho}$ if and only if $\mu_i(h) \neq 1$ for all such h. If $\mathbf{q} = 0$ this is clear since then $\mathbf{Z}[\mu_i(h)]_\mathbf{q}$ is a field. So suppose $\mathbf{q} = p\mathbf{Z}$ for some prime p and that $\mu_i(h) \neq 1$ for all $h \in T^{l,\rho}$. If $p = l$ then h must be p regular, so $1 - \mu_i(h)$ is a unit in $\mathbf{Z}[\mu_i(h)]_\mathbf{q}$. Suppose now that $p \neq l$. It will suffice to show that $\mu_i(h)$ is not a p-power root of unity. But $l \neq p$ and the element g in Definition 3.7 is a p-regular element. Therefore Definition 3.7 implies $h^p \in T^{l,\rho}$ if $h \in T^{l,\rho}$. Hence $\mu_i(h) \neq 1$ for $h \in T^{l,\rho}$ implies no $\mu_i(h)$ can be a p-power root of unity; this completes the proof. □

We now compute an explicit inverse for $\lambda_{-1}(M)$ in $G_0(FT)_\rho$ when this class is invertible.

Write the exponent n of T as $n = n' \cdot n''$, where $n'' = 1$ if $\mathbf{q} = 0$, and where n'' is the power of p dividing n if $\mathbf{q} = p\mathbf{Z} \neq 0$. Let $x_1, \dots, x_d$ be independent commuting indeterminates, and let $s_1, \dots s_d$ be the elementary symmetric functions in the x_i. Let $P_{d,n,\mathbf{q}}(s_1, \dots, s_d)$ be the polynomial with integer coefficients such that

$$P_{d,n,\mathbf{q}}(s_1, \dots, s_d) = \prod_{i=1}^{d}((\sum_{j=1}^{n''-1} x_i^j) \cdot (\sum_{k=1}^{n'-1} k \cdot x_i^{kn''})) \tag{4.3}$$

PROPOSITION 4.2. *Suppose $\lambda_{-1}(M)$ is invertible in $G_0(FT)_\rho$. The inverse of $\lambda_{-1}(M)$ in $G_0(FT)_\rho$ is*

$$(-n')^{-d} \cdot P_{d,n,\mathbf{q}}(\lambda^1(M), \dots, \lambda^d(M))$$

where $-n'$ is a unit in $\mathbf{Z}_\mathbf{q}$.

PROOF. With the notations of Proposition 4.1, the value of the character of $\lambda^j(M)$ on $h \in T^{l,\rho}$ is $S_j = s_j(\mu_1(h), \dots, \mu_d(h))$, where s_j is the j^{th} symmetric function. Thus by Theorem 3.8, to prove Proposition 4.2 it will suffice to show

$$P_{d,n,\mathbf{q}}(S_1, \dots, S_d) \cdot \chi_{\lambda^{-1}(M)}(h) = (-n')^d \tag{4.4}$$

for $h \in T^{l,\rho}$. We have an identity

$$(4.5)\quad (1-x_i)\cdot(\sum_{j=1}^{n''-1} x_i^j)\cdot(\sum_{k=1}^{n'-1} k\cdot x_i^{kn'}) \;= (1-x_i^{n''})\cdot(\textstyle\sum_{k=1}^{n'-1} k\cdot x_i^{kn''})$$

$$(4.6)\quad = \textstyle\sum_{k=1}^{n'} x_i^{kn''} - n' x_i^{n'n''}$$

Suppose now that we substitute $\mu_i(h)$ for x_i in this identity. By Proposition 4.1, $x_i^{n''} = \mu_i(h)^{n''}$ is a nontrivial n'^{th} root of unity, so the right hand side of (4.6) equals $-n'$. Substituting this back into the right hand side of (4.3) and using (4.2) proves (4.4). □

We now discuss a special case of Proposition 4.2.

DEFINITION 4.3. *Suppose T is cyclic of prime order r. For $a \in \mathbf{Z}$, let σ_a be the element of the automorphism group* $\mathrm{Aut}(T)$ *of T for which $\sigma_a(t) = t^a$ for all $t \in T$. We define the Stickelberger element of* $\mathbf{Z}[\mathrm{Aut}(T)]$ *to be*

$$(4.7)\qquad \Theta = \sum_{0<a<r} a \cdot \sigma_a^{-1}.$$

Define a quadratic Stickelberger element of $\mathbf{Z}[\mathrm{Aut}(T)]$ *by*

$$(4.8)\qquad \Theta_2 = \sum_{0<a<r} \frac{a(a-1)}{2} \cdot \sigma_a^{-1}.$$

Suppose M is a T-module and that $\sigma \in \mathrm{Aut}(T)$. Define a T-module $\sigma(M)$ by letting $\sigma(M)$ have the same underlying group as M, and by letting $t \in T$ act on $m \in \sigma(M)$ by $t \underset{\sigma}{\cdot} m = \sigma^{-1}(t)\cdot m$. When we discuss the action of σ on various Grothendieck groups $\mathcal{G}$ of T-modules M, we will mean the action which sends the class (M) of M to $(\sigma(M))$. We will use exponential notation for the induced left action of the group ring $\mathbf{Z}[\mathrm{Aut}(T)]$ on $\mathcal{G}$.

LEMMA 4.4. *Suppose T has prime order r, $G_0(FT)_\rho \neq 0$, M is a non-zero FT-module and that $\lambda_{-1}(M)$ is invertible in $G_0(FT)_\rho$. Then the residue characteristic of ρ is different from r, and so is the characteristic ℓ of F. Suppose further that $M = \xi \oplus \xi^{-1}$ for some non-trivial one-dimensional character $\xi : T \to F^*$. Then*

$$(4.9)\qquad \lambda_{-1}(M)^{-1} = \frac{(1-r)}{2r}\cdot\xi^{\Theta} + \frac{1}{r}\cdot\xi^{\Theta_2} = \frac{1}{2}\cdot\Big(\frac{(r-1)}{2}\cdot 1_T + \frac{1}{r}\cdot M^{\Theta_2}\Big)$$

in the torsion-free group $G_0(F[T])_\rho$, where 1_T denotes the trivial character of the group T.

PROOF. Since $G_0(FT)_\rho \neq 0$, we see from Theorem 3.8(c) that $T^{l,\rho}$ is not empty. Thus if $\ell = r$, $T^{l,\rho}$ must be $\{e\}$, since $T^{l,\rho}$ consists of l-regular elements. However, every eigenvalue of e acting on M is the identity, so $\lambda_{-1}(M)$ cannot be invertible by Proposition 4.1. This proves $\ell \neq r$. The residue characteristic of ρ cannot equal r by Proposition 4.1.

Suppose now that $M = \xi \oplus \xi^{-1}$. The eigenvalues in $\overline{F}$ of an (l-regular) element $h \in T^{l,\rho}$ are $\xi(h)$ and $\xi(h)^{-1}$. By Proposition 4.1, if ζ is the unique root of unity in $W(\overline{F})$ of the same order as $\xi(h)$ which has image $\xi(h)$ in $\overline{F}$, then $\zeta \neq 1$. Thus ζ is a primitive r-th root of unity. By the definition of the action of automorphisms of

T on T-modules, we have $\xi^{\sigma_a^{-1}}(h) = \xi(h^a) = \xi(h)^a$ for $a \in \mathbf{Z}$ prime to r. In view of (4.2), the first equality in (4.9) will follow if we can show

$$\frac{1}{(1-\zeta)\cdot(1-\zeta^{-1})} = \frac{(1-r)}{2r}\cdot \sum_{0<a<r} a\zeta^a + \frac{1}{r}\cdot \sum_{0<a<r} \frac{a(a-1)}{2}\zeta^a \tag{4.10}$$

whenever ζ is a primitive r-th root of unity. It is straightforward to check this identity by multiplying both sides by $2r(1-\zeta)(1-\zeta^{-1})$ and by then using that fact that $\sum_{0\le a<r}\zeta^a = 0$. The second equality in (4.9) is proved by adding the right side of (4.10) to the result of replacing ζ in (4.10) by ζ^{-1}, and by then simplifying using $\sum_{0<a<r} a(\zeta^a+\zeta^{-a}) = \sum_{0<a<r}(a+r-a)\zeta^a = -r$. □

5. Lefschetz Riemann Roch Theorems

Let G be a finite group. By a G-scheme X we will mean a flat equidimensional projective scheme over $\mathrm{Spec}(\mathbf{Z})$ with a right action of G. A $G-X$ sheaf F is a quasi-coherent sheaf of $\mathcal{O}_X$-modules such that the action of G is compatible with the action of G on $\mathcal{O}_X$ (see [**13**, §1.2]). We will call F coherent (resp. locally free) if F is coherent (resp. locally free) as an $\mathcal{O}_X$-module.

Define $K_0(G,X)$ (resp. $G_0(G,X)$) to be the Grothendieck group of coherent locally free $G-X$ sheaves (resp. coherent $G-X$ sheaves). The operation of taking exterior products over $\mathcal{O}_X$ makes $K_0(G,X)$ into a λ-ring, in the sense of [**7**], and $G_0(G,X)$ is a $K_0(G,X)$-module. If X is regular, (5.8) in [**13**] shows that the natural inclusion of categories induces an isomorphism

$$K_0(G,X) \cong G_0(G,X) \tag{5.1}$$

Given a G-morphism $\pi : X \to Y$ of G-schemes, we have a pull-back homomorphism

$$\pi^* : K_0(G,Y) \to K_0(G,X)$$

and if π is flat, a homomorphism

$$\pi^* : G_0(G,Y) \to G_0(G,X).$$

If π is proper, there is a direct image homomorphism

$$\pi_* : G_0(G,X) \to G_0(G,Y).$$

Via tensor products over $\mathbf{Z}$, $K_0(G,X)$ and $G_0(G,X)$ are modules for the ring $G_0^{\mathbf{Z}}(\mathbf{Z}G)$.

Suppose $f : X \to Y$ is a proper G-morphism between G-schemes X and Y, and that G acts trivially on Y. Suppose $\mathcal{F} \in K_0(G,X)$. We will refer to $f_*(\mathcal{F}) \in K_0(G,Y)$ as the equivariant Euler characterisic of $\mathcal{F}$. A prime ideal of $G_0^{\mathbf{Z}}(\mathbf{Z}G)$ is called I-adic if it contains the kernel of the homomomorphism $G_0^{\mathbf{Z}}(\mathbf{Z}G) \to \mathbf{Z}$ induced by taking ranks over $\mathbf{Z}$ of finitely generated $\mathbf{Z}$-modules. The Lefschetz Riemann Roch Theorem concerns the image of $f_*(\mathcal{F})$ in the localizations of $K_0(G,Y)$ at non I-adic primes ρ of $G_0^{\mathbf{Z}}(\mathbf{Z}G)$.

By Propositions 2.1 and 2.2, there is a prime ideal ℓ of $\mathbf{Z}$ and an ℓ-regular element $g \in G$ such that ρ is the prime ideal $\rho_{\ell,g}$ of Definition 2.3. The prime ℓ and the conjugacy class $C(g)$ of g are uniquely determined by ρ. Let X^ρ be the minimal closed G-subscheme of X containing the fixed point subscheme X^g. Then X^ρ is the union of the fixed point schemes $X^{g'}$ as g' ranges over $C(g)$, and X^ρ depends only on ρ. Let $X^{\rho,\mathrm{red}}$ be the reduction of X^ρ.

THEOREM 5.1. (Lefschetz Riemann Roch [**2**, Thm 3.1]). *Suppose ρ is a non I-adic prime of $G_0^{\mathbf{Z}}(\mathbf{Z}G)$, and that X and $X^{\rho,\mathrm{red}}$ are regular. The natural closed immersion $i = i_\rho : X^{\rho,\mathrm{red}} \to X$ is a regular embedding. The conormal bundle $\mathcal{N}^*$ of this embedding is a locally free $G - X^{\rho,\mathrm{red}}$ module. Therefore we can define*

$$\lambda_{-1}(\mathcal{N}^*) = \sum_{i\geq 0}(-1)^i\lambda^i(\mathcal{N}^*)$$

in $K_0(G, X^{\rho,\mathrm{red}})$, where the i-th λ operator λ^i is induced by taking i-th exterior powers. The class $\lambda_{-1}(\mathcal{N}^*)$ is invertible in the localization $K_0(G, X^{\rho,\mathrm{red}})_\rho$ of the $G_0^{\mathbf{Z}}(\mathbf{Z}G)$ algebra $K_0(G, X^{\rho,\mathrm{red}})$ at ρ. Finally, we have a commutative square

$$\begin{array}{ccc} K_0(G,X) & \xrightarrow{\lambda_{-1}(\mathcal{N}^*)^{-1}\cdot i^*} & K_0(G,X^{\rho,\mathrm{red}})_\rho \\ {\scriptstyle f_*}\downarrow & & \downarrow{\scriptstyle (f\circ i)_{*,\rho}} \\ K_0(G,Y) & \longrightarrow & K_0(G,Y)_\rho \end{array}$$

where G acts trivially on Y by assumption.

REMARK 5.2. For all G-schemes W, let $t_W : K_0(G,W) \to G_0(G,W)$ be the natural forgetful homomorphism. Suppose $f|_{X^{\rho,\mathrm{red}}} : X^{\rho,\mathrm{red}} \to Y$ factors as the composition of a proper morphism $g : X^{\rho,\mathrm{red}} \to Z$ followed by a closed immersion $h : Z \to Y$. Then $t_Y \circ f|_{X^{\rho,\mathrm{red}},*} : K_0(G, X^{\rho,\mathrm{red}}) \to G_0(G,Y)$ factors as the composition of $g_* : K_0(G, X^{\rho,\mathrm{red}}) \to G_0(G,Z)$ followed by $h_* : G_0(G,Z) \to G_0(G,Y)$. By the localization sequence, $j^* \circ h_* = 0$ if $j^* : G_0(G,Y) \to G_0(G,U)$ is the restriction homomorphism associated to the open immersion $j : U = Y - Z \to Y$. Thus $j^* \circ t_Y \circ f|_{X^{\rho,\mathrm{red}}} = 0$. Hence under the hypotheses of Theorem 5.1, we have $j_\rho^* \circ t_Y \circ f_* = 0$, where $j_\rho^* : G_0(G,Y)_\rho \to G_0(G,U)_\rho$ is the homomorphism induced by j.

REMARK 5.3. Suppose that the action of G on the generic fiber of X is étale. For each non-I-adic prime ρ of $G_0^{\mathbf{Z}}(\mathbf{Z}G)$, the subset $X^{\rho,\mathrm{red}}$ is then supported off of the generic fiber $Y_{\mathbf{Q}} = Y \otimes_{\mathbf{Z}} \mathbf{Q}$ of Y. Therefore, Remark 5.2 shows $f_*(K_0(G,X)) \subset K_0(G,Y)$ has trivial image in $G_0(G, Y_{\mathbf{Q}})_\rho$. Suppose in particular that $Y_{\mathbf{Q}} = \mathrm{Spec}(F)$ for some field F of characteristic 0. Then $G_0(G, Y_{\mathbf{Q}}) = R_F(G)$, and a character $\chi \in R_F(G)$ has trivial image in $R_F(G)_\rho$ for all non-I-adic primes if and only if $\chi(g) = 0$ for all non-trivial elements $g \in G$. Thus χ must be a multiple of the regular representation FG.

Following [**3**], the action of G on X over Y will be said to be tame if for each $x \in X$, the order of the inertia group of x in G is relatively prime to the residue characteristic of x. Suppose $Y = \mathrm{Spec}(A)$ is affine. Let $CT(AG)$ be the Grothendieck group of all finitely generated AG-modules which are cohomologically trivial as G-modules. It is shown in [**1**] and [**3**, §8] that when the action of G on X is tame, one has a refined Euler characteristic homomorphism $f_*^{CT} : K_0(G,X) \to CT(AG)$. In [**2**, Thm. 6.7], the following counterpart of Theorem 5.1 is shown.

THEOREM 5.4. *With the hypotheses of Theorem 5.1 , suppose $Y = \mathrm{Spec}(\mathcal{O}_N)$ where $\mathcal{O}_N$ is the ring of integers of a number field N. The forgetful homomorphism $K_0(\mathcal{O}_N G) \to CT(\mathcal{O}_N G)$ is then an isomorphism. Suppose that the action of G on X is tame, and that for $x \in X$, two elements of the inertia group of x which are conjugate in G generate the same subgroup of the inertia group. We then have a* *commutative square*

$$\begin{array}{ccc} K_0(G,X) & \stackrel{\lambda_{-1}(\mathcal{N}^*)^{-1}\cdot i^*}{\longrightarrow} & K_0(G,X^{\rho,\mathrm{red}})_\rho \\ f_*^{CT}\Big\downarrow & & \Big\downarrow (f\circ i)_{*,\rho}^{CT} \\ CT(\mathcal{O}_N G) & \longrightarrow & CT(\mathcal{O}_N G)_\rho \end{array}$$

where G acts trivially on $\mathcal{O}_N$ by assumption.

REMARK 5.5. In [**2**], more general versions of Theorems 5.1 and 5.4 are proved in which X and Y are assumed to be projective schemes over $\mathrm{Spec}(\mathcal{O}_K) = S$ when K is a number field. In these versions, one localizes at primes ρ of $K_0(G,S)$ rather than at primes of $G_0^{\mathbf{Z}}(\mathbf{Z}G)$. A version of f_*^{CT} when Y is not affine is discussed in [**3**].

6. Curves over rings of integers

In this section we will suppose $\mathcal{O}_N$ is the ring of integers of a number field N and $Y = \mathrm{Spec}(\mathcal{O}_N)$. We will let $f: X \to Y$ be the structure morphism of a flat regular projective curve X over Y. We will assume the fibers of X over closed fibers of Y are reduced with at most ordinary double points having tangent directions defined over Y. We will assume that $G = T$ is a group of prime order r acting on X over Y, and that the fixed point set X^G is zero-dimensional. If $x \in X^G$, the conormal bundle $\mathcal{N}^*_{X/x}$ on x of the embedding of x into X is the sheaf associated to the two-dimensional $k(x)$ vector space I_x/I_x^2, where I_x is the ideal sheaf of x in X and $k(x)$ is the residue field of x. Here I_x/I_x^2 is just the cotangent space to X at x. Let X_r^G be the subset of X^G not lying over the prime r of $\mathbf{Z}$.

LEMMA 6.1. *Suppose $x \in X_r^G$ and that $y = f(x)$ is the point of Y below x.*

a. *The natural map $k(y) \to k(x)$ is an isomorphism.*
b. *Let $\rho = \rho_{\mathbf{q},g}$ be the prime of $G_0^{\mathbf{Z}}(\mathbf{Z}G)$ specified in Definition 2.3 for a prime ideal $\mathbf{q} \neq r\mathbf{Z}$ of $\mathbf{Z}$ and a non-identity element g of G. The class $\lambda_{-1}(\mathcal{N}^*_{X/x})$ is invertible in the (non-zero) localization $G_0(k(x)G)_\rho$.*
c. *The point x is an ordinary double point on the fiber of X over y.*
d. *The $k(x)G$-module $\mathcal{N}^*_{X/x}$ is isomorphic to $\xi_x \oplus \xi_x^{-1}$, where $\xi: G \to k(x)^*$ is a non-trivial character of G.*

PROOF. Statement (a) follows from the fact that the inertia group of $x \in X_r^G \subset X^G$ is G. In part (b), since g generates G, the fixed point set X^g equals X^G as well as the minimal closed G-stable subset X^ρ of X containing X^g. Since X^G is zero dimensional, the reduction $X^{\rho,\mathrm{red}}$ of X^ρ is the union of G-stable closed points, one of which is x. By Theorem 5.1, the class $\lambda_{-1}(\mathcal{N}^*)$ is invertible in the localization $K_0(G,X^{\rho,\mathrm{red}})_\rho$ of the $G_0^{\mathbf{Z}}(\mathbf{Z}G)$-algebra $K_0(G,X^{\rho,\mathrm{red}})$ at ρ. Here

$$K_0(G,X^{\rho,\mathrm{red}})_\rho = \bigoplus_{x'\in X^G} K_0(G,\mathrm{Spec}(k(x')))_\rho = \bigoplus_{x'\in X^G} G_0(k(x')G)_\rho \tag{6.1}$$

where G acts trivially on $k(x')$ for $x' \in X^G$, and x is one of these x'. One has $G_0(k(x)G)_\rho \neq \{0\}$ by Theorem 3.8 since $\mathbf{q} \neq r\mathbf{Z}$ and $k(x)$ has characteristic different from r. Part (b) of Lemma 6.1 now follows from the fact that relative to the isomorphism (6.1) we have

$$\mathcal{N}^* = \bigoplus_{x'\in X^G} \mathcal{N}^*_{X/x'}. \tag{6.2}$$

To prove (c), let π be a uniformizing parameter of the local ring $\mathcal{O}_{Y,y}$. Since we have assumed the fiber $f^{-1}(y)$ is reduced, if x is non-singular on $f^{-1}(y)$ then π defines a non-zero element of $\mathcal{N}^*_{X/x}$ fixed by G. However, no such element can exist by Proposition 4.1 because we have shown (b). Finally, to prove (d), we have assumed that the (distinct) tangent directions at the ordinary double point x are defined over Y. Thus in the completion $\hat{\mathcal{O}}_{X,x}$ of the local ring $\mathcal{O}_{X,x}$, one has $\pi = f_1 \cdot f_2$ where $\{f_1, f_2\}$ is a set of generators for the maximal ideal $\hat{I}_x$ of $\hat{\mathcal{O}}_{X,x}$. Since $\hat{\mathcal{O}}_{X,x}$ is regular, it is a U.F.D.. The action of $g \in G$ on $\hat{\mathcal{O}}_{X,x}$ fixes π and takes irreducible elements of $\hat{\mathcal{O}}_{X,x}$ to irreducible elements. If $r > 2$, then g^2 also generates G, and g^2 must take f_i to $u_i f_i$ for some unit $u_i \in \hat{\mathcal{O}}^*_{X,x}$. Since $\hat{I}_x/(\hat{I}_x)^2$ is isomorphic to $\mathcal{N}^*_{X/x} = I_x/I_x^2$, this shows $\mathcal{N}^*_{X/x}$ is the direct sum of one-dimensional G-stable $k(x)$-subspaces spanned by the images of f_1 and f_2. This proves (d) when $r > 2$. If $r = 2$, then part (b) and Proposition 4.1 imply that both eigenvalues of g acting on the (semi-simple) $k(x)G$-module $\mathcal{N}^*_{X/x}$ are equal to -1. Hence (d) holds in this case as well. $\square$

DEFINITION 6.2. *Identify $K_0(G, Y)$ with the Grothendieck group $G_0^{\mathcal{O}_N}(\mathcal{O}_N G)$ of $\mathcal{O}_N G$-lattices. Let $\mathrm{Ind}_{\{e\}}^G K_0(\mathcal{O}_N)$ be the subgroup of $G_0^{\mathcal{O}_N}(\mathcal{O}_N G)$ generated by classes of modules of the form $\mathrm{Ind}_{\{e\}}^G P = \mathcal{O}_N G \otimes_{\mathcal{O}_N} P$ for some finitely generated projective $\mathcal{O}_N$-module P. Let*

$$t : K_0(G, X) \to \Big(\frac{G_0(\mathcal{O}_N G)}{\mathrm{Ind}_{\{e\}}^G K_0(\mathcal{O}_N)}\Big) \otimes_{\mathbf{Z}} \mathbf{Z}[\tfrac{1}{r}] \underset{def}{=} M(G, \mathcal{O}_N)$$

be the homomorphism induced by the direct image map $f_* : K_0(G, X) \to K_0(G, Y)$ together with the forgetful isomorphism $K_0(G, Y) = G_0^{\mathcal{O}_N}(\mathcal{O}_N G) \to G_0(\mathcal{O}_N G)$. Suppose the action of G on X is tame. Define $\mathrm{Ind}_{\{e\}}^G G_0(\mathcal{O}_N)$ to be the subgroup of classes in $CT(\mathcal{O}_N G)$ generated by classes of modules of the form $\mathrm{Ind}_{\{e\}}^G M = \mathcal{O}_N G \otimes_{\mathcal{O}_N} M$ for some finitely generated $\mathcal{O}_N$-module M. Let

$$t^{CT} : K_0(G, X) \to \Big(\frac{CT(\mathcal{O}_N G)}{\mathrm{Ind}_{\{e\}}^G G_0(\mathcal{O}_N)}\Big) \otimes_{\mathbf{Z}} \mathbf{Z}[\tfrac{1}{r}] \underset{def}{=} M(G, \mathcal{O}_N)^{CT}$$

be the homomorphism induced by the Euler characteristic map $f^{CT} : K_0(G, X) \to CT(\mathcal{O}_N G)$ defined just prior to Theorem 5.4.

THEOREM 6.3. *For $x \in X_r^G$, the character ξ_x of Lemma 6.1 defines a finite cohomologically trivial $\mathcal{O}_N G$-module via the natural homomorphism $\mathcal{O}_N G \to k(x)G$. In this way, ξ_x defines a class in $G_0(\mathcal{O}_N G)$ as well as a class in $Cl(\mathcal{O}_N G)$; we will denote each of these classes also by ξ_x. Let $1_{G,x}$ be the one-dimensional $k(x)$-module with trivial G-action, which we will regard as an $\mathcal{O}_N G$-module. With the notations of Definition 6.2, one has*

$$\begin{aligned} t(\mathcal{O}_X) &= \sum_{x \in X_r^G} \Big(\frac{(1-r)}{2r} \cdot \xi_x^{\Theta} + \frac{1}{r} \cdot \xi_x^{\Theta_2}\Big) \\ &= \sum_{x \in X_r^G} \frac{1}{2} \cdot \Big(\frac{(r-1)}{2} \cdot 1_{G,x} + \frac{1}{r} \cdot (\mathcal{N}^*_{X/x})^{\Theta_2}\Big) \end{aligned} \tag{6.3}$$

in $M(G, \mathcal{O}_N)$ where Θ and Θ_2 are the elements of the integral group ring of $\mathrm{Aut}(T)$ *defined in Definition 4.3. If the action of G on X is tame, then*

$$\begin{aligned} t^{CT}(\mathcal{O}_X) &= \sum_{x \in X_r^G} \Big(\frac{(1-r)}{2r} \cdot \xi_x^{\Theta} + \frac{1}{r} \cdot \xi_x^{\Theta_2} \Big) \\ &= \sum_{x \in X_r^G} \frac{1}{2} \cdot \Big(\frac{(r-1)}{2} \cdot 1_{G,x} + \frac{1}{r} \cdot (\mathcal{N}^*_{X/x})^{\Theta_2} \Big) \end{aligned} \tag{6.4}$$

in $M(G, \mathcal{O}_N)^{CT}$.

REMARK 6.4. The proof of the Theorem will show that for $x \in X_r^G$, the class

$$\frac{(r-1)}{2} \cdot 1_{G,x} + \frac{1}{r} \cdot (N^*_{X/x})^{\Theta_2}$$

in $G_0(k(x)G) \otimes_{\mathbf{Z}} \mathbf{Z}[\frac{1}{r}]$ is uniquely divisible by 2, which explains the meaning of the summands on the far right sides of (6.3) and (6.4).

PROOF. Let $\rho = \rho_{\mathbf{q},g}$ be the prime ideal of $G_0^{\mathbf{Z}}(\mathbf{Z}G)$ specified in Definition 2.3 for the prime ideal $\mathbf{q}$ of $\mathbf{Z}$ and the $\mathbf{q}$-regular element $g \in G$. Let 1_H be the one-dimensional trivial representation of the subgroup H of G. Suppose $g = e$. The element $z = r \cdot 1_G - \mathrm{Ind}_{\{e\}}^G 1_{\{e\}}$ of $G_0^{\mathbf{Z}}(\mathbf{Z}G)$ then lies in ρ, since the character of z vanishes on $g = e$. However,

$$z \cdot L = r \cdot L - \mathrm{Ind}_{\{e\}}^G 1_{\{e\}} \cdot L = r \cdot L - \mathrm{Ind}_{\{e\}}^G (res_G^{\{e\}} L)$$

for all $\mathcal{O}_N G$-lattices L, and $\mathrm{Ind}_{\{e\}}^G (res_G^{\{e\}} L) \in \mathrm{Ind}_{\{e\}}^G K_0(\mathcal{O}_N)$. Since the classes of $\mathcal{O}_N G$-lattices generate $M(G, \mathcal{O}_N)$, and the multiplication action of r on $M(G, \mathcal{O}_N)$ is invertible, we conclude that the multiplication action of z on $M(G, \mathcal{O}_N)$ is invertible. Since z lies in ρ if $g = e$, and $M(G, \mathcal{O}_N)_\rho$ is finitely generated over the local ring $G_0^{\mathbf{Z}}(\mathbf{Z}G)_\rho \otimes_{\mathbf{Z}} \mathbf{Z}[\frac{1}{r}]$, we conclude from Nakayama's Lemma that $M(G, \mathcal{O}_N)_\rho = 0$ if $g = e$.

Suppose now that ρ is a prime ideal for which $g \neq e$. In the notation of Theorem 5.1, the set $X^{\rho,\mathrm{red}}$ is the reduction of the fixed point set $X^g = X^G$, which is the union of finitely many closed points. By Theorem 5.1, the image of $f_*(\mathcal{O}_X)$ in $K_0(G, Y)_\rho = G_0^{\mathcal{O}_N}(\mathcal{O}_N G)_\rho$ is

$$f_*(\mathcal{O}_X)_\rho = \sum_{x \in X^{\rho,\mathrm{red}}} \lambda_{-1}(\mathcal{N}^*_{X/x})^{-1}. \tag{6.5}$$

By Lemma 4.4, only the x in the subset X_r^G of $X^G = X^\rho$ which do not lie over r contribute to the right hand side of (6.5), since $x \in X^G - X_r^G$ implies $G_0(k(x)G)_\rho = 0$. In view of Lemmas 6.1 and 4.4, the contribution to the right hand side of (6.5) from a point $x \in X_r^G$ corresponds to the the term associated to x in the sums appearing in (6.3). Hence the two sides of each equality in (6.3) have the same image in the localization of $M(G, \mathcal{O}_N)$ at each prime ρ of $G_0^{\mathbf{Z}}(\mathbf{Z}G)$ for which $g \neq e$, while the same is true for those ρ for which $g = e$ because $M(G, \mathcal{O}_N)_\rho = 0$ for such ρ. Hence the equalities in (6.3) must hold in $M(G, \mathcal{O}_N)$. One proves (6.4) similarly. □

COROLLARY 6.5. *Let $\mathcal{G} = G_0(G, \mathcal{O}_N)(\mathrm{tor})$ (resp. $\mathcal{G}[r^\infty] = G_0(G, \mathcal{O}_N)[r^\infty]$) be the subgroup of classes of $G_0(G, \mathcal{O}_N)$ of finite (resp. of r-power) order. Then $\mathcal{G}$*

contains the subgroup $\mathcal{S} = S(G, \mathcal{O}_N)$ of classes of finite $\mathcal{O}_N$ modules of order prime to r having trivial G-action. One has

$$f_*(\mathcal{O}_X) \in \mathcal{G}^{\Theta} + \mathcal{G}^{\Theta_2} + \mathcal{G}[r^\infty] + \mathrm{Ind}_{\{e\}}^G K_0(\mathcal{O}_N)$$

and

$$2 \cdot f_*(\mathcal{O}_X) \in \mathcal{S} + \mathcal{G}^{\Theta_2} + \mathcal{G}[r^\infty] + \mathrm{Ind}_{\{e\}}^G G_0(\mathcal{O}_N)$$

Proof: By the localization sequence, the torsion subgroup of $G_0(\mathcal{O}_N G)$ is generated by the classes of modules of finite order. Therefore Corollary 6.5 follows from Theorem 6.3.

In a similar way one can prove:

COROLLARY 6.6. *The classgroup $Cl(\mathcal{O}_N G)$ may be defined to be the torsion subgroup of $CT(\mathcal{O}_N G)$, where the forgetful map $K_0(\mathcal{O}_N G) \to CT(\mathcal{O}_N G)$ is an isomorphism. Let $Cl(\mathcal{O}_N G)[r^\infty]$ be the r-Sylow subgroup of $Cl(\mathcal{O}_N G)$. The Swan subgroup $\mathcal{S}_{CT}$ of $Cl(\mathcal{O}_N G)$ is the subgroup of $CT(\mathcal{O}_N G)$ generated by classes of finite $\mathcal{O}_N$-modules of order prime to r which have trivial action by G. If the action of G on X is tame, then*

$$f_*^{CT}(\mathcal{O}_X) \in Cl(\mathcal{O}_N G)^{\Theta} + Cl(\mathcal{O}_N G)^{\Theta_2} + Cl(\mathcal{O}_N G)[r^\infty] + \mathrm{Ind}_{\{e\}}^G G_0(\mathcal{O}_N)$$

and

$$2 \cdot f_*(\mathcal{O}_X) \in \mathcal{S}_{CT} + Cl(\mathcal{O}_N G)^{\Theta_2} + Cl(\mathcal{O}_N G)[r^\infty] + \mathrm{Ind}_{\{e\}}^G G_0(\mathcal{O}_N)$$

REMARK 6.7. The first Stickelberger ideal of $\mathbf{Z}[\mathrm{Aut}(G)]$ is defined to be

$$S = \mathbf{Z}[\mathrm{Aut}(G)] \cap (\tfrac{\Theta}{r}) \cdot \mathbf{Z}[\mathrm{Aut}(G)].$$

Define $Cl^0(O_N G)$ to be the kernel of the homomorphism $Cl(O_N G) \to Cl(O_N)$ which is induced by restriction from G to the trivial subgroup of G. In [**10**], McCulloh shows that if N contains a primitive r-th root of unity, then $Cl^0(\mathcal{O}_N G)^S$ is the subgroup of classes of $Cl(\mathcal{O}_N G)$ of the form $[\mathcal{O}_L] - [N : \mathbf{Q}][\mathcal{O}_N G]$, were L ranges over all finite cyclic tamely ramified degree r-extensions of N together with a choice of isomorphism between G and $Gal(L/N)$. (See [**11**] for the generalization of this result to all number fields N and all abelian groups G.) Here $[\mathcal{O}_L] = h_*^{CT}(\mathcal{O}_W)$ if $h : W = \mathrm{Spec}(\mathcal{O}_L) \to \mathrm{Spec}(\mathcal{O}_N) = Y$ is the structure morphism. Thus Corollary 6.6 is a partial counterpart of McCulloh's result for dimension two schemes. However, McCulloh's resolvent theoretic methods yield stronger results for dimension 1 schemes than those which can be obtained by Theorem 5.1. For example, Theorem 5.1 would imply only that for L as above, $[\mathcal{O}_L]$ lies in $Cl(\mathcal{O}_N G)^{\Theta} + Cl(\mathcal{O}_N G)[r^\infty] + \mathrm{Ind}_{\{e\}}^G G_0(\mathcal{O}_N)$.

COROLLARY 6.8. *Suppose $N = \mathbf{Q}$, so $\mathcal{O}_N = \mathbf{Z}$. Let $< \mathbf{Z}G >$ be the subgroup of $G_0(\mathbf{Z}G)$ (resp. $CT(\mathbf{Z}G)$) generated by the class of $\mathbf{Z}G$. Let $\mathcal{G}$ (resp. $\mathcal{G}[r^\infty]$) be the subgroup of classes in $G_0(\mathbf{Z}G)$ of finite (resp. finite r-power) order. We have*

$$f_*(\mathcal{O}_X) \in \mathcal{G}^{\Theta_2} + \mathcal{G}[r^\infty] + < \mathbf{Z}G >$$

on identifying $K_0(G, Y) = K_0(G, \mathrm{Spec}(\mathbf{Z}))$ with $G_0^{\mathbf{Z}}(\mathbf{Z}G) = G_0(\mathbf{Z}G)$. The class group $Cl(\mathbf{Z}G)$ may be defined as the torsion subgroup of $CT(\mathbf{Z}G)$. Let $Cl(\mathbf{Z}G)[r^\infty]$ be the r-Sylow subgroup of $Cl(\mathbf{Z}G)$. If the action of G on X is tame, then

$$f_*^{CT}(\mathcal{O}_X) \in Cl(\mathbf{Z}G)^{\Theta_2} + Cl(\mathbf{Z}G)[r^\infty] + < \mathbf{Z}G > .$$

PROOF. By [**5**, Thm. 39.21 and Th 50.2], the groups $\mathcal{G}$ and $Cl(\mathbf{Z}G)$ may be identified with the ideal class group of the field $\mathbf{Q}(\zeta_r)$ when ζ_r is a primitive r-th root of unity. The first Stickelberger element Θ annihilates this ideal class group by [**14**, Thm. 6.10]. Corollary 6.8 follows from this and Corollary 6.5. $\square$

REMARK 6.9. Suppose $r > 3$. In a later paper we will show that modulo $Cl(\mathbf{Z}G)[r^\infty] + < \mathbf{Z}G >$ each class in $Cl(\mathbf{Z}G)^{\Theta_2}$ arises as $f_*^{CT}(\mathcal{O}_X)$ for some X having a tame action of G. We will also show that there are primes r for which $Cl(\mathbf{Z}G)^{\Theta_2}$ has a non-trivial element of order prime to r. This will show there are X having a tame action of G for which $f_*^{CT}(\mathcal{O}_X)$ is not in $< \mathbf{Z}G >$.

References

[1] Chinburg, T. and Erez, B.: *Equivariant Euler-Poincaré characteristics and tameness,* in Proc. Journées Arithmétiques 1991, Astérisque Soc. Math de France, Paris (1992), 179–194.

[2] Chinburg, T., Erez, B., Pappas, G. and Taylor, M. J.: *Riemann-Roch Type Theorems for Arithmetic Schemes with a Finite Group Action,* J. für die reine und angew. Math. **489** (1997), 151–187.

[3] Chinburg, T., Erez, B., Pappas, G. and Taylor, M. J.: *Tame actions of group schemes: integrals and slices,* Duke Math. J. **82:2** (1996), 269–308.

[4] Curtis, C. and Reiner, R.: *Methods of Representation Theory.* vol. I, Wiley, U.S.A. (1981).

[5] Curtis, C. and Reiner, R.: *Methods of Representation Theory.* vol. II, Wiley, U.S.A. (1987).

[6] Erez, B.: *Geometric trends in Galois module theory,* to appear in the proceedings of the 1996 Durham conference on arithmetic geometry.

[7] Fulton, W. and Lang, S.: *Riemann-Roch algebra,* Springer-Verlag, New York Berlin Heidelberg Tokyo, (1985).

[8] Pappas, G.: *Galois module structure and the γ-filtration,* preprint (1997).

[9] Lang, S.: *Algebra,* second ed., Addison-Wesley, U.S.A. (1984).

[10] McCulloh, L.: *A Stickelberger condition on Galois module structure for Kummer extensions of prime degree,* in Algebraic Number Fields, ed. A. Fröhlich, Academic Press, (1977).

[11] McCulloh, L.: *Galois module structure of abelian extensions,* J. für die reine und angew. Math. **375/376** (1987), 259–306.

[12] Serre, J. P.: *Linear Representations of Finite Groups.* Springer-Verlag, U.S.A. (1977).

[13] Thomassen, R.: *Algebraic K-theory of group scheme actions,* in Algebraic topology and algebraic K-theory, Ann. of Math Studies, vol. 113, Princeton Univ. Press, 539–563.

[14] Washington, L.: *Introduction to Cyclotomic Fields,* Springer-Verlag, New York Heidelberg Berlin (1982).

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF PENNSYLVANIA, PHILADELPHIA PENNSYLVANIA 19104, U. S. A.

E-mail address: `ted@math.upenn.edu`

LABORATOIRE DE MATHÉMATIQUES PURES, UNIVERSITÉ BORDEAUX 1, 33405 TALENCE CEDEX, FRANCE

E-mail address: `erez@math.u-bordeaux.fr`

DEPARTMENT OF MATHEMATICS, PRINCETON UNIVERSITY, PRINCETON, N. J. 08544-1000, U. S. A.

Current address: Department of Mathematics, Michigan State University, East Lansing, Michigan 48824, U. S. A.

E-mail address: `pappas@math.Princeton.EDU`

DEPARTMENT OF MATHEMATICS. U. M. I. S. T., P. O. BOX 88, MANCHESTER M60 1QD, UNITED KINGDOM

E-mail address: `Martin.Taylor@umist.ac.uk`

This page intentionally left blank

http://dx.doi.org/10.1090/conm/224/03193

Contemporary Mathematics
Volume **224**, 1999

INVARIANT STABLE BUNDLES OVER MODULAR CURVES $X(p)$

Igor V. Dolgachev

Introduction.

Let X be a smooth projective algebraic curve of genus $g > 1$ and G be the group of its automorphisms. The problem is to describe vector bundles on X which are invariant with respect to the action of G on X. In this paper we address this problem in the case when the curve X is the modular curve $X(p)$ obtained as a compactification of the quotient of the upper-half plane $H = \{z \in \mathbb{C} : \Im z > 0\}$ by the action of the principal congruence subgroup $\Gamma(p) = \{A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z}) : A \equiv I \mod p\}$. We shall assume that p is a prime number > 5 although some of our results are true for any p not divisible by 2 and 3. Here the group G is isomorphic to the group $\mathrm{PSL}(2,\mathbb{F}_p)$. Also we restrict ourselves with stable bundles. In other words, we are trying to describe the set of fixed points for the natural action of G on the moduli space of rank r stable vector bundles on $X(p)$. The case of rank 1 bundles is rather easy and the answer can be found in **[AR]**. The group of G-invariant line bundles on $X(p)$ is generated by a line bundle λ of degree $\frac{p^2-1}{24}$ which is a $(2p-12)$-th root of the canonical bundle. For the future use we generalize this result to any Riemann surface X with a finite group G of its automorphisms such that $X/G \cong \mathbb{P}^1$. This result must be known to experts but I could not find a reference. When the determinant of the bundle is trivial, we are able to relate our problem to the problem of classifying unitary representations of the fundamental group of the Brieskorn sphere $\Sigma(2,3,p)$, that is, the link of the singularity $x^2+y^3+z^p = 0$. Applying some known results from differential topology we prove that there exist exactly $2n$ rank 2 G-invariant stable bundles with trivial

1991 *Mathematics Subject Classification.* Primary 14H60, 14H45, 30F35; Secondary 11F11, 14L30, 57M05.

Key words and phrases. G-bundles, Riemann surfaces, modular curves.

Research supported in part by NSF grant DMS 9623041.

determinant and $3n^2 \pm n$ rank 3 (if $p \neq 7$) G-invariant stable bundles with trivial determinant on $X(p)$, where $p = 6n \pm 1$. Note that the determinant of a stable G-invariant rank 2 bundle is an even multiple of λ. So, after twisting by a line bundle, we obtain a G-invariant bundle with trivial determinant.

Even in the case of rank 2 and 3 our results are still unsatisfactory since we were able to give a geometric construction of all of these bundles only in the case $p = 7$. Some of the bundles we discuss are intrinsically related to the beautiful geometry of modular curves which goes back to Felix Klein.

I would like to thank the organizers of the conference for giving me the opportunity to revisit Korea. This paper owes much to the work of Allan Adler and correspondence with him. The book **[AR]** was a great inspiration for writing this paper. Finally I would like to thank Hans Boden and Nikolai Saveliev for coaching me in the theory of Casson invariant of 3-dimensional manifolds.

1. G-invariant and G-linearized stable vector bundles.

Let X be a compact Riemann surface of genus g. For each $r > 0$ there is the moduli space $\mathcal{M}_X(r)$ of semi-stable rank r vector bundles over X. Assume that a finite group G acts holomorphically on X (not necessary faithfully). By functoriality G acts holomorphically on $\mathcal{M}_X(r)$ and we denote by $\mathcal{M}_X(r)^G$ the subvariety of fixed points of this action. If $[E] \in \mathcal{M}_X(r)$ is the isomorphism class of a stable bundle, then $[E] \in \mathcal{M}_X(r)^G$ if and only if E is G-*invariant*, i.e. for any $g \in G$, there is an isomorphism of vector bundles

$$\phi_g : g^*(E) \to E.$$

If $[E] \in \mathcal{M}_X(r)$ is the point representing the equivalence class of a semi-stable but not stable bundle E, then it is known that E is equivalent to a decomposable bundle $E' = E_1 \oplus \ldots \oplus E_k$ (in the sense $[E] = [E']$), where all E_i are stable of the same slope $\mu(E_i) = \frac{\deg E_i}{rkE_i}$ as E (see **[Se]**). Then $[E] \in \mathcal{M}_X(r)^G$ if and only if E' is G-invariant. In the following we will always assume that E is either stable or is decomposable as above. Assume that the collection $\phi = \{\phi_g\}_{g\in G}$ can be chosen in such a way that for any $g, g' \in G$

$$\phi_{g\circ g'} = \phi_{g'} \circ g'^*(\phi_g).$$

Then we say that E admits a G-linearization, and the pair (E, ϕ) is called a G-*linearized vector bundle.* Of course, in down-to-earth terms this means that the action of G on X lifts to an action on the total space of E which is linear on each fibre and a G-linearization is such a lift. One naturally defines the notion of a morphism of G-linearized vector bundles, and, in particular, one defines the set $\mathcal{M}_X(G;r)$ of isomorphism classes of G-linearized semi-stable rank r vector bundles over G. There is a natural forgetting map

$$e : \mathcal{M}_X(G;r) \to \mathcal{M}_X(r)^G.$$

Proposition 1.1. *Let E be a stable G-invariant rank r bundle on X. One can assign to E an element*

$$c(E) \in H^2(G, \mathbb{C}^*)$$

such that E belongs to the image of the map e if and only if $c(E) = 1$. Here the cohomology group is taken with respect to the trivial action of G on the group $\mathbb{C}^*$.

Proof. This is of course rather standard. Let $\phi_g : g^*(E) \to E, g \in G$, be some set of isomorphisms defined by E. We have

$$\phi_{gg'} = c_{g,g'}\phi_{g'} \circ g'^*(\phi_g)$$

for some $c_{g,g'} \in \mathrm{Aut}(E)$. Since E is stable, $\mathrm{Aut}(E)$ consists only of homotheties, so that $\mathrm{Aut}(E) = \mathbb{C}^*$. It is easy to check that $\{c_{g,g'}\}_{g,g'\in G}$ defines a 2-cocycle of G with coefficients in the group $\mathbb{C}^*$. Its cohomology class $c(E)$ does not depend on the choice of $\{\phi_g\}_{g\in G}$. It is trivial if and only if $c_{g,g'} = c_{g'} \circ g'^*(c_g)$ for some map $c : G \to \mathrm{Aut}(E), g \to c_g$. Replacing ϕ_g with $\psi_g = c_g \circ \phi_g$, we get

$$\psi_{gg'} = \psi_{g'} \circ g'^*(\psi_g).$$

The set $\{\psi_g\}_{g\in G}$ defines a G-linearization on E. Clearly for any E in the image of e, we have $c(E) = 1$. This checks the assertion.

Corollary 1.2. *Assume G is a perfect group (i.e. coincides with its commutator subgroup). Let*

$$1 \to H^2(G, \mathbb{C}^*) \to \tilde{G} \to G \to 1$$

be the universal central extension of the group G defined by the group of Schur multipliers $H^2(G, \mathbb{C}^*)$. Consider the action of $\tilde{G}$ on X defined by the action of G on X. Then each stable G-invariant bundle E admits a $\tilde{G}$-linearization.

Proof. Use that

$$H^2(\tilde{G}, \mathbb{C}^*) = 1.$$

Now let us describe the fibres of the map e. Let (E, ϕ) be a G-linearized semi-stable bundle. Consider the direct product $G \times \mathrm{Aut}(E)$ which acts on X via the action of G on X and the trivial action of $\mathrm{Aut}(E)$ on X. Obviously

$$E \in \mathcal{M}_X(r)^{G\times \mathrm{Aut}(E)}.$$

Proposition 1.3. *Let E be a G-linearized vector bundle and let $\{\phi_g\}_{g\in G}$ be the family of isomorphisms $\phi_g : g^*(E) \to E$ defining its linearization. For each $(g, \alpha) \in G \times \mathrm{Aut}(E)$ set*

$$\phi_{(g,\alpha)} = \alpha^{-1} \circ \phi_g : (g, \alpha)^*(E) = g^*(E) \to E \to E.$$

Then the set of isomorphisms of vector bundles $\phi_{(g,\alpha)}$ defines a $G \times \mathrm{Aut}(E)$-linearization of E if and only if, for any $g \in G$ and any $\alpha \in \mathrm{Aut}(E)$,

$$\phi_g \circ g^*(\alpha) = \alpha \circ \phi_g. \tag{1.1}$$

Proof. It is immediately verified that

$$\phi_{(g',\alpha')} \circ g'^*(\phi_{(g,\alpha)}) = \alpha'^{-1} \circ \phi_{g'} \circ g'^*(\alpha^{-1}) \circ g'^*(\phi_g).$$

This is equal to

$$\phi_{(gg',\alpha\circ\alpha')} = \alpha'^{-1} \circ \alpha^{-1} \circ \phi_{gg'} = \alpha'^{-1} \circ \alpha^{-1} \circ \phi_{g'} \circ g'^*(\phi_g)$$

if and only if, for any g', α,

$$\alpha^{-1} \circ \phi_{g'} = \phi_{g'} \circ g'^*(\alpha^{-1}).$$

This is of course equivalent to the assertion of the proposition.

Definition A G-linearization $\phi = \{\phi_g\}_{g\in G}$ on $E \in \mathcal{M}_X(G;r)$ is called *distinguished* if ϕ satisfies the condition (1.1) from Proposition 1.3.

Theorem 1.4. *Let $(E,\phi) \in \mathcal{M}_X(G;r)$ be a G-linearized bundle with distinguished linearization. Then any G-linearization ψ on E is equal to*

$$\psi_g = \lambda(g^{-1}) \circ \phi_g,$$

where

$$\lambda : G \to \mathrm{Aut}(E)$$

is a homomorphism of groups.

Proof. First we check that for any homomorphism of groups $\lambda : G \to \mathrm{Aut}(E)$ the collection $\{\psi_g = \phi_g \circ \lambda(g)\}_{g\in G}$ defines a G-linearization of E. This is straightforward:

$$\psi_{gg'} = \lambda((gg')^{-1})\phi_{gg'} = \lambda(g'^{-1}) \circ \lambda(g^{-1}) \circ \phi_{g'} \circ g'^*(\phi_g) =$$

$$\lambda(g'^{-1}) \circ \phi_{g'} \circ g'^*(\lambda(g^{-1})) \circ g'^*(\phi_g) = \psi_{g'} \circ g'^*(\psi_g).$$

So it is checked. Now suppose we have another G-linearization $\psi = \{\psi_g\}_{g\in G}$ on E. Then

$$\phi_g \circ \psi_g^{-1} : E \to g^*(E) \to E$$

is an automorphism of E. Thus $\psi_g = \lambda(g^{-1}) \circ \phi_g$ for some automorphism $\lambda(g^{-1})$ of E. Now reversing the previous computations we check that the map $g \to \lambda(g)$ is a homomorphism of groups.

Example 1.5. Every G-linearization on a stable bundle is distinguished and there is a natural bijection

$$e^{-1}(e((E,\phi))) \to \mathrm{Hom}(G, \mathbb{C}^*).$$

Example 1.6. Let $E = \mathcal{O}_X^r$ be the trivial bundle. It is semi-stable but not stable. Consider the *trivial G-linearization* on E by setting for each $(x,v) \in g^*(E)_x = E_{g\cdot x}$

$$\phi_g(x,v) = (g\cdot x, v).$$

Obviously it is distinguished, and

$$e^{-1}(\mathcal{O}_X^r) = \mathrm{Hom}(G, GL(r,\mathbb{C})).$$

2. Line bundles

Let us consider the special case of line bundles. Here we can say much more. First let us denote by $\mathrm{Pic}(X)^G$ the group of G-invariant line bundles and by $\mathrm{Pic}(G;X)$ the group of G-linearized line bundles. The latter group has the following simple interpretation in terms of G-invariant divisors:

Proposition 2.1. *The group $Pic(G;X)$ is isomorphic to the group of G-invariant divisors on X modulo the subgroup of divisors of G-invariant meromorphic functions.*

Proof. Let $D = \sum_{x\in X} n_x x$ be a G-invariant divisor. This means that, for any $g \in G$,

$$D = g^*(D) = \sum_{x\in X} n_x g^{-1}(x).$$

Let L_D be the line bundle whose sheaf of sections is the invertible sheaf $\mathcal{O}_X(D)$ whose set of sections over an open subset U is equal to $\{f \in \mathbb{C}(X) : \mathrm{d}iv(f) + D \geq 0 \text{ after restriction to } U\}$. The group G acts naturally on the field $\mathbb{C}(X)$ of meromorphic functions on X. If $f \in \mathbb{C}(X)$ is considered as a holomorphic map $f \to \mathbb{P}^1$ then the image ${}^g f$ of f under $g \in G$ is equal to the composition $f \circ g^{-1}$. Since $({}^g f) = g^*((f))$ we have a natural isomorphism of invertible sheaves $\mathcal{O}_X(D) \to \mathcal{O}_X(g^*(D))$. It defines an isomorphism of line bundles $\phi_g : g^*(L_D) \to L_D$ which satisfies $\phi_{g'\circ g} = \phi_g \circ g^*(\phi_{g'})$. This makes L_D a G-linearized line bundle. If L_D is equal to zero in $\mathrm{Pic}(X)$ then $D = (f)$ for some $f \in \mathbb{C}(X)$ with the property $({}^g f) = (f)$ for all $g \in G$. The ratio $\chi_g = {}^g f/f$ is a nonzero constant, and the map $G \to \mathbb{C}^*$ defined by χ_g is a homomorphism of groups. It defines a linearization on L_D. It is trivial if and only if $f \in \mathbb{C}(X)^G$. This shows that the group $\mathrm{D}iv(X)^G/\mathrm{d}iv(\mathbb{C}(X)^G)$ of G-invariant divisors modulo principal divisors of the form $(f), f \in \mathbb{C}(X)^G$, is mapped isomorphically onto a subgroup of $\mathrm{Pic}(G;X)$. I claim that the image is the whole group. In fact, let L be a G-linearized line bundle and $\phi_g : g^*(L) \to L$ be the set of isomorphisms satisfying $\phi_{gg'} = \phi_g \circ g^*(\phi_{g'})$ which define the linearization. Then ϕ_g is defined by a meromorphic function f_g such that $g^*(D) = D + (f_g)$. We have $f_{g'\circ g} = {}^g f_{g'} f_g$ so that $(f_g)_{g\in G}$ is a one-cocycle of G with values in $\mathbb{C}(X)^*$. By Hilbert's Theorem 90 this cocycle must be trivial. Hence we can write $f_g = {}^g a/a$ for some $a \in \mathbb{C}(X)$. Replacing D with $D' = D - (a)$ we obtain $g^*(D') = D'$ for any $g \in G$. This shows that $L_D \cong L_{D'}$ arises from a G-invariant divisor. This proves the assertion.

Proposition 2.2. *There is an exact sequence of abelian groups*

$$0 \to \mathrm{Hom}(G, \mathbb{C}^*) \to \mathrm{Pic}(G;X) \to \mathrm{Pic}(X)^G \to H^2(G, \mathbb{C}^*) \to 0.$$

Proof. The only non-trivial assertion here is the surjectivity of the map

$$e : \mathrm{Pic}(X)^G \to H^2(G, \mathbb{C}^*).$$

To prove it we need a cohomological interpretation of the exact sequence. We use the following two spectral sequences with the same limit (see **[Gr]**, p. 200):

$${}'E_2^{pq} = H^p(G, H^q(X, \mathcal{O}_X^*)) \Rightarrow H^n(G; X, \mathcal{O}_X^*),$$

$${}''E_2^{pq} = H^p(Y, R^q\pi_*^G(\mathcal{O}_X^*)) \Rightarrow H^n(G; X, \mathcal{O}_X^*).$$

Here $\pi : X \to Y = X/G$ is the canonical projection and the group $H^1(G; X, \mathcal{O}_X^*)$ is isomorphic to $\mathrm{Pic}(G;X)$. The first spectral sequence gives the exact sequence

$$0 \to \mathrm{Hom}(G, \mathbb{C}^*) \to \mathrm{Pic}(G;X) \to \mathrm{Pic}(X)^G \to H^2(G, \mathbb{C}^*) \to H^2(G; X, \mathcal{O}_X^*).$$

In order to show that $H^2(G; X, \mathcal{O}_X^*) = 0$ we use the second spectral sequence. We have

$${}'E_2^{20} = H^2(Y, \pi_*^G(\mathcal{O}_X^*)) = H^2(Y, \mathcal{O}_X^*) = 0,$$

as it follows from the exponential exact sequence $0 \to \mathbb{Z} \to \mathcal{O}_Y \to \mathcal{O}_Y^* \to 0$.

$$'E_2^{11} = H^1(Y, R^1\pi_*^G(\mathcal{O}_X^*)) = 0$$

since $R^1\pi_*^G(\mathcal{O}_X^*)$ is concentrated at a finite set of branch points of π.

$$'E_2^{02} = H^0(Y, R^2\pi_*^G(\mathcal{O}_X^*)) = 0$$

since $R^2\pi_*^G(\mathcal{O}_X^*)_y \cong H^2(G_x, \mathbb{C}^*)$, where G_x is the isotropy group of a point $x \in \pi^{-1}(y)$, and the latter group is trivial because G_x is a cyclic group. All of this shows that $H^2(G; X, \mathcal{O}_X^*) = 0$.

Corollary 2.3. *Let $Div(X)^G$ be the group of G-invariant divisors and $P(X)^G$ be its subgroup of principal G-invariant divisors. Then $\mathrm{Div}^G(X)/P(X)^G$ is isomorphic to a subgroup of $\mathrm{Pic}(X)^G$ and the quotient group is isomorphic to $H^2(G, \mathbb{C}^*)$.*

Now let us use the second spectral sequence for the map $\pi : X \to X/G$ to compute $\mathrm{Pic}(G; X)$ more explicitly. Let $y_1, \dots, y_n$ be the branch points of π and $e_1, \dots, e_n$ be the corresponding ramification indices. For each point $x \in \pi^{-1}(y_i)$ the stabilizer subgroup G_x is a cyclic group of order e_i. The exact sequence arising from the second spectral sequence looks as follows:

$$0 \to \mathrm{Pic}(Y) \to \mathrm{Pic}(G; X) \to \oplus_{i=1}^n \mathbb{Z}/e_i\mathbb{Z} \to 0. \tag{2.1}$$

Here the composition of the first homomorphism with the forgetting map $e : \mathrm{Pic}(G; X) \to \mathrm{Pic}(X)$ is the natural map $\pi^* : \mathrm{Pic}(Y) \to \mathrm{Pic}(X)$. The second homomorphism is defined by the local isotropy representation $\rho_{x_i} : G_{x_i} \to \mathbb{C}^*$ defined by the G-linearized bundle L. Here we fix some x_i in each fibre $\pi^{-1}(y_i)$. Let $D_i = \pi^{-1}(y_i)$ considered as a reduced G-invariant divisor on X. Let us assume that

$$Y = \mathbb{P}^1.$$

Then the isomorphism classes s_i of $L_i = L_{D_i}, i = 1, \dots, n$, generate $\mathrm{Pic}(G; X)$ and satisfy the relations $e_1 s_1 = \ldots = e_n s_n$. This easily implies that

$$\mathrm{Pic}(G; X) \cong \mathbb{Z} \oplus \mathbb{Z}/d_1 \oplus \mathbb{Z}/(d_2/d_1) \oplus \ldots \oplus \mathbb{Z}/(d_{n-1}/d_{n-2}), \tag{2.2}$$

where

$$d_1 = (e_1, \dots, e_n), d_2 = (\dots, e_i e_j, \dots,), \dots, d_{n-1} = (e_1 \cdots e_{n-1}, \dots, e_2 \cdots e_n).$$

To define a generator of the free part of $\mathrm{Pic}(G; X)$ we use the Hurwitz formula for the canonical line bundle of X:

$$K_X = \pi^*(K_Y) \otimes \left(\otimes_{i=1}^n L_i^{e_i - 1} \right).$$

We know that $\mathrm{Pic}(Y)$ is generated by the isomorphism class α of the line bundle L_y corresponding to the divisor $D = 1 \cdot y$ where $y \in Y$. Then $\pi^*(\alpha) = N\gamma$, where N is a positive integer and γ generates $\mathrm{Pic}(G; X)$ modulo the torsion subgroup. Applying (2.1) we obtain that

$$\mathbb{Z}/N \oplus \mathrm{Tors}(\mathrm{Pic}(G; X)) \cong \oplus_{i=1}^n \mathbb{Z}/e_i\mathbb{Z},$$

and hence

$$N = \frac{e_1 \cdots e_n}{(e_1 \cdots e_{n-1}, \dots, e_2 \cdots e_n)} = l.c.m.(e_1, \dots, e_n).$$

Now, switching to the additive notation,

$$e_1 \dots e_n K_X = e_1 \dots e_n \pi^*(-2\alpha) + \sum_{i=1}^{n} (e_i - 1) e_1 \dots e_n L_i =$$

$$= -2e_1 \dots e_n N\gamma + \sum_{i=1}^{n} (e_i - 1) \frac{e_1 \dots e_n}{e_i} N\gamma = e_1 \dots e_n (n - 2 - \sum_{i=1}^{n} e_i^{-1}) N\gamma.$$

This implies that

$$K_X = \frac{(n-2)e_1 \dots e_n - e_1 \cdots e_{n-1} - \dots e_2 \cdots e_n}{(e_1 \cdots e_{n-1}, \dots, e_2 \cdots e_n)} \gamma =$$

$$l.c.m(e_1, \dots, e_n)(n - 2 - \sum_{i=1}^{n} \frac{1}{e_i})\gamma. \tag{2.3}$$

Now we are ready to compute $\mathrm{Pic}(X(p))^G$, where $X(p)$ is the modular curve of level p and $G = \mathrm{PSL}(2, \mathbb{F}_p)$.

The following result is contained in **[AR]**, Corollaries 24.3 and 24.4. However, keeping in mind some possible applications to more general situations, we shall give it another proof which is based on the previous discussion.

Theorem 2.4. *Assume $p \geq 5$ is prime. Let $G = \mathrm{PSL}(2, \mathbb{F}_p)$. Then*

$$\mathrm{Pic}(X(p))^G = \mathrm{Pic}(\mathrm{SL}(2, \mathbb{F}_p); X(p)) = \mathbb{Z}\lambda,$$

where

$$\lambda^{2p-12} = K_{X(p)}$$

and

$$\deg \lambda = \frac{p^2 - 1}{24}.$$

Moreover, $\mathrm{Pic}(G; X(p))$ *is the subgroup of* $\mathrm{Pic}(X(p))^G$ *generated by* λ^2.

Proof. We use that the map $\pi : X(p) \to X(p)/\mathrm{PSL}(2, \mathbb{F}_p)$ is ramified over three points with ramification indices $2, 3$ and p. It follows from the previous computation that $\mathrm{Pic}(G; X(p))$ is a free cyclic group generated by a $(p-6)$-th root of the canonical class. We use Proposition 2.1 and well-known facts that $\mathrm{Hom}(G, \mathbb{C}^*) = \{1\}, H^2(G, \mathbb{C}^*) \cong \mathbb{Z}/2$. This gives us that $\mathrm{Pic}(X(p))^G = \mathrm{Pic}(G; X(p))$ is a subgroup of index 2 in $\mathrm{Pic}(X(p))^G$. It remains to show that $\mathrm{Pic}(X(p))^G$ does not contain 2-torsion elements. Let $L \in \mathrm{Pic}(X)^G_n$ be a torsion element of order n in $\mathrm{Pic}(X)^G$. Let μ_n be the constant sheaf of n-th roots of unity. The Kummer sequence

$$0 \to \mu_n \to \mathcal{O}_X^* \to \mathcal{O}_X^* \to 0$$

implies that $\mathrm{Pic}(X)^G_n = H^1(X, \mu_n)^G$. Replacing $\mathcal{O}_X^*$ with μ_n in the proof of Proposition 2.2, we obtain that all arguments extend to this situation except that we cannot use that $H^2(G_x, \mu_n) = 0$. As a result we obtain an exact sequence

$$0 \to \mathrm{Pic}(G; X)_2 \to \mathrm{Pic}(X)^G_2 \to H^2(G, \mu_2) \to H^2(G_{x_1}, \mu_2).$$

The last homomorphism here is the restriction homomorphism for group cohomology. Here x_1 is a ramification point of index 2. The exact sequence

$$0 \to \mu_2 \to \mathbb{C}^* \to \mathbb{C}^* \to 0$$

shows that $H^2(G,\mu_2) = H^2(G,\mathbb{C}^*)_2 = \mathbb{Z}/2$ (because $\mathrm{Hom}(G,\mathbb{C}^*) = 1$) and also $H^2(G_{x_1},\mu_2) = \mathbb{Z}/2$ (because $H^1(G_{x_1},\mathbb{C}^*) = \mathbb{Z}/2$). I claim that the restriction homomorphism is bijective. Let α be the non-trivial element of $H^2(G,\mu_2)$. It is represented by the extension

$$1 \to \mu_2 \to \mathrm{SL}(2,\mathbb{F}_p) \to \mathrm{PSL}(2,\mathbb{F}_p) \to 1.$$

Let $\tilde{g} \in \mathrm{SL}(2,\mathbb{Z})$ be a lift of the generator g of G_{x_1}. Then $\tilde{g}^2 = -1$ has order 4 and therefore the exact sequence restricts to the nontrivial extension

$$1 \to \mu_2 \to \mu_4 \to G_{x_1} \to 1$$

representing the nontrivial element of $H^2(G_{x_1},\mu_2)$.

The last assertion follows from the known genus, and hence the degree of the canonical class, of a modular curve (see **[Sh]**, p. 23).

Remark 2.5 The previous result implies that the group of $\mathrm{PSL}(2,\mathbb{F}_p)$-invariant divisors on $X(p)$ modulo principal divisors is generated by a divisor of degree $(p^2-1)/12$. This result can be also found in (**[AR]**, Corollary 24.3) together with an explicit representative of this class

$$D = \epsilon(D_2 - D_3 - pD_p),$$

where $\epsilon = \pm 1$ and $p = 6n + \epsilon$. Here D_k denote the G-orbit of points with isotropy subgroup of order k.

The tensor powers of the line bundle λ generating the group $\mathrm{Pic}(X(p))^G$ allows one to embed $X(p)$ $\mathrm{SL}(2,\mathbb{F}_p)$-equivariantly in projective space. We state without the proof the following result (see **[AR]**, Corollary 24.5):

Theorem 2.6. *Assume p is prime ≥ 5. Denote by V_- (resp. V_+) one of the two irreducible representations of $SL(2,\mathbb{F}_p)$ of dimension $\frac{p-1}{2}$ (resp. $\frac{p+1}{2}$). Then*
1. *a base-point free linear subsystem of $|\lambda^{(p-3)/2}|$ maps $X(p)$ in $\mathbb{P}(V_-) = \mathbb{P}^{(p-3)/2}$ onto a curve of degree $(p-3)(p^2-1)/48$;*
2. *a base-point-free linear subsystem of $|\lambda^{(p-1)/2}|$ maps $X(p)$ in $\mathbb{P}(V_+) = \mathbb{P}^{(p-1)/2}$ onto a curve of degree $(p-1)(p^2-1)/48$.*

It is conjectured that the linear systems embedding $X(p)$ in $\mathbb{P}(V_-)$ and in $\mathbb{P}(V_+)$ are complete (see **[AR]**, p.106). This is known to be true only for $p = 7$.

Remark 2.7 As was shown in **[AR]**, Corollary 24.5, the image of $X(p)$ in $\mathbb{P}(V_+)$ (resp. $\mathbb{P}(V_-)$) described in the previous theorem is the z-curve (resp. A-curve) of Klein. From the modern point of view these embeddings can be described as follows. Recall that $X(p)$ is a compactification of the moduli space of isomorphism classes of pairs (E,ϕ), where E is an elliptic curve and (e_1,e_2) is a basis of its group $E_p \cong (\mathbb{F}_p)^2$ of p-torsion points. Let O be the origin of E. There is a special basis $(X_0,\ldots,X_{p-1})$ in the space $\Gamma(E,\mathcal{O}_E(pO))$ which defines a map

$$f : E \to \mathbb{P}^{p-1}, \quad x \to (X_0(x),\ldots,X_{p-1}(x))$$

satisfying the following properties:
1. $(X_0(x-e_1),\ldots,X_{p-1}(x-e_1)) = (X_1(x),X_2(x),\ldots,X_{p-1}(x),X_0(x))$;

2. $(X_0(x+e_2),\dots,X_{p-1}(x+e_2)) = (X_0(x),\zeta X_1(x),\dots,\zeta^{p-1}X_{p-1}(x))$, where $\zeta = e^{2\pi i/p}$;
3. $(X_0(-x),\dots,X_{p-1}(-x)) = (X_{p-1}(x),X_{p-2}(x),\dots,X_1(x),X_0(x))$.

Let $\pi : \mathcal{X}(p) \to X(p)$ be the universal family of elliptic curves (E,e_1,e_2) (its fibres over cusps are certain degenerate curves, p-gons of lines). The p-torsion points of the fibres determine p^2 sections of the elliptic surface $\mathcal{X}(p)$. The functions X_m define a morphism $\mathcal{X}(p) \to \mathbb{P}^{p-1}$ whose restriction to the fibre (E,e_1,e_2) is equal to the map f. The functions $z_m = X_m - X_{p-1-m}, m = 0,\dots,\frac{p-3}{2}$, define a projection of the image of $\mathcal{X}(p)$ in $\mathbb{P}^{(p-3)/2}(\mathbb{C})$. The image of the section of π defined by the 0-point is the z-curve of Klein. On the other hand if we consider the functions $y_m = X_m + X_{p-1-m}$ we get the projection of $\mathcal{X}(p)$ in $\mathbb{P}^{(p-1)/2}(\mathbb{C})$. The center of this projection contains the 0-section so that the restriction of the projection map to each curve $f(E)$ is the projection from the origin $f(0)$ and still defines the image of $f(0)$. The set of these images forms the A-curve of Klein. There are certain modular forms $A_0,\dots,A_{\frac{p-1}{2}}$ defined on the upper-half plane which define the map from $X(p)$ to the A-curve.

It is proven in **[Ve]**, Thm. 10.6, that the z-curve is always nonsingular.

Example 2.8. Let $p = 7$. Then $\deg\lambda = 2$, $K_X = \lambda^2$ is of degree 4 so that $X(7)$ is a curve of genus 3. The divisor class λ is an even theta-characteristic on $X(7)$. It is the unique theta characteristic invariant with respect to the group of automorphisms $G = \mathrm{PSL}(2,\mathbb{F}_7)$ of $X(7)$ (see other proofs of this fact in **[Bu]**, pp. 22-25, **[DK]**, pp.292-294). The z-curve is a canonical model of $X(7)$, a plane quartic. This is the famous Klein's quartic with 168 automorphisms. In an appropriate coordinate system it is given by the equation

$$x_0^3x_1 + x_1^3x_2 + x_2^3x_0 = 0.$$

The A-curve is a space sextic with equations

$$t^2x + \sqrt{2}ty^3 + 2yz^2 = t^2y + \sqrt{2}tz^2 + 2zx^2 = t^2z + \sqrt{2}tx^2 + 2xy^2 = 2\sqrt{2}xyz - t^3 = 0$$

(see **[E1]**, p. 163).

It is well-known (see, for example, **[Tj]**, p. 95 and p.104) that a theta characteristic θ with $H^0(X,\theta) = 0$ on a plane nonsingular curve X of degree n with equation $F = 0$ gives rise to a representation of F as the determinant of a symmetric $n\times n$ matrix with linear forms as its entries. In other words, θ defines a net of quadrics in $\mathbb{P}^{n-1}$ and X parametrizes the set of singular quadrics from the net. The pair (X,θ) is called the *Hesse invariant* of the net. It follows from Table 2 in Appendix 1 that $S^2(V_+)$ contains V_- as a direct summand (as representations of $\mathrm{SL}(2,\mathbb{F}_7)$). This defines a $\mathrm{SL}(2,\mathbb{Z})$-invariant net of quadrics in $\mathbb{P}(V_+)$ with the Hessian invariant (X,λ). The corresponding representation of X as the determinant of a symmetric matrix of linear forms is known since Klein (see **[E1]**, p. 161):

$$x_0^3x_1 + x_1^3x_2 + x_2^3x_0 = \det\begin{pmatrix} -x_0 & 0 & 0 & -x_1 \\ 0 & x_1 & 0 & -x_2 \\ 0 & 0 & x_2 & -x_0 \\ -x_1 & -x_2 & -x_0 & 0 \end{pmatrix}. \tag{2.4}$$

Example 2.9. Let $p = 11$. Then $\deg\lambda = 5$, $K_X = \lambda^{10}$ is of degree 50 so that $X(11)$ is a curve of genus 26. The z-curve is a curve of degree 20 in $\mathbb{P}^4$. According to F. Klein [**Kl1**], pp. 153-156 (cf. [**AR**], Lemma 37.4, p.128) it is equal to the locus

$$\{(v,w,x,y,z)\in\mathbb{P}^4 : rk\begin{pmatrix} w & v & 0 & 0 & z\\ v & x & w & 0 & 0\\ 0 & w & y & x & 0\\ 0 & 0 & x & z & y\\ z & 0 & 0 & y & v\end{pmatrix}\leq 3\}.$$

The matrix in above is the Hessian matrix of a G-invariant cubic hypersurface W given by the equation

$$v^2w + w^2x + x^2y + y^2z + z^2v = 0.$$

This hypersurface has the group of automorphisms isomorphic to $\mathrm{PSL}(2,\mathbb{F}_{11})$. The A-curve is a curve of degree 25 in $\mathbb{P}^5$. It is the curve of singularities of a unique quartic ruled hypersurface in $\mathbb{P}(V_+)$ (see Appendix V in [**AR**] which contains the results of the first author). We refer for these and other beautiful facts about the geometry of $X(11)$ to [**AR**] and [**E2**].

3. Rank 2 bundles

We shall use the following result of S. Ramanan which is a special case of Proposition 24.6 from [**AR**]:

Theorem 3.1. *Let G be a finite subgroup of the group of automorphisms of a curve X and E be a G-linearized rank r vector bundle over X. Then there exists a flag*

$$0\subset E_1\subset E_2\subset\ldots\subset E_{r-1}\subset E$$

of G-invariant subbundles, where each E_i is of rank i and all inclusions are G-equivariant.

Because of the importance of this result for the sequel we shall sketch a proof. Choose an ample G-linearized line bundle L with trivial isotropy representations. This is always possible by taking products and powers of the translates of an ample line bundle by elements from G. Then we apply the Lefschetz Fixed Point Formula for coherent sheaves:

$$tr(g|H^0(X,E\otimes L^n)) - tr(g|H^1(X,E\otimes L^n)) = \sum_{g(x)=x}\frac{tr(g|L_x^n\otimes E_x)}{1-dg_x}.$$

Since g acts identically on L_x, the right-hand side is independent of n. Taking n sufficiently large, we get rid of H^1. Since the dimension of H^0 will grow with n and the trace of $g\neq 1$ on H^0 does not change with n we easily obtain that H^0 contains the trivial irreducible representation for large n. This implies that there exists a G-invariant section of $E\otimes L^n$. It gives a G-invariant embedding of L^{-n} in E. It generates a G-invariant subbundle of E. Now we take the quotient and apply induction on the rank.

Corollary 3.2. *Let E be a* $\mathrm{PSL}(2,\mathbb{F}_p)$*-invariant rank r vector bundle over $X(p)$. Then there is a* $\mathrm{PSL}(2,\mathbb{F}_p)$*-equivariant flag*

$$0\subset E_1\subset E_2\subset\ldots\subset E_{r-1}\subset E \tag{3.1}$$

of $\mathrm{PSL}(2,\mathbb{F}_p)$*-invariant rank* i *vector bundles* E_i.

Proof. To see that the previous theorem applies, we use Corollary 1.2 that shows that E admits an $\mathrm{SL}(2,\mathbb{F}_p)$-linearization. If the center $C=\{\pm 1\}$ of $\mathrm{SL}(2,\mathbb{F}_p)$ does not act identically on E, hence acts as -1 on each fibre, we replace E by $E'=E\otimes\lambda$. Since λ is $\mathrm{SL}(2,\mathbb{F}_p)$-linearized but not $\mathrm{PSL}(2,\mathbb{F}_p)$-linearized the center C acts as -1 on λ. So E' is $\mathrm{PSL}(2,\mathbb{F}_p)$-linearized and the theorem applies.

We shall call a flag (3.1) a *Ramanan flag* of E. Let $L_i=E_i/E_{i-1}, i=1,\dots,r$, where $E_0=0, E_r=E$, be the factors of a Ramanan flag of E. We know that each L_i is equal to λ^{a_i} for some integer a_i. We shall call the sequence $(a_1,\dots,a_r)$ a *sequence of exponents* of E. Clearly the sequence $(-a_r,\dots,-a_1)$ is a sequence of exponents of the dual bundle E^*. Note that the same bundle may have different sequences of exponents.

Proposition 3.3. *Let* $(a_1,\dots,a_r)$ *be a sequence of exponents of a* $\mathrm{PSL}(2,\mathbb{F}_p)$*-invariant stable rank* r *bundle over* $X(p)$. *Let* $a=a_1+\ldots+a_r$. *Then, for any* $s<r$,

$$a_1+\ldots+a_s<\frac{s}{r}a.$$

Proof. This follows immediately from the definition of stability.

In the case $r=2$ we will be able to say more about sequences of exponents of a rank 2 bundle (see Corollary 4.3) but now let us note the following result (see **[AR]**, Lemma 24.6):

Proposition 3.4. *Assume* $r=2$ *and let* (a_1,a_2) *be a sequence of exponents of a* G*-stable bundle* E. *Then* a_1+a_2 *is even.*

This follows from the fact that any G-invariant extension

$$0\to\lambda^{a_1}\to E\to\lambda^{a_2}\to 0$$

has obstruction class for splitting in

$$H^1(X,\lambda^{a_1-a_2})^{SL(2,\mathbb{F}_p)}=(H^0(X,\lambda^{a_2-a_1+2p-12})^*)^{SL(2,\mathbb{F}_p)}.$$

Since -1 acts as -1 in $H^0(X,\lambda^{odd})^*$ the latter space is trivial.

Corollary 3.5. *Each* $\mathrm{PSL}(2,\mathbb{F}_p)$*-invariant stable bundle of rank 2 over* $X(p)$ *has determinant isomorphic to* λ^a, *where* a *is even.*

By tensoring E with $E\otimes\lambda^{-a/2}$ we may assume now that $\det E$ is trivial. This allows us to invoke some results from topology. Recall the following fundamental result from **[NS]**, pp. 556-558:

Theorem 3.6. *Let* E *be a degree* 0 *stable vector bundle on a compact Riemann surface* X. *Then there exists an irreducible unitary representation*

$$\rho:\pi_1(X)\to\mathrm{U}(r)$$

such that E *is isomorphic to the vector bundle* $H\times\mathbb{C}^r/\pi_1(X)\to X=H/\pi_1(X)$, *where* H *is the universal cover of* X *with the natural action of* $\pi_1(X)$ *on it, and the fundamental group* π_1 *acts on the product by the formula* $\gamma:(z,v)\to(\gamma\cdot z,\rho(\gamma)\cdot v)$. *This construction defines a bijective correspondence between the set of isomorphism* *classes of stable rank r bundles of degree zero and the set of irreducible unitary representations of $\pi_1(X)$ of dimension r up to conjugation by a unitary transformation of $\mathbb{C}^r$. In this correspondence stable bundles with trivial determinant correspond to irreducible representations $\rho : \pi_1(X) \to \mathrm{SU}(r)$.*

Note that this theorem also gives a representation theoretical description of points of the moduli space $\mathcal{M}_X(r,0)$ of semi-stable rank r vector bundles over X representated by semi-stable but not stable bundles of degree 0. They correspond to reducible unitary representations.

We shall apply this theorem to our situation. First we need the following:

Definition. A G-linearized vector bundle is called *G-stable* if for any G-linearized subbundle F of E one has $\mu(F) < \mu(E)$ (see 1.1 for the definition of μ).

Notice that a G-stable bundle is always semi-stable since it is known that any bundle always contains a unique, hence G-invariant, maximal semi-stable subbundle (see [**Se**], Proposition 2, p. 15). Obviously a stable bundle is G-stable. However, a semi-stable bundle could be also G-stable. For example, the trivial bundle defined by an irreducible representation of G is G-stable but not stable. Recall from section 1 that we always assume that a semi-stable G-linearized bundle is a direct sum of stable bundles.

Theorem 3.7. *Let E be a G-linearized semi-stable vector bundle of degree 0 given by a unitary representation $\rho : \pi_1(X) \to \mathrm{U}(r)$. Let Π be the group of automorphisms of the universal cover H of X generated by lifts of elements of G. In other words, Π is the subgroup of $G \times \mathrm{Aut}(H)$ consisting of pairs $(g, \tilde{g})$ such that $\tilde{g}$ is a lifting to H of the automorphisms of X determined by g. Then ρ can be extended to a unitary representation $\tilde{\rho} : \Pi \to \mathrm{U}(r)$. Moreover this defines a bijective correspondence between the set of isomorphism classes of G-stable rank r bundles of degree 0 and the set of irreducible unitary representations $\Pi \to \mathrm{U}(r)$ up to conjugation by a unitary transformation of $\mathbb{C}^r$.*

Proof. First we fix the trivial C^∞ bundle $\mathcal{E}$ of rank r over X, and a G-invariant Hermitian metric on E. We can always do it since X is compact. Let $\mathcal{A}$ be the set of unitary connections on $\mathcal{E}$ whose curvature form has type $(1,1)$ with trivial cohomology class. Any $A \in \mathcal{A}$ defines a holomorphic structure E_A on $\mathcal{E}$ of degree 0; its sheaf of holomorphic sections is equal to the set of local solutions of the equation $\bar{\partial}_A = 0$, where $\bar{\partial}_A$ is the $(0,1)$ component of the covariant derivative of A. Any holomorphic structure E on $\mathcal{E}$ of degree 0 is defined in this way by a unique unitary connection $A \in \mathcal{A}$ ([**DoK**], Proposition 2.1.56, p. 46). The natural action of the unitary gauge group $\mathcal{G}$ on $\mathcal{A}$ extends to an action of the complexified gauge group $\mathcal{G}^{\mathbb{C}}$ and the set of orbits of $\mathcal{G}^{\mathbb{C}}$ in $\mathcal{A}$ can be identified with the set of isomorphism classes of holomorphic structures on E of degree 0 (loc. cit., p. 210). A proof of Theorem 3.6 given by S. Donaldson [**Don**] consists of showing that the $\mathcal{G}^{\mathbb{C}}$-orbit corresponding to the isomorphism class of a semi-stable holomorphic bundle E of degree 0 contains a unique $\mathcal{G}$-orbit of flat unitary connections. In particular, replacing E by an isomorphic bundle, we may assume that E is defined by a unique flat unitary connection A_E. Now the isomorphism $\phi_g : g^*(E) \to E$ defined by the G-linearization of E sends the flat unitary connection $g^*(A_E)$ on $g^*(E)$ to a flat unitary connection on E which must coincide with A_E. Considered as a horizontal distribution on the total space $\mathbb{V}(E)$ of E the connection $g^*(A_E)$ is equal to A_E.

This shows that A_E is preserved under the G-linearization, considered as an action on $\mathbb{V}(E)$. Let $\mathcal{V}$ be the sheaf of horizontal sections of E with respect to A_E. It is a sheaf of complex unitary vector spaces of dimension equal to the rank of E. If we are willing to identify a vector bundle with the corresponding sheaf $\mathcal{E}$ of holomorphic sections, then $\mathcal{V}$ is a subsheaf of $\mathcal{E}$. In fact we have an isomorphism of $\mathbb{C}$-sheaves $\mathcal{E} \cong \mathcal{V} \otimes \mathcal{O}_X$. It follows from above that $\mathcal{V}$ admits a G-linearization, the restriction of the G-linearization of $\mathcal{E}$. This G-linearization preserves the unitary structure on fibres. The group Π acts on the pull-back $\tilde{\mathcal{V}}$ of $\mathcal{V}$ on H via a representation $\tilde{\rho}$ of Π in $\mathrm{U}(r)$. Conversely given such a representation $\tilde{\rho}$, we consider the semi-stable vector bundle $E_\rho = H \times \mathbb{C}^r/\Gamma$, where $\Gamma = \pi_1(X)$ acts on $H \times \mathbb{C}^r$ via the restriction ρ of $\tilde{\rho}$, $(z, v) \mapsto (g \cdot z, \rho(g)(v))$. The group $G = \Pi/\Gamma$ acts naturally on E_ρ and defines a G-linearization.

Now, if $\tilde{\rho}$ is irreducible, then E_ρ is G-stable since otherwise it contains a G-invariant semi-stable subbundle of degree 0, and by the above construction it will define a unitary subrepresentation of $\tilde{\rho}$. Conversely, if E_ρ is G-stable, the representation $\tilde{\rho}$ is irreducible, since otherwise its direct summand will define a G-invariant semi-stable subbundle of E_ρ of degree 0.

Let Π be as above. It is given by an extension of groups

$$1 \to \Gamma \to \Pi \to G \to 1,$$

where $\Gamma \cong \pi_1(X)$. Assume that $X/G = H/\Pi = \mathbb{P}^1$. Then Π, as an abstract group, is given by the genetic code:

$$\Pi =< \gamma_1, \dots , \gamma_n | \gamma_1^{e_1} = \dots = \gamma_n^{e_n} = \gamma_1 \cdots \gamma_n = 1 >,$$

where $\sum e_i^{-1} < n - 2$. As a group of transformations of H, Π is isomorphic to a discrete subgroup of $\mathrm{PSL}(2, \mathbb{R})$ which acts on H as a subgroup generated by even products of reflections in sides of a geodesic n-gon with angles π/e_i. Such a subgroup of $\mathrm{PSL}(2, \mathbb{R})$ is called a *Dyck group* (or a *triangle group* if $n = 3$) of signature $(e_1, \dots , e_n)$. Conversely, let Π be an abstract group as above and Γ be a normal torsion-free subgroup of finite index. Choose an isomorphism from Π to a Dyck group (if $n = 3$ it is defined uniquely, up to a conjugation). Let us identify Π with its image. The group Γ acts freely on H and the quotient H/Γ is a compact Riemann surface X_Γ with $\pi_1(X) \cong \Gamma$. The factor group $G = \Pi/\Gamma$ acts on X_Γ by holomorphic automorphisms. The projection $\pi : X_\Gamma \to X_\Gamma/G = \mathbb{P}^1$ ramifies over n points with ramification indices $e_1, \dots , e_n$.

The modular curve $X(p)$ is a special case of this construction. One takes $(e_1, \dots , e_n) = (2, 3, p)$ and $\Gamma = \pi_1(X(p))$.

Let $\tilde{\Pi}$ be the group with the genetic code

$$\tilde{\Pi} =< \tilde{\gamma}_1, \dots , \tilde{\gamma}_n, h | h \ \text{ central}, \tilde{\gamma}_1^{e_1} = \dots = \tilde{\gamma}_n^{e_n} = \tilde{\gamma}_1 \dots \tilde{\gamma}_n = h > .$$

It is a central extension of Π with infinite cyclic center generated by h:

$$1 \to (h) \to \tilde{\Pi} \to \Pi \to 1. \tag{3.2}$$

We shall assume that Π is perfect, i.e. coincides with its commutator $\Pi' = [\Pi, \Pi]$. This happens if and only if the e_i's are pairwise prime. In this case the commutator group $\tilde{\Pi}' = [\tilde{\Pi}, \tilde{\Pi}]$ is a universal central extension of Π (see **[Mi]**, §5):

$$1 \to (t) \to [\tilde{\Pi}, \tilde{\Pi}] \to \Pi \to 1. \tag{3.3}$$

Its center (t) is a subgroup of (h) generated by h^s, where

$$s = e_1 \cdots e_n(n - 2 - \sum_{i=1}^{n} e_i^{-1}).$$

The genetic code of $\tilde{\Pi}'$ is

$$\tilde{\Pi}' =< \tilde{g}_1, \dots, \tilde{g}_n, t | t \quad \text{central}, \tilde{g}_1^{e_1} = t^{b_1}, \dots, \tilde{g}_n^{e_n} = t^{b_n}, \tilde{g}_1 \cdots \tilde{g}_n = t^b >, \tag{3.4}$$

where

$$sb_i \equiv 1 \bmod e_i, \quad 0 < b_i < e_i,$$
$$b - \sum_{i=1}^{n} \frac{b_i}{e_i} = \frac{1}{e_1 \cdots e_n}.$$

All of this is well-known in 3-dimensional topology (see for example, **[S]**, §10 and §12). We have

$$\tilde{\Pi}' = \pi_1(\Sigma(e_1, \dots, e_n)),$$

where $\Sigma(e_1, \dots, e_n)$ is a Seifert-fibred 3-dimensional homology sphere given explicitly as the intersection of a sphere S^{2n-1} with center at the origin in $\mathbb{C}^n$ and the algebraic surface given by the equations

$$z_1^{e_1} + z_i^{e_i} + z_n^{e_n} = 0, \quad i = 2, \dots, n - 1.$$

The group Π is the fundamental group of the link of a canonical Gorenstein singularity admitting a good $\mathbb{C}^*$-action (see **[Do]**).

Corollary 3.8. *Keep the notation of Theorem 3.7. Assume that the group Π is perfect. Let $1 \to H^2(G, \mathbb{C}^*) \to \tilde{G} \to G \to 1$ be the universal central extension of G and let $d = |H^2(G, \mathbb{C}^*)|$. Then $\tilde{\Pi}'$ is mapped surjectively on $\tilde{G}$ and there is a bijective correspondence between irreducible unitary representations $\rho : \tilde{\Pi}' \to \mathrm{SU}(r)$ with $\rho(h)^d = 1$ which restrict to an irreducible representation of $\tilde{\Gamma} = \mathrm{Ker}(\tilde{\Pi}' \to \tilde{G})$ and G-invariant stable rank r bundles over X_Γ with trivial determinant.*

Proof. Let $\Pi \cong F/R$ where F is a free group. It is known that the universal central extension $\tilde{\Pi}'$ is isomorphic to $[F, F]/[R, F]$ (see **[Mi]**, §5). Since $G \cong F/R'$, where $R \subset R'$ we obtain that $\tilde{G} \cong [F, F]/[R', F]$ and there is a surjective homomorphism $\tilde{\Pi}' \to \tilde{G}$. Let $\tilde{\Gamma}$ be the kernel of this homomorphism. We have a central extension for $\tilde{\Gamma}$:

$$1 \to (t^{d'}) \to \tilde{\Gamma} \to \Gamma \to 1,$$

where $d'|d$. Given an irreducible representation $\rho : \tilde{\Pi}' \to \mathrm{SU}(r)$ with $\rho(h)^d = 1$ we define $\beta : \Gamma \to \mathrm{SU}(r)$ by first restricting ρ to $\tilde{\Gamma}$ and then factoring it through the quotient $\tilde{\Gamma}/(t^d) \cong \Gamma$. Since, by the assumption, the restriction of ρ to $\tilde{\Gamma}$ is irreducible, β is irreducible. This defines a stable rank r bundle E on X_Γ with trivial determinant. Since $\tilde{\Gamma}$ is normal in $\tilde{\Pi}'$, the group $\tilde{G}$ acts on $E = H \times \mathbb{C}^r/\tilde{\Gamma}$ and makes E a G-invariant bundle. Conversely, by Corollary 1.2, any G-invariant stable bundle E with trivial determinant admits a $\tilde{G}$-linearization. This linearization defines a $\tilde{G}$-linearization on the local coefficient system $\mathcal{V}$ defined by the flat unitary connection on E. The group $\tilde{\Gamma}$ acts on the pull-back $\bar{\mathcal{V}} = \mathcal{V} \times_X H$ of $\mathcal{V}$ on H via the action of Γ on H and the trivial action on $\mathcal{V}$. Since $\bar{\mathcal{V}}$ trivializes on H, it coincides with the universal covering of $\mathcal{V}$. Thus the action of $\tilde{G}$ lifts to an action of $\bar{\mathcal{V}}$ and defines an action of Π' on $\bar{\mathcal{V}} = H \times \mathbb{C}^r$. This defines a unitary representation of the group $\tilde{\Pi}'$ in $\mathrm{SU}(r)$.

Remark 3.9 If $r = 2$ we do not need the assumption that the restriction β of $\rho : \tilde{\Pi}' \to \mathrm{SU}(2)$ to $\tilde{\Gamma}$ is irreducible. Assume it is not. Then it decomposes into sum of one-dimensional unitary representations $V_1 + V_2$. By Theorem 3.6 they define two line bundles on X_Γ with determinants of degree 0. These bundles are invariant with respect to the group $G = \Pi/\Gamma$. However, the computations from the first section show that $\mathrm{Pic}(X_\Gamma)$ is generated by an element of positive degree. This shows that β must be the trivial representation. Thus ρ factors through a representation $\bar{\rho} : G \to \mathrm{SU}(2)$. However, it is easy to see using the classification of finite subgroups of $\mathrm{SU}(2)$ that G does not admit non-trivial 2-dimensional unitary representations. This gives us that ρ is the trivial representation which contradicts the assumption that ρ is irreducible.

Corollary 3.10. *Let (a_1, a_2) be a sequence of exponents of a stable G-invariant rank 2 vector bundle over $X(p)$. Then $(a_1 - a_2)/2$ is an odd number.*

Proof. We already know from Proposition 3.4 that $a_1 + a_2$ is even. By tensoring with $\lambda^{\frac{a_2 - a_1}{2}}$ we may assume that E has trivial determinant, i.e. $a_1 + a_2 = 0$. Assume a_1 is even. Then the extension

$$0 \to \lambda^{a_1} \to E \to \lambda^{a_2} \to 0$$

shows that the center of $\mathrm{SL}(2, \mathbb{F}_p)$ acts identically on E. Hence the bundle E admits a $\mathrm{PSL}(2, \mathbb{F}_p)$-linearization. By Theorem 3.7, this defines a unitary representation $\rho : \Pi \to \mathrm{SU}(2)$. Let g_1 be a generator of Π of order 2. Then $\rho(g_1)^2 = 1$ and hence $\rho(g_1) = \pm 1$. This implies that $\rho(g_2)^3 = \rho(g_3)^p = 1$ and $\rho(g_2 g_3) = \rho(g_1) = \pm 1$. This gives that $\rho(g_i) = 1, i = 1, 2, 3$, i.e. ρ is trivial. This contradicts the assumption that E is stable.

Theorem 3.11. *Let $p = 6n \pm 1$. Then there exist exactly $2n$ non-isomorphic rank 2 stable G-invariant vector bundles over $X(p)$ with trivial determinant.*

Proof. This is an immediate corollary of Theorem 3.7, Remark 3.9, and the known computation of the number of irreducible unitary representation of the fundamental group of the Brieskorn sphere $\Sigma(e_1, e_2, e_3)$ (see **[FS]**, Proposition 2.8, p.116).

We will give an independent verification of this result for the case $p = 7$ in §6. We shall also say more about how to use the results of **[FS]** when we sketch the proof of Theorem 4.2.

4. Isotropy representation

Let us return to the general situation of a finite group G acting on a compact Riemann surface X. Let $\mathcal{C}(X; G)$ be the set of pairs (C, g), where C is a connected component of the fixed locus of $g \in G$, modulo the natural action of G on these pairs by

$$g' \cdot (C, g) = (g'(C), g' g g'^{-1}).$$

Since X is a curve, C is either a single point or all of X. In the latter case the element g belongs to the kernel A of the action of G on X. Let $\check{\mathcal{C}}(X; G)$ denote the set of complex valued functions on the set $\mathcal{C}(X;G)$. We define the *isotropy representation* map:

$$\rho : \mathcal{M}_X(G;r) \to \check{\mathcal{C}}(X;G)$$

as follows. For each $E \in \mathcal{M}_X(G;r)$ defined by isomorphisms $\phi_g : g^*(E) \to E$ and for each $(C,g) \in \mathcal{C}(X;G)$ we let

$$\rho(E)(C,g) = \mathrm{Trace}(\phi_{g,x} : g^*(E)_x = E_x \to E_x),$$

where $x \in C$.

Consider the quotient

$$Y = X/G$$

and let $p : X \to Y$ be the natural orbit map. There is a finite set of G-orbits in X with non-trivial isotropy subgroup. They correspond to the set S of points $y_1, \dots, y_n$ in Y such that p is ramified over any point $x \in p^{-1}(S)$. For any $g \in G$, we have $gG_xg^{-1} = G_{g\cdot x}$. In each fibre $p^{-1}(y_i)$ pick a point x_i and denote the corresponding isotropy subgroup G_{x_i} by G_i. This is an extension of a cyclic subgroup $\bar{G}_i$ of $\bar{G}$ of order e_i and the group A. It is clear that each $(C,g) \in \mathcal{C}(X;G)$ can be represented by a pair $(x_i, g_i), g_i \in G_i$, or by a pair $(X,a), a \in A$. Assume A is central in G (as it will be in our case). Then this representation is unique since G_{x_i} is cyclic. Thus we have

$$|\mathcal{C}(X;G)| = \sum_{i=1}^{n}(e_i - 1) + |A|.$$

The representatives of $\mathcal{C}(X;G)$ can be chosen as follows:

$$(x_1, g_1), \dots, (x_1, g_1^{e_1-1}), \dots, (x_n, g_n), \dots, (x_n, g_n^{e_n-1}), (X,a), a \in A,$$

where each $g_i \in G$ is a representative of a generator of $(G/A)_{x_i}$.

Now we place ourselves in the situation discussed in the previous section and assume that $X = X_\Gamma$, where Γ is a torsion free normal subgroup of a Dyck group Π of signature $(e_1, \dots, e_n)$. Also we assume that Π is perfect. In this case we can choose representatives of $\mathcal{C}(X_\Gamma;G)$ taking for g_i the images of the standard generators $\tilde{\gamma}_i$ of $\tilde{\Pi}'$.

Theorem 4.1. *Keep the notation of Corollary 3.8. Let E be a stable vector bundle on X_Γ arising from a unitary representation $\rho : \tilde{\Pi}' \to \mathrm{SU}(r)$. Then, for any integer k,*

$$\mathrm{Trace}(\rho(\tilde{g}_i^k)) = \mathrm{Trace}((\phi_{g_i^k})_{x_i} : E_{x_i} \to E_{x_i}), \quad i = 1, \dots, n.$$

Proof. This follows easily from the construction of E by means of a unitary representation of $\tilde{\Pi}'$.

In the case $r = 2$ an algorithm for computations of the traces $\mathrm{Trace}(\rho(\tilde{g}_i^k))$ of a unitary representation ρ of the group $\tilde{\Pi}'$ of signature (e_1, e_2, e_3) is described in **[FS]**, p. 111-112. In our case $(e_1, e_2, e_3) = (2, 3, p = 6n + \epsilon)$ we can use the values $b = 1, b_1 = 1, b_2 = 1, b_3 = n$ if $\epsilon = 1$ and $b = 2, b_1 = 1, b_2 = 2, b_3 = 5n - 1$ if $\epsilon = -1$ in the presentation (3.4) of the group $\tilde{\Pi}'$. Following the example from loc. cit. on p. 112, we get the following

Theorem 4.2. *Let $(e_1, e_2, e_3) = (2, 3, p)$ and let $\rho : \tilde{\Pi}' \to \mathrm{SU}(2)$ be an irreducible representation. Write $p = 6n + \epsilon$, where $\epsilon = \pm 1$. Then*

$$[\mathrm{Trace}(\rho(\tilde{\gamma}_1)), \mathrm{Trace}(\rho(\tilde{\gamma}_2)), \mathrm{Trace}(\rho(\tilde{\gamma}_3))] = [0, \epsilon, 2\cos(\frac{\pi k}{p})],$$

where k is an integer with $(-1)^{k+n} = \epsilon$ between $n+1$ and $5n$ if $\epsilon = 1$ and between n and $5n-1$ if $\epsilon = -1$.

Recall that we have $2n$ unitary irreducible representations $\rho : \tilde{\Pi}' \to \mathrm{SU}(2)$ and this agrees with the number of all possible triples of the characters.

The conjugation classes of the unitary matrices $\rho(\tilde{\gamma}_i)$ are represented accordingly by

$$\left[\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} e^{(3-\epsilon)\pi i/6} & 0 \\ 0 & e^{-(3-\epsilon)\pi i/6} \end{pmatrix}, \begin{pmatrix} e^{k\pi i/p} & 0 \\ 0 & e^{-k\pi i/p} \end{pmatrix}\right].$$

So raising the corresponding matrices in powers and computing the traces, we get the expression for the traces of powers of the generators $\tilde{\gamma}_i$ and of the central element t.

In fact, following A. Adler, we can easily write down actual matrices defining the representation ρ:

$$\rho(\tilde{g}_1) = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix},$$

$$\rho(\tilde{g}_2) = \epsilon \begin{pmatrix} \frac{1}{2} - i\cos(\frac{k\pi}{p}) & \sqrt{\frac{3}{4} - \cos^2(\frac{k\pi}{p})} \\ -\sqrt{\frac{3}{4} - \cos^2(\frac{k\pi}{p})} & \frac{1}{2} + i\cos(\frac{k\pi}{p}) \end{pmatrix},$$

$$\rho(\tilde{g}_3) = \begin{pmatrix} -\frac{i}{2} + \cos(\frac{k\pi}{p}) & -i\sqrt{\frac{3}{4} - \cos^2(\frac{k\pi}{p})} \\ -i\sqrt{\frac{3}{4} - \cos^2(\frac{k\pi}{p})} & \frac{i}{2} + \cos(\frac{k\pi}{p}) \end{pmatrix}.$$

Corollary 4.3. *Let E be a stable rank 2 $\mathrm{SL}(2, \mathbb{F}_p)$-linearized bundle on $X(p)$ with trivial determinant. Let $[0, \epsilon, 2\cos(\frac{\pi k}{p})]$ define its isotropy representations and let $(a, -a)$ be a sequence of exponents of E. Then a is an odd negative integer, and*

$$an \equiv \pm k \mod p, \quad a \equiv \pm 1 \mod 6.$$

Proof. Let

$$0 \to \lambda^a \to E \to \lambda^{-a} \to 0$$

be the extension defined by the sequence of exponents $(a, -a)$. Since E is stable of degree 0, a must be negative. From Corollary 3.10 we know that a is odd. Clearly the isotropy representation of E is determined in terms of the isotropy representation of λ^a. We know that $\lambda^{2p-12} = K_{X(p)}$. The isotropy representation of the cotangent line bundle K_X is easy to find. Any generator g_i of the isotropy group G_{x_i} acts as a primitive e_i-th root of unity. Let us take it to be $e^{2\pi i/e_i}$. Then the isotropy representation of λ at (x_i, g_i) is given by some $2e_i$-th root of unity $e^{s_i \pi i/e_i}, 0 \le s_i < 2e_i$, which satisfies $(p-6)s_i \equiv 1 \bmod e_i$. We easily find

$$s_i = \begin{cases} 1, 3 & \text{if } i = 1 \\ \frac{3-\epsilon}{2}, \frac{3-\epsilon}{2} + 3 & \text{if } i = 2 \\ n, n+p & \text{if } i = 3, \epsilon = 1 \\ p-n, 2p-n & \text{if } i = 3, \epsilon = -1. \end{cases} \tag{4.1}$$

This shows that $[2\cos(as_1\pi/2), 2\cos(as_2\pi/3), 2\cos(as_3\pi/p)] = [0, \epsilon, 2\cos(k\pi/p)]$. We check that the first entries coincide automatically because a is odd (this also gives another proof of the fact that a is odd). The equality $2\cos(as_2\pi/3) = \epsilon$ easily gives $a \equiv \pm 1 \mod 6$ and $s_2 = \frac{3-\epsilon}{2}$. Here we use that a must be odd. To satisfy $\cos(as_3\pi/p) = \cos(k\pi/p)$ we must have $as_3 \equiv \pm k \mod 2p$. If $\epsilon = 1$, we have $k+n$ is even. This easily gives $s_3 = n$ and $an \equiv \pm k \mod 2p$. Since $an \equiv \pm k \mod 2$ when $\epsilon = 1$, we get the condition $an \equiv \pm k \mod p$. If $\epsilon = -1$, we have $k+n$ is odd. This gives $s_3 = p - n$ and $a(p-n) \equiv \pm k \mod 2p$. Again $a(p-n) \equiv \pm k \mod 2$ when $\epsilon = -1$. This gives again $an \equiv \pm k \mod p$. This proves the assertion.

The proof also gives the following information about the isotropy representation of the line bundle λ (proven by other methods in [**AR**]):

Corollary 4.4. *Let (s_1, s_2, s_3) be the triple of integers defining the isotropy representation of λ as in (4.1). Then*

$$s_i = \begin{cases} 1, 3 & \text{if } i = 1 \\ \frac{3-\epsilon}{2} & \text{if } i = 2 \\ n & \text{if } i = 3, \epsilon = 1 \\ p - n & \text{if } i = 3, \epsilon = -1. \end{cases}$$

5. The Adler-Ramanan-Klein bundle

It was introduced by A. Adler and S. Ramanan ([**AR**], §24). It arises from an interpretation of Klein's quartic equations defining the z-curve $X(p)$ (see [**KF**], p.268). We refer to [**AR**] and [**Ve**] for a modern treatment of these equations. We shall prove that this bundle is stable when $p = 7$ and find its sequence of exponents.

Recall that $\mathrm{SL}(2, \mathbb{F}_p)$ has two non-isomorphic irreducible representations of dimension $\frac{p-1}{2}$ and two non-isomorphic representations of dimension $\frac{p+1}{2}$. When $p \equiv 3$ modulo 4 the two representations from each pair are dual to each other. One can combine one representation from each pair to form the sum isomorphic to a Weil representation V of $\mathrm{SL}(2, \mathbb{F}_p)$ of dimension p (see, for example, [**AR**], Appendix 1). The nontrivial central element -1 of $\mathrm{SL}(2, \mathbb{F}_p)$ decomposes this representation in even and odd part of dimension $(p+1)/2$ and $(p-1)/2$, respectively. We denote these representations by V_+ and V_-. The z curve $X(p)$ lies in the projectivization of V_-. The A-curve $X(p)$ lies in the projectivization of V_-.

Combining the interpretation of Klein's equations ([**Kl2**], p.195) from [**AR**], Theorem 19.7, p. 56, together with a result from [**Ve**], Thèoreme 10.6, p. 145, we obtain the following result:

Theorem 5.1. *There is an isomorphism of representations of* $\mathrm{SL}(2, \mathbb{F}_p)$:

$$\tau : S^2(V_-) \cong \Lambda^2(V_+).$$

Let $\nu_2 : \mathbb{P}(V_-) \to \mathbb{P}(S^2(V_-))$ be the Veronese embedding given by the complete linear system of quadrics in $\mathbb{P}(V_-)$. Identifying $\mathbb{P}(S^2(V_-))$ with $\mathbb{P}(\Lambda^2(V_+))$ by means of τ, we have

$$X(p) = \nu_2^{-1}(G(2, V_+)),$$

where $G(2, V_+)$ is the Grassmann variety of 2-dimensional linear subspaces in V_+.

Definition. The *Adler-Ramanan-Klein bundle* (the ARK bundle for brevity) over $X(p)$ is the inverse image of the tautological rank 2 bundle over $G(2, V_+)$ under the map $\nu_2 : X(p) \to G(2, V_+)$.

Theorem 5.2. *The determinant of the ARK bundle E is equal to λ^{3-p}. It is stable provided the following condition is satisfied:*

$$H^0(X(p), \lambda^a) \text{ does not contain } V_+^* \text{ as in irreducible summand if } a \leq \tfrac{p-3}{2} \qquad (*)$$

Proof. Since the dual bundle E^* embeds $X(p)$ in $G(2, V_+)$ and the corresponding Plücker embedding of $X(p)$ is given by quadrics we obtain that the determinant of E^* is equal to λ^{p-3}. Assume E is not stable. Then E^* is unstable too and contains a destabilizing subbundle of degree $\geq \frac{p-3}{2}\deg \lambda$. By **[Se]**, Proposition 2, p. 15, one can always choose a unique maximal destabilizing subbundle. This implies that E^* contains a G-invariant subbundle isomorphic to λ^a with $a \geq \frac{p-3}{2}$. Then E^* has a quotient of the form λ^a, where $a \leq \frac{p-3}{2}$. Since E^* defines an embbeding in $G(2, V_+)$ it is spanned by the subspace V_+^* of its space of global sections. This shows that λ^a is spanned by V_+^* too. This implies that there is a $\mathrm{SL}(2, \mathbb{F}_p)$-invariant non-trivial linear map $V_+^* \to H^0(X(p), \lambda^a)$. This contradicts the assumption of the theorem.

Remark 5.3 It is conjectured (see **[AR]**, p.106) that

$$V_-^* = H^0(X(p), \lambda^{(p-3)/2}), \quad V_+^* = H^0(X(p), \lambda^{(p+1)/2}).$$

This makes plausible that (*) is always satisfied. In fact, together with Adler and Ramanan, I believe that $H^0(X(p), \lambda^a) = 0$ for $a < \frac{p-3}{2}$ and $H^0(X(p), \lambda^{\frac{p-3}{2}}) \cong V_-$ (see the "WYSIWYG" Hypothesis in **[AR]**, p.106).

6. Example: $p = 7, r = 2$

To simplify notation X will denote in this section the modular curve $X(7)$. We know from Theorem 3.11 that there exist exactly two non-isomorphic stable rank 2 bundles with trivial determinant. Let us prove it without using topology. We use the following well-known description of the moduli space of semi-stable rank 2 bundles over a compact Riemann surface of genus 3 (see **[NR]**):

Theorem 6.1. *Let $\mathrm{SU}_X(2)$ be the moduli space of semi-stable rank 2 bundles with trivial determinant over a compact Riemann surface of genus 3. Then there is an embedding $\Phi : SU_X(2) \hookrightarrow \mathbb{P}(H^0(J^2(X), \mathcal{O}(2\Theta))) \cong \mathbb{P}^7$, where $J^2(X)$ is the Picard variety of divisor classes of degree 2 and Θ is the hypersurface of effective divisor classes. For every $E \in \mathrm{SU}_X(2)$ its image is a divisor in $\mathbb{P}(H^0(J^2(X), \mathcal{O}(2\Theta))) = |2\Theta|$ whose support is equal to the set of $L \in J^2(X)$ such that $H^0(X, E \otimes L) \neq 0$.*

Lemma 6.2. *Let V_6 be the unique irreducible 6-dimensional representation of $\mathrm{PSL}(2, \mathbb{F}_7)$. Then there are isomorphisms of $\mathrm{PSL}(2, \mathbb{F}_7)$-representations*

$$V_6 \cong V_6^* \cong S^2(V_-) \cong \Lambda^2(V_+),$$

$$S^2(V_6) \cong V_6 \oplus S^4(V_-^*).$$

Proof. The last isomorphism in the first line was observed already in Theorem 5.1. The Veronese map $\mathbb{P}(V_-) \to \mathbb{P}(S^2(V_-)) \cong \mathbb{P}(V_6)$ is obviously $\mathrm{PSL}(2, \mathbb{F}_7)$-equivariant. The isomorphism in the second line is obtained by considering the restriction of the linear system of quadrics in $\mathbb{P}(V_6)$ to the Veronese surface, the image of the Veronese map. The subspace V_6 is the subspace of quadrics vanishing on the Veronese surface. The quotient space is isomorphic to the space of quartics in $\mathbb{P}(V_-)$.

Corollary 6.3. *Let $X = X(7)$ be the Klein quartic. Then the group $G = \mathrm{PSL}(2, \mathbb{F}_7)$ acts naturally on $\mathrm{SU}_X(2)$ and has exactly three fixed points represented by the trivial bundle and two stable bundles.*

Proof. By construction the map Φ from Theorem 6.1 is $\mathrm{PSL}(2, \mathbb{F}_7)$-invariant. So the group $\mathrm{SL}(2, \mathbb{F}_7)$ acts linearly in $H^0(J^2(X), \mathcal{O}(2\Theta))$. Consider the embedding of X in $\mathbb{P}^5$ given by the linear system $|2K_X|$. Since $H^0(X, \mathcal{O}(2K_X)) = S^2(V_-^*)$ we see from Lemma 6.2 that X is embedded equivariantly in $\mathbb{P}(V_6)$ where V_6 is the unique irreducible 6-dimensional representation of $\mathrm{PSL}(2, \mathbb{F}_7)$. We have the restriction map

$$r : H^0(J^2(X), \mathcal{O}(2\Theta)) \to H^0(\Theta, \mathcal{O}_\Theta(2\Theta))$$

whose kernel is one-dimensional and is spanned by a section with the divisor of zeroes equal to 2Θ. This gives the decomposition of representations

$$H^0(J^2(X), \mathcal{O}(2\Theta)) = \mathbb{C} \oplus H^0(\Theta, \mathcal{O}_\Theta(2\Theta)). \tag{6.1}$$

Now one can show that there is a canonical isomorphism of representations

$$H^0(\Theta, \mathcal{O}_\Theta(2\Theta)) \cong H^0(\mathbb{P}(V_6), \mathcal{I}_X(2)),$$

where $\mathcal{I}_X$ is the ideal sheaf of X embedded in the space $\mathbb{P}(V_6)$ (see **[BV]**, 4.12) and $H^0(\mathbb{P}(V_6), \mathcal{I}_X(2))$ is accordingly the space of quadrics vanishing on X. Since $X \subset \mathbb{P}^5$ is projectively normal the restriction map

$$H^0(\mathbb{P}(V_6), \mathcal{O}(2)) \to H^0(X, \mathcal{O}_X(4K_X))$$

is surjective and its kernel is isomorphic to $H^0(\mathbb{P}(V_6), \mathcal{I}_X(2))$. This gives an isomorphism of representations

$$S^2(V_6) \cong H^0(\mathbb{P}(V_6), \mathcal{I}_X(2)) \oplus H^0(X, \mathcal{O}_X(4K_X)).$$

Since $S^4(V_-^*) \cong H^0(X, \mathcal{O}_X(4K_X)) \oplus \mathbb{C}$, we obtain from Lemma 6.2

$$H^0(\mathbb{P}(V_6), \mathcal{I}_X(2)) \cong V_6 \oplus \mathbb{C}.$$

Collecting everything together we get an isomorphism of $\mathrm{SL}(2, \mathbb{F}_7)$-representations

$$H^0(J^2(X), \mathcal{O}(2\Theta)) \cong \mathbb{C} \oplus \mathbb{C} \oplus V_6. \tag{6.2}$$

This shows that the set of fixed points of $\mathrm{PGL}(2, \mathbb{F}_7)$ in the linear system $|2\Theta| = \mathbb{P}(H^0(J^2(X), \mathcal{O}(2\Theta)))$ is equal to the line $\ell = \mathbb{P}(\mathbb{C} \oplus \mathbb{C})$. It remains to see that it intersects $\mathrm{SU}_X(2)$ at 3 points. One point corresponds to the trivial bundle and the other two to stable bundles. Let $\mathbb{C}$ be one of the trivial one-dimensional summands in $H^0(J^2(X), \mathcal{O}(2\Theta))$ which corresponds to $\mathrm{Ker}(r)$. It follows from the construction of Φ that the corresponding point in $|2\Theta|$ is equal to the divisor 2Θ which is the value of Φ at the trivial bundle. The map r defines a projection map $|2\Theta| \setminus \{2\Theta\} \to \mathbb{P}(H^0(\mathbb{P}(V_6), \mathcal{I}_X(2)))$ with the center at the point defined by the divisor $2\Theta \in |2\Theta|$. The line ℓ is the closure of the fibre of this projection over the $\mathrm{PSL}(2, \mathbb{F}_p)$-invariant quadric containing the curve X. This quadric can be identified with the Grassmanian $G(2, 4)$ in the Plücker space $\mathbb{P}^5$. By Proposition 1.19 and

Theorem 3.3 of **[BV]** the intersection $(\ell \setminus \{2\Theta\}) \cap \mathrm{SU}_X(2)$ consists of two stable bundles. One is the the restriction to X of the universal quotient bundle twisted by λ^{-1} and another is the dual of the restriction of the universal subbundle twisted by λ. This proves the assertion.

So we know how to construct the two stable G-invariant bundles on $X(7)$ with trivial determinant. We embed $X(7)$ in $\mathbb{P}(S^2(V_-)^*) = \mathbb{P}^5$ by $|2K_X|$. Then identify the representations $S^2(V_-)$ and $\Lambda^2(V_+)$, consider the Grassmanian $G(2, V_+)$ embedded by the Plücker map, and then restrict to $X(7)$ the universal bundle and the universal subbundle and twist them to get the trivial determinant. The ARK bundle corresponds to the universal subbundle.

The next lemma must be a special case of computations from **[AR]**, pp. 101-105, however some typographical errors make it an unsuitable reference. We refer to **[A3]** for the corrections and more general results.

Lemma 6.4. *There is an isomorphism of representations of* $\mathrm{SL}(2, \mathbb{F}_7)$*:*

$$H^0(X(7), \lambda^k) \cong \begin{cases} V_+^* & \text{if } k = 3 \\ V_8' & \text{if } k = 5 \\ V_+ \oplus V_8' & \text{if } k = 7 \\ V_+ \oplus V_6' \oplus V_6'^* & \text{if } k = 9 \end{cases}$$

where V_8' *and* V_6' *are the* 8*-dimensional and the* 6*-dimensional irreducible representations of the group* $\mathrm{SL}(2, \mathbb{F}_7)$ *on which* -1 *does not act identically.*

Proof. By a theorem of H. Hopf (cf. **[ACGH]**, p.108), given any linear map

$$f : A \otimes B \to C$$

where A, B, C are complex linear spaces and f is injective on each factor separately, then

$$\dim f(A \otimes B) \geq \dim A + \dim B - 1.$$

We apply it to the map

$$H^0(X, \lambda^2) \otimes H^0(X, \lambda^3) = V_-^* \otimes V_+^* \to H^0(X, \lambda^5).$$

Using Table 3, Appendix 2, we find that $V_-^* \otimes V_+^* \cong V_+ \oplus V_8'$. Thus $H^0(X, \lambda^5)$ must contain V_8' as its direct summand. By Riemann-Roch, it must be equal to V_8'. Similarly, considering the map

$$H^0(X, \lambda^2) \otimes H^0(X, \lambda^5) = V_-^* \otimes V_8' \to H^0(X, \lambda^7)$$

we get that its image is of dimension ≥ 10. Since, by Riemann-Roch, $H^0(X, \lambda^7)$ is of dimension 12, and $H^0(X, \lambda^5)$ does not have vectors invariant with respect to $\mathrm{SL}(2, \mathbb{F}_7)$ (use that -1 acts non-trivially) , we obtain that the multiplication map is surjective. Using Table 4, Appendix 2, we find that

$$V_-^* \otimes V_8' = V_+ \oplus V_6' \oplus V_6'^* \oplus V_8'.$$

This gives us two possibilities: $H^0(X, \lambda^7) = V_+ \oplus V_8'$ or $H^0(X, \lambda^7) = V_6' \oplus V_6'^*$. If the second case occurs, we consider the map $H^0(X, \lambda^5) \otimes H^0(X, \lambda^7) \to H^0(X, \lambda^{12})$. Here, we find that the image is of dimension ≥ 19. We know the direct sum decomposition for the 22-dimensional $\mathrm{SL}(2, \mathbb{F}_7)$-module $H^0(X, \lambda^{12})$ (see Appendix 1). It tells us that it contains exactly one one-dimensional summand. However, Tables 3 and 4 from Appendix 2 tell us that $H^0(X,\lambda^5)\otimes(V_6'\oplus V_6'^*) = V_8'\otimes(V_6'\oplus V_6'^*)$ does not contain one-dimensional summands. Hence the one-dimensional summand must be in the cokernel of the multiplication map. But since the cokernel is of dimension ≤ 3 and $\mathrm{SL}(2,\mathbb{F}_7)$ does not have two-dimensional irreducible representations, we get a contradiction. Therefore $H^0(X,\lambda^7) = V_+ \oplus V_8'$.

Finally $|\lambda^9|$ is cut out by the linear system of cubics in $\mathbb{P}(V_+)$. We know from Table 2, Appendix 1, that $S^3(V_+)^* = V_+ \oplus V_+^* \oplus V_6' \oplus V_6'^*$. The linear system of cubics spanned by the polars of the unique invariant quartic in $\mathbb{P}(V_+)$ realizes the summand V_+. The A-curve $X(7)$ is contained in a linear system of cubics isomorphic to V_+^*. This implies that $H^0(X,\lambda^9) \cong V_+ \oplus V_6' \oplus V_6'^*$.

The next lemma concerns the even powers of λ:

Lemma 6.5. *Let $\mathcal{R}$ be the representation ring of* $\mathrm{SL}(2,\mathbb{F}_7)$. *Then we have the following identity in the ring $R[[t]]$:*

$$\sum_{n=0}^{\infty} H^0(X(7),\lambda^{2n})t^n = (1-t^4)\sum_{n=0}^{\infty} S^n(V_-)^* t^n.$$

Proof. It suffices to remark that the ring $\sum_{n=0}^{\infty} H^0(X(7),\lambda^{2n})$ is the coordinate ring of the Klein quartic, and the ring $\sum_{n=0}^{\infty} S^n(V_-)^*$ is the coordinate ring of the projective plane.

Theorem 6.6. *The ARK bundle E over $X(7)$ is stable and is isomorphic to $N^* \otimes \lambda^5$, where N is the normal bundle of the A-curve $X(7)$ in $\mathbb{P}(V_+) = \mathbb{P}^3$.*

Proof. The stability of E immediately follows from Theorem 5.2 since we have $H^0(X(7),\lambda^2) = V_-$. By definition of the normal bundle we have the following exact sequences of $\mathrm{SL}(2,\mathbb{F}_7)$-linearized bundles over X

$$0 \to \lambda^{-2} \to T \to N \to 0,$$

$$0 \to \mathcal{O}_X \to V_+ \otimes \lambda^3 \to T \to 0,$$

where T is the tangent bundle of $\mathbb{P}^3$. Combining them together we get an exact sequence

$$0 \to F \to V_+ \otimes \lambda^3 \to N \to 0, \tag{6.3}$$

where

$$0 \to \mathcal{O}_X \to F \to \lambda^{-2} \to 0. \tag{6.4}$$

First we see that

$$\det(N) = \lambda^{12} \otimes \det F^{-1} = \lambda^{12} \otimes \lambda^2 = \lambda^{14}.$$

Twisting (6.3) by λ^{-5}, we get

$$0 \to F \otimes \lambda^{-5} \to V_+ \otimes \lambda^{-2} \to N' \to 0, \tag{6.5}$$

where $N' = N \otimes \lambda^{-5}$ with $\det N' = \lambda^4 = K_X^2$. I claim that $N' = E^*$. Taking the exact sequence of cohomology for (6.5) we get

$$H^0(X,N') = \mathrm{Ker}(H^1(X,F\otimes\lambda^{-5}) \to H^1(X,V_+\otimes\lambda^{-2}). \tag{6.6}$$

Tensoring (6.4) with λ^{-5} and taking cohomology we obtain

$$0 \to H^1(X,\lambda^{-5}) \to H^1(X,F\otimes\lambda^{-5}) \to H^1(X,\lambda^{-7}) \to 0. \tag{6.7}$$

Everything here is in the category of $\mathrm{SL}(2,\mathbb{F}_7)$-modules. By Serre's duality

$$H^1(X,\lambda^{-5}) \cong H^0(X,\lambda^7)^*, \quad H^1(X,\lambda^{-7}) \cong H^0(X,\lambda^9)^*. \tag{6.8}$$

Applying Lemma 6.4 to (6.8) and using (6.7), we get

$$H^1(X,F\otimes\lambda^{-5}) \cong V_+^* \oplus V_+^* \oplus V_8' \oplus V_6' \oplus V_6'^*. \tag{6.9}$$

Now, using Table 3 from Appendix 2 and Lemma 6.5, we obtain

$$H^1(X,V_+\otimes\lambda^{-2}) = V_+ \otimes H^1(X,\lambda^{-2}) =$$

$$V_+\otimes H^0(X,\lambda^4)^* = V_+\otimes V_6 = V_+^* \oplus V_8' \oplus V_6' \oplus V_6'^*. \tag{6.10}$$

The sequence (6.6) and a comparison of (6.9) and (6.10) gives us a summand V_+^* in $H^0(X,N')$ and defines a nonzero map of vector bundles

$$\psi : V_+^* \otimes \mathcal{O}_X \to N'.$$

Assume the image of ψ spans a line subbundle. Then N' contains a line subbundle L of the form λ^a. Since V_+ is irreducible, it maps injectively into $H^0(X,\lambda^a)$, hence $a \geq 3$. In fact, using Lemmas 6.4 we find that $a = 3$ or $a \geq 11$. Using the exact sequences (6.3) and (6.4) it is easy to see that $\dim H^0(X,N) = 24$. Since $\lambda^{a+5} \subset N$, we see that the case $a \geq 11$ is impossible. So $a = 3$. This also gives that L is saturated in N', i.e. the quotient N/L is torsion free (otherwise we find a G-invariant line subbundle of N' strictly containing λ^3). Since $\det N' = \lambda^4$, we obtain that $N'/L \cong \lambda$. But then we have an extension

$$0 \to \lambda^8 \to N \to \lambda^6 \to 0.$$

This easily gives, using Lemma 6.5 and Table 2 from Appendix 1, that $H^0(X,N)^G = h^0(X,\lambda^6)^G \cong \mathbb{C}$. The exact sequence (6.4) gives $H^0(X,F)^G = \mathbb{C}, H^1(X,F)^G = 0$, and the exact sequence (6.3), together with the decomposition $V_+ \otimes H^0(X,\lambda^3) = V_+\otimes V_+^* = \mathbb{C}\oplus V_7 \oplus V_8$ from Table 3 of Appendix 2, gives that $H^0(X,N)^G = 0$.

This contradiction proves that the image of ψ generates a rank 2 subbundle of N'. Thus the cokernel of ψ is concentrated over a finite set of points in $X(7)$ contained in the set S of zeroes of $s \wedge s'$ for some sections of $\Lambda^2(N')$. However, $\Lambda^2(N') = K_X^2$ and hence S consists of at most 8 points. Since S is obviously G-invariant, this is impossible. So ψ is surjective. This implies that N' defines an equivariant embedding of $X(7)$ in $G(2,V_+)$. The composition of this embedding with the Plücker map is given by $|2K_X|$ and, hence is defined uniquely (since there is only one equivariant isomorphism $S^2(V_-)^* \cong \Lambda^2(V_+)^*$). This shows that the restriction of the universal subbundle on the Grassmannian to the image of $X(7)$ coincides with the ARK bundle. Hence N'^* is this bundle.

Remark 6.7 Since the condition of stability is open we get a curious fact that the normal bundle of a general sextic curve of genus 3 in $\mathbb{P}^3$ is stable. I do not know whether it was previously known.

Theorem 6.8. *Let E be the ARK bundle over $X(7)$. Then there is an exact sequences of* $\mathrm{SL}(2,\mathbb{F}_7)$*-linearized bundles:*

$$0 \to E\otimes\lambda^{-3} \to V_-\otimes\mathcal{O}_X \to \lambda^{10} \to 0, \tag{6.11}$$

$$0 \to \lambda^{-11} \to E\otimes\lambda \to \lambda^{11} \to 0. \tag{6.12}$$

Proof. Let N be the normal bundle of the A-curve $X(7)$. Tensoring (6.3) with λ^{-2} we find the exact sequence

$$0 \to F \otimes \lambda^{-2} \to V_+ \otimes \lambda \to N \otimes \lambda^{-2} \to 0. \tag{6.13}$$

Taking cohomology we easily get

$$H^0(X, N \otimes \lambda^{-2}) = H^1(X, F \otimes \lambda^{-2}) = H^1(X, \lambda^{-2}) \oplus H^1(X, \lambda^{-4}) =$$
$$H^0(X, \lambda^4)^* \oplus H^0(X, \lambda^6)^* = V_6 \oplus V_-^* \oplus V_7. \tag{6.14}$$

This defines a map of sheaves $\psi : V_-^* \otimes \mathcal{O}_X \to N \otimes \lambda^{-2}$. Assume that its image generates a line subbundle. Using the same argument as in the proof of Theorem 6.6 we get that $N \otimes \lambda^{-2}$ fits in the exact sequence

$$0 \to \lambda^2 \to N \otimes \lambda^{-2} \to \lambda^8 \to 0.$$

Taking the global sections and using (6.14) we obtain that the representation $V_6 \oplus V_7$ is a direct summand of $H^0(X, \lambda^8) \cong V_6 \oplus V_8$. This is impossible. Thus the image of ψ generates a subbundle of rank 2 of $\det N \otimes \lambda^{-2} = \lambda^{10}$. Since there are no G-invariant subsets in $X(7)$ of cardinality $\leq \deg \lambda^{10} = 20$, we conclude that this map is surjective. Thus we have an exact sequence

$$0 \to \lambda^{-10} \to V_-^* \otimes \mathcal{O}_X \to N \otimes \lambda^{-2} \to 0.$$

After dualizing and using Theorem 6.6, we obtain the sequence (6.11).

To get (6.12), we twist (6.13) by λ^6 to obtain

$$0 \to F \otimes \lambda^4 \to V_+ \otimes \lambda^7 \to N \otimes \lambda^4 \to 0. \tag{6.15}$$

The exact sequence

$$0 \to \lambda^4 \to F \otimes \lambda^4 \to \lambda^2 \to 0$$

gives

$$H^1(X, F \otimes \lambda^4) = H^1(X, \lambda^2) = \mathbb{C}, \quad H^0(X, F \otimes \lambda^4) = V_6 \oplus V_-^*.$$

Since $H^1(X, V_+ \otimes \lambda^7) = 0$, we obtain that $H^0(X, N \otimes \lambda^4)$ is mapped surjectively onto $H^1(X, F \otimes \lambda^4)$, and hence contains a G-invariant section. This section defines a non-trivial (and hence injective) map of sheaves $\mathcal{O}_X \to N \otimes \lambda^4$ and hence an injective map

$$\lambda^{-11} \to N \otimes \lambda^{-7} = E \otimes \lambda.$$

The cokernel of this map does not have torsion since otherwise its support will be a G-invariant subset of cardinality $\leq \deg \lambda^{11} = 22$. The smallest cardinality of a G-invariant set on $X(7)$ is 24. Thus the cokernel is isomorphic to λ^{11}.

Remark 6.9 The exact sequence (6.11) can be defined as follows. We have a linear system of curves of degree 5 which are polars of a unique G-invariant sextic in $\mathbb{P}(V_-)$. This defines a map $V_- \to H^0(X, \mathcal{O}_X(K_X^5)) = H^0(X, \lambda^{10})$ and also a surjective map $V_- \otimes \mathcal{O}_X \to \lambda^{10}$.

Remark 6.10 Let E be the ARK bundle over $X(7)$. The ruled surface $\mathbb{P}(E)$ can be projected to $\mathbb{P}(V_+)$ with the image equal to the tri-secant scroll S of the A-curve $X(7)$. Recall that any even-theta characteristic θ on a canonical curve X of genus 3 defines a (3-3)-correspondence R on X (see, for example, **[DK]**, p.277):

$$R = \{(x, y) \in X \times X : |\theta + x - y| \neq \emptyset\}.$$

The set $R(x)$ consists of points in the unique positive divisor equivalent to $\theta + x$. Let X' be the image of X in $\mathbb{P}^3$ under the map given by the complete linear system $|3\theta|$. Since $|3\theta - (\theta + x)| = |2\theta - x| = |K_X - x|$ is a pencil, we obtain that the image of $R(x)$ lies on a line $< R(x) >$. This is a tri-secant line of X'. When x runs over the set of points of X, the tri-secant lines form a scroll S containing X' as a singular curve of multiplicity 3. The map $x \to < R(x) >$ defines an embedding of X in $G(2,4)$. This scroll also can be described as follows (see **[SR]**, pp. 179-180, or **[Hu]**, pp. 294-306). The linear system of cubics through X' is of dimension 3 and defines a birational transformation of $\mathbb{P}^3$ to $\mathbb{P}^3$. It factors through the blow-up $Y \to \mathbb{P}^3$ of X' and the blow-down of the proper inverse transform S' of S to X' in another copy of $\mathbb{P}^3$. This shows that S' is isomorphic to the projectivization of the normal bundle of X'. In our case the tri-secant scroll S is a surface in $\mathbb{P}(V_+)$ defined by an invariant polynomial of degree 8 (see **[E1]**, pp.202-205). Also in our case the correspondence R on $X(7)$ is a modular correspondence T_2. This was discovered by F. Klein **[Kl3]**, footnote 16, pp.177-178 (see also **[A2]**).

What is the second stable G-invariant bundle with trivial determinant over $X(7)$? It is very well-known. It can be described, for example, as follows. Embed $X(7)$ into the Jacobian $\mathrm{Jac}^1(X)$ and take the normal bundle tensored with λ^{-1}. In other words, consider a natural bijective map $V_-^* \to H^0(X, \mathcal{O}_X(K_X))$. It defines an exact sequence

$$0 \to E' \to V_-^* \otimes \mathcal{O}_X \to \lambda^2 \to 0. \tag{6.16}$$

Then $E = E' \otimes \lambda$ is a G-invariant rank 2 bundle with trivial determinant.

Another way to see it is to restrict the tangent bundle of $\mathbb{P}(V_-)$ to the Klein quartic. This bundle is $E \otimes \lambda^3$.

Theorem 6.11. *Let $E = E' \otimes \lambda$, where E' is defined by the exact sequence (6.16). Then E is a stable rank 2 G-invariant bundle over $X(7)$ which admits a non-split G-invariant extension*

$$0 \to \lambda^{-5} \to E \to \lambda^5 \to 0. \tag{6.17}$$

Proof. Twisting (6.11) by λ^6 we obtain the exact sequence

$$0 \to E \otimes \lambda^5 \to V_-^* \otimes \lambda^6 \to \lambda^8 \to 0. \tag{6.18}$$

This gives

$$H^0(X, E \otimes \lambda^5) = \mathrm{Ker}(V_-^* \otimes H^0(X, \lambda^6) \to H^0(X, \lambda^8)) =$$

$$\mathrm{Ker}(V_-^* \otimes (V_- \oplus V_7) \to V_6 \oplus V_8),$$

where V_7 and V_8 are the 6-dimensional and the 8-dimensional irreducible representations of the group $\mathrm{PSL}(2, \mathbb{F}_7)$. Since $V_-^* \otimes V_-$ contains a one-dimensional summand, we find a G-invariant section of $E \otimes \lambda^5$. This gives a G-invariant inclusion λ^{-5} in E, and hence the extension (6.17).

Now let us check the stability of E. Assume that E is not stable. Then it must contain a G-invariant destabilizing subbundle λ^a for some $a \geq 0$. Twisting (6.16) by λ^{1-a} we obtain an extension

$$0 \to E \otimes \lambda^{-a} \to V_- \otimes \lambda^{1-a} \to \lambda^{3-a} \to 0,$$

where $H^0(X, E \otimes \lambda^{-a}) \neq 0$. However $H^0(X, V_- \otimes \lambda^{1-a})$ does not have $\mathrm{SL}(2, \mathbb{F}_7)$-invariant sections when $a \geq 0$. This proves that E is stable.

We denote by $E_{(-5,5)}$ and $E_{(-11,11)}$ the two non-isomorphic stable G-invariant rank 2 bundles with trivial determinant over $X(7)$ with corresponding exponential sequences. Notice that the exponential sequences agree with Theorem 4.2 and Corollary 4.3. As we know from the proof of Corollary 6.3 the bundles $E_{(-11,11)}$ and $E_{(-5,5)}$ arise as the restrictions of the universal subbundle and the universal quotient bundle on the Grassmanian $G(2, V_+)$. In other words they are dual in the following sense: there exists an exact sequence

$$0 \to E_{(-11,11)} \otimes \lambda^{-2} \to V_+ \otimes \mathcal{O}_X \to E_{(-5,5)} \otimes \lambda^2 \to 0 \tag{6.19}$$

We have seen already that $E_{(-11,11)} \otimes \lambda^{-2}$ is the ARK bundle and its projectivization is a non-singular model of the tri-secant scroll of the A-curve $X(7)$. The projectivization of the bundle $E_{(-5,5)} \otimes \lambda^{-2} = (E_{(-5,5)} \otimes \lambda^2)^*$ is a nonsingular model of a scroll S^* in the dual space V_+^*. We can change the roles of V_+ and V_+^* by changing the action of $\mathrm{PSL}(2, \mathbb{F}_7)$ on $X(7)$ via an outer automorphism of the group. Then we consider S^* as a scroll of degree 8 in the A-space invariant with respect to $\mathrm{PSL}(2, \mathbb{F}_7)$. It is equal to the Hessian of the quartic G-invariant surface in $\mathbb{P}(V_+)$ (see **[E1]**, pp.202-205).

Remark 6.12 There are some natural non-stable G-invariant rank 2 bundles over $X(7)$. For example, the bundle F which is defined by the (non-split) exact sequence (6.4). Tensoring with λ we see that F is unstable. A sequence of exponents of $F \otimes \lambda$ is equal to $(1, -1)$. The same bundle can be obtained by a construction similar to the construction of $E_{(-5,5)}$ and $E_{(-11,11)}$. Using the polar linear system of the Klein quartic we realize V_3 as a submodule of $S^3(V_3)^*$ and obtain an exact sequence

$$0 \to E' \to V_- \otimes \mathcal{O}_X \to \lambda^6 \to 0.$$

The bundle $E = E' \otimes \lambda^3$ is a G-invariant rank 2 bundle with trivial determinant. To see that it is unstable we use that

$$H^0(X, E \otimes \lambda^{-1}) = \mathrm{Ker}(V_- \otimes H^0(X, \lambda^2) \to H^0(X, \lambda^8)) =$$

$$\mathrm{Ker}(V_- \otimes V_-^* \to V_6 \oplus V_8) = \mathrm{Ker}(\mathbb{C} \oplus V_8 \to V_6 \oplus V_8) \supset \mathbb{C}.$$

This shows that E contains λ as its subbundle. It is easy to see that the quotient is the line bundle λ^{-1} and the corresponding extension does not split. Since $\mathrm{Ext}^1(\lambda^{-1}, \lambda) = H^1(X, \lambda^2) = \mathbb{C}$, we obtain that E is isomorphic to $F \otimes \lambda$.

7. Example: $p = 7, r = 3$

We use the following result from **[Bo]**, p. 214 (cf. Fig.3 on p.213):

Theorem 7.1. *Let $p = 6n \pm 1$. The number of irreducible 3-dimensional unitary representation of the Brieskorn sphere $\Sigma(2, 3, p)$ is equal to $3n^2 \pm n$. All these representations are trivial on the center of $\pi_1(\Sigma(2, 3, p))$.*

Applying Theorem 3.7, we obtain

Corollary 7.2. *Let $p = 6n \pm 1$ and $G = \mathrm{PSL}(2, \mathbb{F}_p)$. There are exactly $3n^2 \pm n$ non-isomorphic G-stable rank 3 bundles with trivial determinant over $X(p)$. Moreover each such a bundle admits a unique G-linearization. If $p \neq 7$ each G-stable bundle* *of rank 3 and trivial determinant decomposable as the direct sum of stable bundles is stable (and hence indecomposable).*

Proof. Only the last assertion does not follow immediately from Theorem 7.1 and Theorem 3.7. Let us prove it. Suppose that $E = \oplus E_i$ is G-stable but not stable. Since E is G-stable we see immediately that each summand must be of rank 1 and of degree 0. Since there are no nontrivial G-invariant line bundles of degree 0 on $X(p)$ we obtain that either E is trivial, and hence is defined by a 3-dimensional representation of $\mathrm{SL}(2, \mathbb{F}_p)$. It is possible only for $p = 7$. In this case E must be trivial.

Remark 7.3. As was pointed out to me by A. Adler the previous argument shows more: If $G = \mathrm{SL}(2, \mathbb{F}_p)$ has no nontrivial permutation representation of prime degree r then there is a bijection between the set of strictly semistable points in $\mathrm{SU}_{X(p)}(r)^G$ and the set of irreducible representations of degree r of G.

Let us assume $p = 7$. We need to exhibit four rank 3 G-stable vector bundles with trivial determinant over $X(7)$. This is easy. First of all we take the two rank 2 bundles $E_{(-5,5)}$ and $E_{(-11,11)}$ and consider their second symmetric powers $S^2(E_{(-5,5)}), S^2(E_{(-11,11)})$. The other two are obtained by considering the trivial bundles $V_- \otimes \mathcal{O}_X, V_-^* \otimes \mathcal{O}_X$ with linearizations defined by two irreducible 3-dimensional representations of G. It is easy to compute their sequences of exponents (a_1, a_2, a_3):

Theorem 7.4. *We have*

$$(a_1, a_2, a_3) = \begin{cases} (-10, 0, 10) & \text{if } E = S^2(E_{(-5,5)}) \\ (-22, 0, 22) & \text{if } E = S^2(E_{(-11,11)}) \\ (-2, -4, 6) & \text{if } E = V_- \otimes \mathcal{O}_X \\ (-6, 4, 2) & \text{if } E = V_-^* \otimes \mathcal{O}_X. \end{cases}$$

Proof. The first two sequences can be immediately computed from the known sequences of exponents of the rank 2 bundles. To compute the third sequence we use that $H^0(X, V_- \otimes \lambda^2) = V_- \otimes V_-^*$ contains a trivial summand. This implies that E contains a G-linearized subbundle isomorphic to λ^{-2}. Using Theorem 6.11 and the dual of the exact sequence (6.16) we see that the quotient F is isomorphic to $E_{(-5,5)} \otimes \lambda$. Now we use that $(-4, 6)$ is a sequence of exponents for $E_{(-5,5)} \otimes \lambda$. By the sentence preceding Proposition 3.3, $(-6, 4, 2)$ is then a sequence of exponents for $V_-^* \otimes \mathcal{O}_X$.

Remark 7.5 The first two bundles correspond to unitary representations of the group $\pi_1(\Sigma(2, 3, 7))$ which arise from a representation $\rho : \pi_1 \to \mathrm{SO}(3) \subset \mathrm{SU}(3)$. The remaining two bundles correspond to "additional" ([**Bo**], p.211) irreducible representations. The new information here is that the additional representations factor through an irreducible representation of $\mathrm{PSL}(2, \mathbb{F}_7)$. This was verified directly by H. Boden.

We have a canonical exact sequence corresponding to the embedding of $X(7)$ as the A-curve:

$$0 \to E' \to V_+^* \otimes \mathcal{O}_X \to \lambda^3 \to 0 \tag{7.1}$$

Twisting by λ we obtain a rank 3 G-invariant bundle E with trivial determinant. One can show that $E \cong S^2(E_{(-11,11)})$.

Similarly, the exact sequence

$$0 \to E' \to V_+^* \otimes \mathcal{O}_X \to \lambda^9 \to 0$$

defined by the polar linear system of the $\mathrm{SL}(2, \mathbb{F}_7)$-invariant quartic surface in the A-space defines the G-invariant rank 3 bundle $E = E' \otimes \lambda^3$ with trivial determinant. Once can show that it is isomorphic to $S^2(E_{(-5,5)})$.

8. Example: $p = 11, r = 2$

By Theorem 3.11 we expect to find four non-isomorphic $\mathrm{PSL}(2, \mathbb{F}_{11})$-invariant stable bundles of rank 2 with trivial determinant. Here we have of course the ARK bundle which is stable if one checks that $V_+^* \not\subset H^0(X(11), \lambda^a)$ for $a \leq 4$. Assume $H^0(X(11), \lambda^4)$ contains V_+. Since it contains already V_-^* we would have $\dim H^0(X(11), \lambda^4) \geq 11$. This contradicts the Clifford theorem (see **[ACGH]**, p. 107). The same theorem implies that $V_+^* \not\subset H^0(X(11), \lambda^a)$ for $a \leq 2$. So, it remains to verify that $V_+^* \not\subset H^0(X(11), \lambda^3)$. We use the following fact from the theory of algebraic curves (cf. **[ACGH]**, Exercise E-1, p.198, there is a misprint in the formula, and I think some assumptions must be added too):

Lemma 8.1. *Let C be a compact Riemann surface of genus g and L be a line bundle on C of degree $d \leq g - 1$. Assume that the complete linear system $|L|$ is of dimension $r > 0$ and base-point-free. Then*

$$2d \geq g + 2r - \dim H^0(C, K_C \otimes L^{-2}).$$

Proof. Let W_r^d denote the subvariety of $\mathrm{Jac}^d(C)$ whose support is the set of line bundles M of degree d with $\dim H^0(M, L) \geq r + 1$. By Proposition 4.2 of **[ACGH]**, p. 189, we have the following formula for the dimension of the tangent space of W_d^r:

$$\dim T_L(W_d^r) = g - \dim \mathrm{Image}\ \mu_0, \tag{8.1}$$

where

$$\mu_0 : H^0(C, L) \otimes H^0(C, K_C \otimes L^{-1}) \to H^0(C, K_C)$$

is the natural map. Let $V \subset H^0(C, L)$ corresponding to a base-point-free subpencil of $|L|$. Applying the base-point-free pencil trick (loc. cit., p.126), we obtain that the kernel of the restriction of the map μ_0 to $V \otimes H^0(C, K_C \otimes L^{-1})$ is isomorphic to $H^0(C, K_C \otimes L^{-2})$. Thus

$$\dim \mathrm{Image}\ \mu_0 \geq 2 \dim H^0(C, K_C \otimes L^{-1}) - \dim H^0(C, K_C \otimes L^{-2}).$$

Using (8.1) and the Riemann-Roch Theorem we get

$$0 \leq \dim T_L(W_d^r) \leq g - (2 \dim H^0(C, K_C \otimes L^{-1}) - \dim H^0(C, K_C \otimes L^{-2}) =$$

$$g - 2(\dim H^0(C, L) - d - 1 + g) + \dim H^0(C, K_C \otimes L^{-2}) =$$

$$-g - 2r + 2d + \dim H^0(C, K_C \otimes L^{-2}).$$

This is the asserted inequality.

Theorem 8.2. *The ARK-bundle on $X(11)$ is stable.*

Proof. As we have noticed before we have to check that $H^0(X(11), \lambda^3)$ does not contain V_+^* as a direct summand. Assume this is not true. Since $\deg \lambda^3 = 15$, the complete linear system $|\lambda^3|$ has no base points (otherwise we find a G-invariant subset of X(11) of cardinality ≤ 15). Applying the previous Lemma we have

$$30 \geq 26 + 2\dim H^0(X(11), \lambda^3) - 2 - \dim H^0(X(11), \lambda^4) \geq 36 - \dim H^0(X(11), \lambda^4).$$

This implies that $\dim H^0(X(11), \lambda^4) \geq 6$. Since $H^0(X(11), \lambda^4)$ already contains V_- of dimension 5 we have $\dim H^0(X(11), \lambda^4) \geq 10$ (notice that $H^0(X(11), \lambda^4)^G = \{0\}$ since otherwise X contains a G-invariant subset of cardinality 20 which as is easy to see does not exist on $X(11)$). By Clifford's theorem dim $|\lambda^4| < \frac{1}{2}\deg \lambda^4 = 10$. Thus $\dim H^0(X(11), \lambda^4) = 10$. The complete linear system $|\lambda^4|$ maps $X(11)$ onto a curve C in $\mathbb{P}^9$. Its projection to $\mathbb{P}^4$ given by the linear subsystem $|V_-|$ of $|\lambda^4|$ is the Klein z-curve $X(11)$ of degree 20 and genus 26. This implies that C is also of degree 20 and genus 26. This contradicts the Castelnuovo bound for the genus of a curve of degree d in $\mathbb{P}^r$([**ACGH**], p. 116):

$$g \leq \frac{m(m-1)}{2}(r-1) + me,$$

where $d - 1 = m(r-1) + e$ for some positive integers m and e with $0 \leq e < r - 1$.

Note that the assertion that $H^0(X(11), \lambda^3)$ does not contain V_+^* was independently checked by A. Adler by the methods of [**AR**], App. III (see [**A4**]). In fact he also shows that this assertion follows from the equality dim $H^0(X(11), \lambda^4) = 5$ and the latter is equivalent to the fact that there is only one G-equivariant morphism of $X(11)$ onto a curve of degree 20 in $\mathbb{P}^4$.

Another potential candidate is the vector bundle defined by using the fact that the z-curve $X(11)$ parametrizes polar quadrics of corank 2 of the invariant cubic hypersurface W (see Example 2.9). This defines a bundle with determinant λ^6 which embeds $X(11)$ in $G(2, V_-)$. The corresponding ruled surface in $\mathbb{P}(V_-)$ is the four-secant scroll of the z-curve $X(11)$ of degree 30 (see [**E2**], p. 65). Similar to the tri-secant scroll of $X(7)$ it is defined by a modular $(4,4)$-correspondence on $X(11)$ (see [**A2**], Theorem 1, p.433).

To introduce the third candidate, we use that the cubic hypersurface W admits a G-invariant representation as the Pfaffian hypersurface (see [**AR**], p. 164):

$$v^2w + w^2x + x^2y + y^2z + z^2v = \mathrm{P}f \begin{pmatrix} 0 & v & w & x & y & z \\ -v & 0 & 0 & z & -x & 0 \\ -w & 0 & 0 & 0 & v & -y \\ -x & -z & 0 & 0 & 0 & w \\ -y & x & -v & 0 & 0 & 0 \\ -z & 0 & y & -w & 0 & 0 \end{pmatrix}. \qquad (8.1)$$

This representation is obtained by considering a linear map $V_- \to S^2(V_-^*)$ defined by the polar linear system of W and then identifying the representations $S^2(V_-^*)$ and $\Lambda^2(V_+)^*$ (see Theorem 5.1). The cubic hypersurface W is equal to the pre-image of the cubic hypersurface in $\mathbb{P}(\Lambda^2(V_+)^*)$ which coincides with the chordal variety C of the Grassmanian $G(2, V_+^*)$. The latter carries a canonical rank 2 bundle whose fibre over a point $t \in C$ is equal to the null-space $L_t \subset V_+$ of the corresponding skew-symmetric matrix. To get a bundle over $X(11)$ we use the decomposition of $\mathrm{PSL}(2, \mathbb{F}_{11})$-representations

$$H^0(X, K_X) = V_- \oplus V_{10} \oplus V_{11}, \qquad (8.2)$$

where V_{10} and V_{11} are 10-dimensional and 11-dimensional irreducible representations of $\mathrm{PSL}(2,\mathbb{F}_{11})$ (see **[He]**). This decomposition allows us to project $X(11)$ to $\mathbb{P}(V_-)$ as a curve of degree 50. It turns out that the image of the projection is contained in the cubic W. This result is due to F. Klein **[KF]**, p. 413, and is reproduced by A. Adler (see **[AR]**, Appendix 3). This allows us to restrict the bundle E to obtain a G-invariant bundle over $X(11)$. This bundles embeds $X(11)$ in $G(2,V_+)$ by the linear system of quadrics spanned by the Pfaffians of order four principal submatrices of the skew-symmetric matrix from (8.1). So, the determinant of the bundle is equal to λ^8.

Note a beautiful result of M. Gross and S. Popescu **[GP]** who show that the cubic Wwhich establishes a natural birational isomorphism between the cubic W and a compactification of the moduli space of abelian surfaces with polarization of type $(1,11)$. Using this one could probably see in another way how $X(11)$ embeds in $\mathbb{P}(V_-)$ as a curve of degree 50.

Finally one may try to consider the normal bundle of $X(11)$ in the cubic W. I do not know yet whether any of the last three bundles is stable, nor do I know their sequence of exponents. I also do not know the sequence of exponents of the ARK-bundle.

Appendix 1. Decompositions of $S^n(V_-)$ and $S^n(V_+)$ for $p = 7$

It follows from the character table of the groups $\mathrm{SL}(2,\mathbb{F}_p)$ (see, for example, **[D]**, vol. B, pp. 498-499) that $\mathrm{SL}(2,\mathbb{F}_7)$ has eleven non-isomorphic irreducible representations. In the following we denote by V_k the irreducible representation of $\mathrm{SL}(2,\mathbb{F}_7)$ of dimension k and by V_k' another representation of the same dimension which does not factor through $\mathrm{PSL}(2,\mathbb{F}_7)$. We assume that

$$V_- = V_3, \quad V_+ = V_4.$$

The following generating function was computed in **[BI]**):

$$Q_V(t) = \sum_{t=0}^{\infty} \dim_{\mathbb{C}} \mathrm{Hom}^{\mathrm{PSL}(2,\mathbb{F}_7)}(V, S^n(V_-))t^n.$$

We have

$$Q_{V_1}(t) = \frac{1+t^{21}}{(1-t^4)(1-t^6)(1-t^{14})},$$
$$Q_{V_3}(t) = \frac{t+t^7+t^{11}+t^{13}}{(1-t^4)(1-t^7)(1-t^8)},$$
$$Q_{V_3^*}(t) = \frac{t^3+t^5+t^9+t^{15}}{(1-t^4)(1-t^7)(1-t^8)},$$
$$Q_{V_6}(t) = \frac{t^2+t^8}{(1-t^2)(1-t^4)(1-t^7)},$$
$$Q_{V_7}(t) = \frac{t^3}{(1-t^2)(1-t^3)(1-t^4)},$$
$$Q_{V_8}(t) = \frac{t^4}{(1-t)(1-t^3)(1-t^7)}.$$

Using the similar arguments one can compute the generating function

$$P_V(t) = \sum_{t=0}^{\infty} \dim_{\mathbb{C}} \mathrm{Hom}^{\mathrm{SL}(2,\mathbb{F}_7)}(V, S^n(V_+))t^n.$$

We have

$$P_{V_1}(t) = \frac{1+t^8+t^{10}+t^{12}+t^{16}+t^{18}+t^{20}+t^{28}}{(1-t^4)(1-t^6)(1-t^8)(1-t^{14})},$$

$$P_{V_3}(t) = \frac{t^2-t^4+t^6+2t^8+t^{12}+2t^{14}+2t^{18}}{(1-t^2)(1-t^4)(1-t^8)(1-t^{14})},$$

$$P_{V_3^*}(t) = \frac{2t^6+2t^{10}+t^{12}+2t^{16}+t^{18}-t^{20}+t^{22}}{(1-t^2)(1-t^4)(1-t^8)(1-t^{14})},$$

$$P_{V_6}(t) = \frac{2t^4+t^8+2t^{10}+t^{12}+2t^{16}}{(1-t^2)(1-t^4)^2(1-t^{14})},$$

$$P_{V_7}(t) = \frac{t^2+t^4+2t^6+2t^{10}+t^{12}+t^{14}}{(1-t^2)(1-t^4)(1-t^6)(1-t^8)},$$

$$P_{V_8}(t) = \frac{t^4+t^6+2t^8+2t^{12}+t^{14}+t^{16}}{(1-t^2)^2(1-t^6)(1-t^{14})},$$

$$P_{V_4}(t) = \frac{t-t^3+t^5+2t^9-t^{11}+t^{13}+t^{17}}{(1-t^2)^2(1-t^6)(1-t^{14})},$$

$$P_{V_4^*}(t) = \frac{t^3+t^7-t^9+2t^{11}+t^{15}-t^{17}+t^{19}}{(1-t^2)^2(1-t^6)(1-t^{14})},$$

$$P_{V_6'}(t) = P_{V_6'^*}(t) = \frac{t^3+2t^9+t^{15}}{(1-t^2)^2(1-t^4)(1-t^{14})},$$

$$P_{V_8'}(t) = \frac{2t^5+t^7+t^9+t^{11}+t^{13}+2t^{15}}{(1-t^2)^2(1-t^6)(1-t^{14})}.$$

A suspicious reader may check (for example using Maple) that

$$P_{V_1}(t)+3P_{V_3}(t)+3P_{V_3^*}(t)+6P_{V_6}(t)+7P_{V_7}(t)+8P_{V_8}(t)+4P_{V_4}(t)+$$
$$4P_{V_4^*}(t)+12P_{V_6'}(t)+8P_{V_8'}(t) = \sum_{n=0}^{\infty} \dim S^n(V_+)t^n = \frac{1}{(1-t^4)}.$$

The generating functions $P_V(t)$ and $Q_V(t)$ allows one, in principle, decompose any symmetric power $S^n(V_-^*)$ or $S^n(V_+^*)$ in irreducible representations of $\mathrm{SL}(2,\mathbb{F}_7)$. We give a few examples:

$S^2(V_3)^*$	$=$	V_6
$S^3(V_3)^*$	$=$	V_3+V_7
$S^4(V_3)^*$	$=$	$V_1+V_6+V_8$
$S^5(V_3)^*$	$=$	$V_3+V_3^*+V_7+V_8$
$S^6(V_3)^*$	$=$	$V_1+2\cdot V_6+V_7+V_8$
$S^7(V_3)^*$	$=$	$V_3+V_3^*+2\cdot V_7+2\cdot V_8$
$S^8(V_3)^*$	$=$	$V_1+V_3^*+3\cdot V_6+V_7+2\cdot V_8$
$S^9(V_3)^*$	$=$	$2\cdot V_3+2\cdot V_3^*+V_6+3\cdot V_7+2\cdot V_8$
$S^{10}(V_3)^*$	$=$	$V_1+V_3+4\cdot V_6+2\cdot V_7+3\cdot V_8$
$S^{11}(V_3)^*$	$=$	$2\cdot V_3+2\cdot V_3^*+V_6+4\cdot V_7+4\cdot V_8$

Table 1: Decomposition of $S^n(V_3^*)$

$$\begin{array}{rcl}
S^2(V_4)^* &=& V_3+V_7\\
S^3(V_4)^* &=& V_4+V_4^*+V_{6'}+V_{6'}^*\\
S^4(V_4)^* &=& V_1+2\cdot V_6+2\cdot V_7+V_8\\
S^5(V_4)^* &=& 2\cdot V_4+2\cdot V_4^*+2\cdot V_{6'}+2\cdot V_{6'}^*+2\cdot V_{8'}\\
S^6(V_4)^* &=& V_1+2\cdot V_3+2\cdot V_3^*+2\cdot V_6+5\cdot V_7+3\cdot V_8
\end{array}$$

Table 2: Decomposition of $S^n(V_4^*)$

To deduce from this the decompositions for $H^0(X(7),\lambda^{2n}) = H^0(X(7),K^n_{X(7)})$ we have to use Lemma 6.5 which gives

$$\sum_{n=0}^{\infty}\dim H^0(X(7),\lambda^{2n})t^n = (1-t^4)\sum_{n=0}^{\infty}\dim S^n(V_3)^*t^n.$$

Appendix 2. Tables for tensor products of representations of SL(2,$\mathbb{F}_7$)

We use the notation from Appendix 1. For brevity we skip V in the notation V_n. The following tables give the decompositions for the tensor products of irreducible representations of $\mathrm{SL}(2,\mathbb{F}_7)$. This was computed by hand from the known character table of the group $\mathrm{SL}(2,\mathbb{F}_7)$ (see for example, **[D]**, vol. B, pp. 498-499). However, one can also check these computations using one of the standard computer algebra programs (for example,GAP).

	V_3	V_3^*	V_6
V_3	3^*+6	$1+8$	3^*+7+8
V_3^*	$1+8$	$3+6$	$3+7+8$
V_6	3^*+7+8	$3+7+8$	$1+2\cdot 6+7+2\cdot 8$
V_7	$6+7+8$	$6+7+8$	$3+3^*+6+2\cdot 7+2\cdot 8$
V_8	$3+6+7+8$	$3^*+6+7+8$	$3+3^*+2\cdot 6+2\cdot 7+2\cdot 8$
V_4	$4^*+8'$	$6'+6'^*$	$4^*+6'+6'^*+8'$
V_4^*	$6'+6'^*$	$4+8'$	$4+6'+6'^*+8'$
V_6'	$4+6'+8'$	$4^*+6'+8'$	$4+4^*+6'+6'^*+2\cdot 8'$
$V_6'^*$	$4+6'^*+8'$	$4^*+6'^*+8'$	$4+4^*+6'+6'^*+2\cdot 8'$
V_8'	$4^*+6'+6'^*+8'$	$4+6'+6'^*+8'$	$4+4^*+2\cdot 6'+2\cdot 6'^*+2\cdot 8'$

Table 1

	V_7	V_8
V_3	$6+7+8$	$3+6+7+8$
V_3^*	$6+7+8$	$3^*+6+7+8$
V_6	$3+3^*+6+2\cdot 7+2\cdot 8$	$3+3^*+2\cdot 6+2\cdot 7+2\cdot 8$
V_7	$1+3+3^*+2\cdot 6+2\cdot 7+2\cdot 8$	$3+3^*+2\cdot 6+2\cdot 7+3\cdot 8$
V_8	$3+3^*+2\cdot 6+2\cdot 7+3\cdot 8$	$1+3+3^*+2\cdot 6+3\cdot 7+3\cdot 8$
V_4	$4+4^*+6'+6'^*+8'$	$4+6'+6'^*+2\cdot 8'$
V_4^*	$4+4^*+6'+6'^*+8'$	$4^*+6'+6'^*+2\cdot 8'$
V_6'	$4+4^*+2\cdot 6'+6'^*+2\cdot 8'$	$4+4^*+2\cdot 6'+2\cdot 6'^*+2\cdot 8'$
$V_6'^*$	$4+4^*+6'+2\cdot 6'^*+2\cdot 8'$	$4+4^*+2\cdot 6'+2\cdot 6'^*+2\cdot 8'$
V_8'	$4+4^*+2\cdot 6'+2\cdot 6'^*+3\cdot 8'$	$2\cdot 4+2\cdot 4^*+2\cdot 6'+2\cdot 6'^*+3\cdot 8'$

Table 2

	V_4	V_4^*	V_6'
V_3	$4^*+8'$	$6'+6'^*$	$4+6'+8'$
V_3^*	$6'+6'^*$	$4+8'$	$4^*+6'+8'$
V_6	$4^*+6'+6'^*+8'$	$4+6'+6'^*+8'$	$4+4^*+6'+6'^*+2\cdot 8'$
V_7	$4+4^*+6'+6'^*+8'$	$4+4^*+6'+6'^*+8'$	$4+4^*+2\cdot 6'+6'^*+2\cdot 8'$
V_8	$4+6'+6'^*+2\cdot 8'$	$4^*+6'+6'^*+2\cdot 8'$	$4+4^*+2\cdot 6'+2\cdot 6'^*+2\cdot 8'$
V_4	3^*+6+7	$1+7+8$	$3+6+7+8$
V_4^*	$1+7+8$	$3+6+7$	$3^*+6+7+8$
V_6'	$3+6+7+8$	$3^*+6+7+8$	$6+2\cdot 7+2\cdot 8$
$V_6'^*$	$3+6+7+8$	$3^*+6+7+8$	$1+3+3^*+6+7+2\cdot 8$
V_8'	$3^*+6+7+2\cdot 8$	$3+6+7+2\cdot 8$	$3+3^*+2\cdot 6+2\cdot 7+2\cdot 8$

Table 3

	$V_6'^*$	$V_8'^*$
V_3	$4+6'+8'$	$4^*+6'+6'^*+8'$
V_3^*	$4^*+6'+8'$	$4+6'+6'^*+8'$
V_6	$4+4^*+6'+6'^*+2\cdot 8'$	$4+4^*+2\cdot 6'+2\cdot 6'^*+2\cdot 8'$
V_7	$4+4^*+6'+2\cdot 6'^*+2\cdot 8'$	$4+4^*+2\cdot 6'+2\cdot 6'^*+3\cdot 8'$
V_8	$4+4^*+2\cdot 6'+2\cdot 6'^*+2\cdot 8'$	$2\cdot 4+2\cdot 4^*+2\cdot 6'+2\cdot 6'^*+3\cdot 8'$
V_4	$3^*+6+7+8$	$3^*+6+7+2\cdot 8$
V_4^*	$3+6+7+8$	$3+6+7+2\cdot 8$
V_6'	$6+2\cdot 7+2\cdot 8$	$3+3^*+2\cdot 6+2\cdot 7+2\cdot 8$
$V_6'^*$	$1+3+3^*+6+7+2\cdot 8$	$3+3^*+2\cdot 6+2\cdot 7+2\cdot 8$
V_8'	$3+3^*+2\cdot 6+2\cdot 7+2\cdot 8$	$3+3^*+2\cdot 6+3\cdot 7+3\cdot 8$

Table 4

References

[A1] Adler A., *Characterization of modular correspondences by geometric properties*, Pacific J. Math. **155** (1992), 1–27.

[A2] Adler A., *Modular correspondences on X(11)*, Proc. Edinburgh Math. Soc. **35** (1992), 427-435.

[A3] Adler A., *The Euler characters of invariant line bundles on X(p)*, in preparation.

[A4] Adler A., *Stability of the ARK bundle on X(11)*, preprint.

[AR] Adler A., Ramanan S., *Moduli of Abelian Varieties*, Lect. Notes in Math. vol. 1644, Springer, 1996.

[ACGH] Arbarello E., Cornalba M., Griffiths P., Harris J., *Geometry of Algebraic Curves*, Springer, 1985.

[BI] Bauer M., Itzykson C., *A case study in finite groups:* $\mathrm{PSL}(2,\mathbb{F}_7)$, in Recent Developments in Conformal Field Theories, Trieste Conference 1989, World Scient., 1990, p. pp 10–38.

[Bo] Boden H., *Unitary representations of Brieskorn spheres*, Duke Math. J. **75** (1994), 193-220.

[BV] Brivio S., Verra A., *The theta divisor of* $\mathrm{SU}_C(2,2d)^s$ *is very ample if* C *is not hyperelliptic*, Duke Math. J. **82** (1996), 503–552.

[Bu] Burns D., *On the geometry of elliptic modular surfaces and representations of finite groups*, in Algebraic Geometry, Proceedings, Ann Arbor 1981, Lect. Notes in Math., vol. 1008 (I. Dolgachev, ed.), Springer, 1983, pp. 1–29.

[D] Dornhoff L., *Group Representation Theory*, Marcel Dekker, New York, 1971/72.

[Do] Dolgachev I., *On the link space of a Gorenstein surface singularity*, Math. Ann. **265** (1983), 529–540.

[DK] Dolgachev I., Kanev V., *Polar covariants of cubics and quartics*, Advances in Math. **98** (1993), 216-301.

[DoK] Donaldson S., Kronheimer P., *The Geometry of Four-Manifolds*, Oxford Science Publications, 1990.

[Don] Donaldson S., *A new proof of a theorem of Narasimhan and Seshadri*, Journal of Differential Geometry **18** (1983), 269-277.

[E1] Edge W.L., *The Klein group in three dimensions*, Acta Math. **79** (1947), 153–223.

[E2] Edge W.L., *Klein's encounter with the simple group of order 660*, Proc. London Math. Soc. **24** (1972), 647–668.

[FS] Fintushel R., Stern R., *Instanton homology of Seifert fibred homology three spheres*, Proc. London Math. Soc. **61** (1990), 109–137.

[GP] Gross M., Popescu S., *Equations of* $(1,d)$*-polarized abelian surfaces*, alg-geom/9609011.

[Gr] Grothendieck A., *Sur quelques points d'algèbre homologique*, Tohoku Math. J. **9** (1957), 119–221.

[He] Hecke E., *Ueber ein Fundamentalproblem aus der theorie der elliptische Modulfunktionen*, Abh. Math. Sem. Hamburg **6** (1928), 235-257 [Mathematische Werke, art. 28, pp. 525–547].

[Hu] Hudson H.,, *Cremona Transformations in Plane and Space*, Cambridge, Univ. Press, 1927.

[KF] Klein F., Fricke R., *Vorlesungen über die Theorie der Elliptischen Modulfunktionen, vol. 2*, Teubner, Stuttgart, 1892.

[Kl1] Klein F., *Über die Transformation elfter Ordnung der elliptischen Funktionen*, Math. Ann. **15** (1879), [Ges. Math. Abh., B. III, art. LXXXVI, pp. 140-168].

[Kl2] Klein F., *Über gewisse Teiwerte der* Θ*-Funktion*, Math. Ann. **17** (1881), [Ges. Math. Abh., B. III, art. LXXXIX, pp. 186-197].

[Kl3] Klein F., *Systematik der Modulfunktionen*, Math. Ann. **17** (1880/81), [Ges. Math. Abh., B. III, art. LXXXVII, pp. 169-178].

[Mi] Milnor, J., *Introduction to Algebraic K-Theory*, Princeton Univ. Press, 1971.

[NR] Narasimhan M., Ramanan S., 2θ*-linear systems on abelian varieties*, in Vector Bundles on Algebraic Varieties, Tata Institute for Fund. Res. , Oxford Press, 1970, pp. pp. 415–428.

[NS] Narasimhan M., Seshadri C., *Stable and unitary bundles on a compact Riemann surface*, Ann. Math., **82** (1965), 540–567.

[S] Seifert H., *Topologie dreidimensionaler gefaserter Räume*, Acta Mathematica **60** (1933), 147-288 [English translation: in Seifer and Threfall, A Textbook of topology, Acad. Press. 1980].

[Se] Seshadri C., *Fibrés Vectoriels sur les Courbes Algébriques*, Asterisque, vol. 96. Soc. Math. France, 1982.

[Sh] Shimura G., *Introduction to the Arithmetic Theory of Automorphic Forms*, Princeton Univ. Press, 1971.

[SR] Semple J., Roth L., *Introduction to Algebraic Geometry*, Oxford Press, 1949. (reprinted Oxford Science Publ, 1987)

[Tj] Tjurin A., *On intersections of quadrics*, Russian Math. Surveys **30** (1975), 51–105.

[Ve] Vélu. J., *Courbes elliptiques munies d'un sousgroupe $\mathbb{Z}/n\mathbb{Z} \times \mu_n$*, Bull Soc. Math. France. Memoire **57** (1978), 5–152.

Department of Mathematics, University of Michigan, Ann Arbor, MI 48109
e-mail:idolga@math.lsa.umich.edu

This page intentionally left blank

http://dx.doi.org/10.1090/conm/224/03186

Contemporary Mathematics
Volume **224**, 1999

Okubo Algebras and Twisted Polynomials

Alberto Elduque

Dedicated to Professor Hyo Chul Myung on the occasion of his sixtieth birthday.

ABSTRACT. Okubo algebras form a class of nonunital composition algebras with very interesting properties. The classification of these algebras was completed recently and presents a quite different behavior over fields of characteristic three. The aim of this work is to show that this is not really so, since the construction of the Okubo algebras in characteristic three is a kind of limit of the one in other characteristics.

1. Introduction

On the set of trace zero 3×3 matrices over a field F containing a cubic primitive root ω of 1 (hence the characteristic of F is supposed to be $\neq 3$), Okubo [**O**] considered the new multiplication

$$x * y = \mu xy + (1-\mu)yx - \frac{1}{3}T(xy)1 \tag{1}$$

where $\mu = \dfrac{1-\omega}{3}$, xy denotes the usual product of matrices and T denotes the trace. He realized that the algebra thus obtained, denoted by $P_8(F)$, verifies

$$(x*y)*x = x*(y*x) = n(x)y \tag{2}$$

for any x, y, where $n(x) = \frac{1}{6}T(x^2)$ (which has sense even in characteristic 2 since $T(x^2)$ "can be divided by 2" for any $x \in sl(3,F)$). Moreover, n is a strictly nondegenerate quadratic form on $P_8(F)$ (i.e. the symmetric bilinear form obtained by polarization, given by $n(x,y) = n(x+y) - n(x) - n(y)$, is nondegenerate), which permits composition:

$$n(xy) = n(x)n(y), \tag{3}$$

1991 *Mathematics Subject Classification.* Primary 17A75; Secondary 17D25.
Supported by the Spanish DGICYT (PB 94-1311-C03-03) and by the Universidad de La Rioja (96PYB07PBC and API-97/B05).

for any $x, y \in P_8(F)$, so that $P_8(F)$ is a nonunital composition algebra. Besides, the norm n is invariant ([**OO1**, Lemma II.2.3]):

$$n(x * y, z) = n(x, y * z) \tag{4}$$

for any $x, y, z \in P_8(F)$.

The algebra $P_8(F)$ satisfies some very interesting properties. It is flexible ($(x * y) * x = x * (y * x)\ \forall x, y$), Lie-admissible (that is, it becomes a Lie algebra with the commutator product $[x, y]^* = x * y - y * x$, namely, the Lie algebra $sl(3, F)$) and simple, since so is the attached Lie algebra. It was termed the *pseudo-octonion* algebra in [**O**] and its forms (that is, those algebras B over a field F such that the algebra obtained by extending scalars up to the algebraic closure $\bar{F}$ of F, $\bar{B} = \bar{F} \otimes B$, is isomorphic to $P_8(\bar{F})$) were called *Okubo algebras* [**EM1**].

Over fields F of characteristic 3, the pseudo-octonion algebra $P_8(F)$ was defined in [**OO2**] by means of its multiplication table. A more conceptual, but equivalent, definition was given in [**EP**], borrowing ideas from [**Pe**], as follows: let $C = C(F)$ be the algebra of Zorn's vector matrices

$$C(F) = \left\{ \begin{pmatrix} \alpha & u \\ v & \beta \end{pmatrix} : \alpha, \beta \in F, u, v \in F \times F \times F \right\}$$

with multiplication

$$\begin{pmatrix} \alpha & u \\ v & \beta \end{pmatrix} \begin{pmatrix} \alpha' & u' \\ v' & \beta' \end{pmatrix} = \begin{pmatrix} \alpha\alpha' + u \cdot v' & \alpha u' + \beta' u - v \times v' \\ \alpha' v + \beta v' + u \times u' & \beta\beta' + v \cdot u' \end{pmatrix}$$

where $u \cdot v$ and $u \times v$ denote the usual dot and vector product in $V = F \times F \times F$, let us take the endomorphism φ of V which permutes cyclically the canonical basis of V and define

$$\begin{pmatrix} \alpha & u \\ v & \beta \end{pmatrix}^{\tau} = \begin{pmatrix} \alpha & u^{\varphi} \\ v^{(\varphi^*)^{-1}} & \beta \end{pmatrix},$$

where φ^* is the adjoint relative to the dot product. Then τ is an automorphism of $C(F)$ of order 3 and the algebra $C(F)$ with the new multiplication given by

$$x * y = \bar{x}^{\tau} \bar{y}^{\tau^{-1}},$$

is called the *pseudo-octonion algebra* and denoted too by $P_8(F)$. Again the forms of $P_8(F)$ are called *Okubo algebras*. This definition is actually valid in any characteristic.

Apart from Okubo algebras, there is just another family of nonunital composition algebras with invariant associated quadratic norm. They are obtained as follows: let C be any unital composition algebra (also termed Hurwitz algebra) of dimension ≥ 2 (see [**ZSSS**, Chapter 2]) with norm n over a field F and let $x \mapsto \bar{x} = n(x, 1)1 - x$ its standard involution. Then define a new multiplication on C by means of

$$x * y = \bar{x}\bar{y}$$

for any $x, y \in C$. The new algebra $(C, *)$ thus obtained is called the *para-Hurwitz* algebra associated to C. Relations (2), (3) and (4) are easily verified for $(C, *)$.

Okubo algebras, together with para-Hurwitz algebras and some forms of two-dimensional para-Hurwitz algebras comprise all the *symmetric composition algebras*, that is, all the composition algebras with invariant norm (see [**OO1**], [**OO2**], [**EP**] and [**E**]).

This property of the invariance of the norm makes it possible to study very nicely the classical phenomenon of triality by using the eight-dimensional symmetric composition algebras instead of the Hurwitz algebras (see [**KMRT**]).

The last step in the classification of the symmetric composition algebras was given recently in [**E**], where the Okubo algebras over fields of characteristic 3 were determined, but in a completely different way to the path followed in other characteristics.

The next two results (Theorems 1 and 2) present the classification of the Okubo algebras. The first one shows the classification obtained in [**EM3**] over fields of characteristic $\neq 2, 3$, which was inspired in [**F**] and extended previous results in [**EM2**]. Actually, as remarked in [**E**], the arguments in [**EM3**], with some minor changes, are valid in characteristic 2 as well. Also, the result will be stated following [**KMRT**, (36.38)]. The second result will state the classification in characteristic 3 obtained in [**E**], extending previous results in [**EP**].

In order to state Theorem 1, some notation is needed. Given a central simple associative algebra A of degree 3 over a field K, any element $x \in A$ satisfies its generic minimum polynomial:

$$p_x(\lambda) = \lambda^3 - T(x)\lambda^2 + S(x)\lambda - N(x)1, \tag{5}$$

for a linear form T (the trace), a quadratic form S, with $2S(x) = T(x)^2 - T(x^2)$ (something that can be checked just for the algebra of 3×3–matrices over the algebraic closure and only for the diagonal elements, since the diagonalizable matrices form a Zariski dense subset), and a cubic form N over K. The set of trace zero elements will be denoted by A_0. Besides, if A is equipped with an involution J of the second kind, so that the subfield F of fixed elements of K by J satisfies that K/F is a separable field extension of degree two, then J will be said to be a K/F-involution and $H(A, J)_0$ will denote the set of fixed elements of A by J with zero trace (which is an F-subspace, but not a K-subspace). Then:

THEOREM 1. *Let F be a field of characteristic $\neq 3$ and let ω be a cubic primitive root of* 1 *(in an algebraic closure of F).*

(i) *If $\omega \in F$ then the Okubo algebras over F are, up to isomorphism, exactly the algebras $(A_0, *)$, where A is a central simple associative algebra over F of degree* 3 *and $*$ is the multiplication given by* (1).
Two Okubo algebras over F are isomorphic if and only if so are the corresponding central simple associative algebras.

(ii) *If $\omega \notin F$ and $K = F[\omega]$ then the Okubo algebras over F are, up to isomorphism, exactly the algebras $(H(A, J)_0, *)$, where A is a central simple associative algebra over K of degree* 3 *equipped with a K/F-involution J and where $*$ is again given by formula* (1).
Two Okubo algebras over F are isomorphic if and only if so are the corresponding central simple associative algebras as algebras with involution.

In both items of this Theorem, the norm n of the Okubo algebra is the restriction, either to A_0 or to $H(A, J)_0$, of $-\frac{1}{3}S(x)$ (which equals $\frac{1}{6}T(x^2)$ if the characteristic is not 2).

In order to state Theorem 2 (characteristic 3) some extra notation is needed too. Let α and β be two nonzero scalars in a field F of characteristic 3 and let $F^{\alpha,\beta}[x, y]$ be the (commutative and associative) algebra obtained as the quotient of the algebra $F[X, Y]$ of polynomials in two variables by the ideal generated by

$X^3-\alpha$ and $Y^3-\beta$. Here x and y denote the classes of the variables X and Y modulo this ideal. On $F^{\alpha,\beta}[x,y]$ consider the new multiplication determined by (see [**E**]):

$$x^iy^j \diamond x^{i'}y^{j'} = \left(1-\begin{vmatrix} i & j \\ i' & j'\end{vmatrix}\right) x^{i+i'}y^{j+j'}\,. \tag{6}$$

Then for any $u,v\in F^{\alpha,\beta}[x,y]_0 \stackrel{\text{def}}{=} \operatorname{span}\langle x^iy^j : 0\le i,j\le 2,\ (i,j)\neq(0,0)\rangle$, the product $u\diamond v$ decomposes as

$$u\diamond v = n(u,v)+u*v \tag{7}$$

with $n(u,v)\in F$ and $u*v\in F^{\alpha,\beta}[x,y]_0$. Then

THEOREM 2. *Up to isomorphism, the Okubo algebras over a field F of characteristic 3 are exactly the algebras $(F^{\alpha,\beta}[x,y]_0,*)$ for nonzero scalars α and β in F.*

The norm in the Okubo algebra $(F^{\alpha,\beta}[x,y]_0,*)$ is given by $n(u)=\frac{1}{2}n(u,u)=-n(u,u)$, where $n(\,,\,)$ is given by (7). The conditions for isomorphisms between two such algebras $(F^{\alpha,\beta}[x,y]_0,*)$ and $(F^{\alpha',\beta'}[x,y]_0,*)$ are given in [**E**] in terms of the scalars α,β,α' and β'. It also turns out that all the Okubo algebras over fields of characteristic 3 have isotropic norm or, equivalently, there are no division Okubo algebras over these fields.

In spite of the big difference in the results and methods of proof of both Theorems above, it will be shown in the next section that the Okubo algebras over fields of characteristic $\neq 3$ with isotropic norm can be built starting with algebras of twisted polynomials and in that respect, the situation in characteristic 3 is a "kind of limit" of the isotropic case in other characteristics. This will allow us to give in section 3 a common multiplication table for the Okubo algebras with isotropic norm, depending on two parameters and valid over any field.

2. Okubo algebras and twisted polynomials

The idea behind the results in this section grew out of a conversation with professor M.A. Knus, to whom the author wants to express his appreciation, during a visit to the ETH at Zürich.

It consists of expressing the central simple associative algebras which appear in Theorem 1, giving rise to the Okubo algebras with isotropic norm, as quotients of a twisted polynomial ring. To begin with, let K be a field of characteristic $\neq 3$ containing a cubic primitive root ω of 1 and consider the twisted polynomial ring $K_\omega[X,Y]$, which is the usual polynomial ring but where the variables do not commute, but satisfy instead the relation

$$YX=\omega XY\,.$$

The center of $K_\omega[X,Y]$ is the subring generated by X^3 and Y^3: $K[X^3,Y^3]$. Now, given two nonzero scalars α and β in K, let $I_{\alpha,\beta}$ be the ideal generated by the central elements $X^3-\alpha$ and $Y^3-\beta$, so that $I_{\alpha,\beta}=K_\omega[X,Y](X^3-\alpha)+K_\omega[X,Y](Y^3-\beta)$. Let x and y denote the classes of X and Y modulo $I_{\alpha,\beta}$ and denote by $K_\omega^{\alpha,\beta}[x,y]$ the quotient $K_\omega[X,Y]/I_{\alpha,\beta}$.

Therefore, $K_\omega^{\alpha,\beta}[x,y]$ is the unital associative K–algebra generated by x and y and subject to the relations $x^3=\alpha$, $y^3=\beta$ and $yx=\omega xy$ (see for instance [**Pi**, Chapter 15], where this algebra is denoted by $\left(\dfrac{\alpha,\beta}{K,\omega}\right)$).

In order to describe the central simple associative algebras in Theorem 1 which are related to the Okubo algebras with isotropic norm a Lemma is needed:

LEMMA 3. *Let $(A,*)$ be any Okubo algebra with nonzero idempotents and isotropic norm n over a field F of characteristic $\neq 3$. Then there is an element $x\in A$ such that $n(x)=0$ and $n(x,x*x)=1$.*

PROOF. By [**EP**, Theorem 3.5], there is a Cayley-Dickson algebra C over F, with standard involution $x\mapsto\bar{x}$ and multiplication that will be denoted by juxtaposition, equipped with an automorphism τ of order 3 such that $H=\{a\in C: a^\tau=a\}$ is a quaternion subalgebra of C and A is isomorphic to the algebra C_τ defined on C but with the new product:

$$x*y=\bar{x}^\tau\bar{y}^{\tau^{-1}}\,.$$

Moreover, under the isomorphism the norm of A corresponds to the norm of C as a composition algebra, which will also be denoted by n. In case H is a split quaternion subalgebra, that is, H is isomorphic to $\mathrm{Mat}_2(F)$ as composition algebras (the norm of the algebra of 2×2–matrices is the determinant), the element that corresponds to $\begin{pmatrix}1&0\\0&0\end{pmatrix}$ verifies $n(x)=0$ and

$$n(x,x*x)=n(x,\bar{x}^2)=n\left(\begin{pmatrix}1&0\\0&0\end{pmatrix},\begin{pmatrix}0&0\\0&1\end{pmatrix}\right)=\begin{vmatrix}1&0\\0&1\end{vmatrix}=1\,,$$

as required. Otherwise H is a division algebra but C is split since the norm is isotropic. Then we may find an element $v\in H^\perp$ with $0=n(1+v)=1+n(v)$. Since τ fixes elementwise H and $H^\perp=Hv$, $v^\tau=wv$ for some $w\in H$ such that $w^2+w+1=0$ (because $\tau^3=1$). Hence the element $x=-1-v$ verifies $n(x)=0$ and computing in $C=H\oplus Hv$ we get

$$\begin{aligned}x*x&=(-1+wv)(-1+w^2v)=1-(w+w^2)v+(\bar{w}^2w)v^2\\&=1+v+w^2=-w+v\end{aligned}$$

and

$$n(x,x*x)=n(-1-v,-w+v)=n(1,w)-n(v,v)=-1+2=1\,,$$

as required. □

Now, the announced description:

THEOREM 4. *Let F be a field of characteristic $\neq 3$ and let ω be a cubic primitive root of 1 (in an algebraic closure of F):*

(i) *If $\omega\in F$ and A is a central simple associative algebra of degree 3 over F then there are nonzero scalars $\alpha,\beta\in F$ such that A is isomorphic to $F_\omega^{\alpha,\beta}[x,y]$.*
(ii) *If $\omega\notin F$, $K=F[\omega]$ and (A,J) is a central simple associative K-algebra of degree 3, equipped with a K/F-involution J of the second kind, such that the norm of the associated Okubo algebra $(H(A,J)_0,*)$ is isotropic, then there are nonzero scalars $\alpha,\beta\in F$ such that (A,J) is isomorphic (as an algebra*

with involution) to $(K_\omega^{\alpha,\beta}[x,y],I)$*, where* I *is the unique* K/F*–involution of the second kind on* $K_\omega^{\alpha,\beta}[x,y]$ *which fixes* x *and* y*.*

Conversely, the norm of the Okubo algebras associated to $F_\omega^{\alpha,\beta}[x,y]$ *in item* (i) *and to* $(K_\omega^{\alpha,\beta}[x,y],I)$ *in item* (ii) *are isotropic.*

PROOF. If $\omega\in F$, the element x in $F_\omega^{\alpha,\beta}[x,y]$ verifies $T(x)=S(x)=0$ (and $N(x)=\alpha$). Hence $x\in F_\omega^{\alpha,\beta}[x,y]_0$ and $n(x)=-\frac{1}{3}S(x)=0$. The same happens to the element $x\in H(K_\omega^{\alpha,\beta}[x,y],I)_0$ in case $\omega\notin F$. Hence the converse is clear.

Assume now that $\omega\in F$, then item (i) follows from standard results in associative algebras (see [**Pi**, Chapter 15]). For completeness we include the argument: either $A=\mathrm{Mat}_3(F)$ (up to isomorphism), and then A is the algebra generated by the elements

$$x=\begin{pmatrix}1&0&0\\0&\omega&0\\0&0&\omega^2\end{pmatrix}\qquad\text{and}\qquad y=\begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix}\tag{8}$$

which satisfy $x^3=y^3=1$ and $yx=\omega xy$, so that A is isomorphic to $F_\omega^{1,1}[x,y]$, or A is a central division algebra and hence cyclic. Since $\omega\in F$, there are elements $x\in A\setminus F$ with $x^3=\alpha\in F$ and, by the Skolem-Noether theorem another element y can be found with $yxy^{-1}=\omega x$. Hence y^3 centralizes x and y, which generate A and hence $y^3=\beta\in F$ and A is isomorphic to $F_\omega^{\alpha,\beta}[x,y]$.

Finally, assume that $\omega\notin F$ and (A,J) is an algebra as in the statement of item (ii). By hypothesis there is an element $0\neq x\in H(A,J)_0$ with $S(x)=0$, so that its generic minimum polynomial (5) is $\lambda^3-\alpha$ for some $\alpha\in F$ (since $x\in H(A,J)$, $\alpha=N(x)$ is fixed by J). If A is a division algebra $\alpha\neq 0$, $K[x]$ is a cyclic field extension of K and by the Skolem-Noether theorem there is an invertible element $z\in A$ with $zxz^{-1}=\omega x$. Then $y=(zJ(z))^2$ also verifies $yx=\omega xy$ and belongs to $H(A,J)$. Besides y^3 centralizes A and belongs to $H(A,J)$, so $y^3=\beta\in F$ and it follows that (A,J) is isomorphic to $(K_\omega^{\alpha,\beta}[x,y],I)$.

But even in case $A=\mathrm{Mat}_3(K)$, so that the associated Okubo algebra has nonzero idempotents by [**EM3**, Proposition 7.4], for any $x\in H(A,J)_0$ with $n(x)=0$ and $n(x,x*x)=1$ as in the Lemma above, one has $0=2n(x)=-\frac{2}{3}S(x)=\frac{1}{3}T(x^2)$, so that $x*x=x^2$ and $1=n(x,x*x)=-\frac{1}{3}S(x,x^2)=\frac{1}{3}T(x^3)$; hence it follows from (5) and from $T(x)=0=S(x)$ and $T(x^3)=3$ that $x^3=1$. Besides, from $T(x)=T(x^2)=0$ it follows that $1,x$ and x^2 are linearly independent. Therefore x is similar to the diagonal matrix in (8) and there is another invertible element $z\in A=\mathrm{Mat}_3(K)$ with $zx=\omega xz$. As above, the element $y=(zJ(z))^2$ also verifies $yx=\omega xy$, it is invertible and fixed by J. It then follows $0\neq y^3=\beta\in F$, that $y\in H(A,J)_0$ and that (A,J) is isomorphic to $(K_\omega^{1,\beta}[x,y],I)$. □

COROLLARY 5 ([**EM3**, Proposition 7.3]). *There do not exist division Okubo algebras over fields containing the cubic primitive roots of* 1.

A general result can be given in case $\omega\notin F$ about the central simple associative algebras of degree 3 over $K=F[\omega]$ equipped with a K/F-involution:

PROPOSITION 6. *Let* (A,J) *be a central simple associative algebra of degree* 3 *over* $K=F[\omega]$*, where* F *is a field of characteristic* $\neq 3$ *and* ω *a cubic primitive root of* 1*,* $\omega\notin F$*, equipped with a* K/F*-involution (of second kind). Then there are nonzero scalars* $\alpha,\beta\in F$ *such that* (A,J) *is isomorphic to* $(K_\omega^{\alpha,\beta}[x,y],I_a)$*, where* I

is the K/F-involution of $K_\omega^{\alpha,\beta}[x,y]$ that fixes x and y, a is an invertible element in $K_\omega^{\alpha,\beta}[x,y]$ fixed by I and I_a is the K/F–involution given by $I_a(u) = aI(u)a^{-1}$ for any u.

PROOF. In case $A = \mathrm{Mat}_3(K)$, then the elements x and y in (8) satisfy $x^3 = y^3 = 1$, $yx = \omega xy$ and they are fixed by the K/F-involution I given by $I(u) = gu^*g^{-1}$, where $g = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$ and $(u_{ij})^* = (\overline{u_{ji}})$, with $\gamma \mapsto \bar{\gamma}$ the nontrivial F-automorphism of K. Then (see [**J**, p.192]) there is an invertible element a fixed by I such that $J(u) = aI(u)a^{-1}$ for any u and $(A,J) \cong (K_\omega^{1,1}[x,y], I_a)$.

In case A is a division algebra, by [**HK**, Proposition 1] there are elements $0 \neq x \in A_0$ with $x^3 = \alpha \in F$ and x fixed by a K/F-involution I. Then $K[x]/K$ is a cyclic field extension and by the Skolem-Noether theorem there is a $0 \neq z \in A$ with $zx = \omega xz$. Then, as before, the element $y = (zI(z))^2$ is fixed by I and also satisfies $yx = \omega xy$. Besides $y^3 = \beta \in F$ and again (A,J) is isomorphic to $(K_\omega^{\alpha,\beta}[x,y], I_a)$ for a suitable element a. □

Theorem 4 tells us that in case the associated Okubo algebra has isotropic norm, then the element a in Proposition 6 can be taken to be 1.

3. Common multiplication table

The results in the previous section make clear the similarities in the construction of the Okubo algebras in characteristic 3 and $\neq 3$. First, let us assume for a while that F is a field of characteristic $\neq 3$ containing the cubic roots of 1 ($\omega \in F$) and α and β are nonzero scalars in F. The set of trace zero elements in $F_\omega^{\alpha,\beta}[x,y]$ is

$$F_\omega^{\alpha,\beta}[x,y]_0 = \mathrm{span}\langle x^i y^j : 0 \leq i,j \leq 2,\ (i,j) \neq (0,0)\rangle\,.$$

With $\mu = \dfrac{1-\omega}{3}$, define on $F_\omega^{\alpha,\beta}[x,y]$ a new product by

$$u \diamond v = \mu uv + (1-\mu)vu\,.$$

Then for any $u, v \in F_\omega^{\alpha,\beta}[x,y]_0$

$$u \diamond v = n(u,v) + u * v$$

where $u * v$ is given by (1) and $n(u,v) = \frac{1}{3}T(uv) = -\frac{1}{3}S(u,v)$. This is completely analogous to (7).

Besides, the elements $\omega^{-ij}x^iy^j$ $(i,j \in \mathbb{Z})$ of $F_\omega^{\alpha,\beta}[x,y]$ multiply according to

(9)
$$\begin{aligned}
\omega^{-ij}x^iy^j \diamond \omega^{-i'j'}x^{i'}y^{j'} &= \omega^{-(ij+i'j')}\left(\mu x^iy^jx^{i'}y^{j'} + (1-\mu)x^{i'}y^{j'}x^iy^j\right) \\
&= \omega^{-(ij+i'j')}\left(\mu\omega^{i'j} + (1-\mu)\omega^{j'i}\right)x^{i+i'}y^{j+j'} \\
&= \left(\mu\omega^{\Delta} + (1-\mu)\omega^{-\Delta}\right)\left(\omega^{-(i+i')(j+j')}x^{i+i'}y^{j+j'}\right)
\end{aligned}$$

where $\Delta = \begin{vmatrix} i & j \\ i' & j' \end{vmatrix}$. Also notice that since $\mu = \frac{1-\omega}{3} = \frac{\omega^2}{\omega^2-\omega}$ and $1-\mu = \frac{\omega}{\omega-\omega^2}$:

$$\mu\omega^{\Delta} + (1-\mu)\omega^{-\Delta} = \begin{cases} 1 & \text{if } \Delta \equiv 0 \pmod 3, \\ 0 & \text{if } \Delta \equiv 1 \pmod 3, \\ -1 & \text{if } \Delta \equiv 2 \pmod 3. \end{cases}$$

Therefore,

$$\mu\omega^{\Delta} + (1-\mu)\omega^{-\Delta} \equiv 1 - \Delta \pmod 3\,, \tag{10}$$

which shows how close (6) and (9) are.

On the other hand,

$$\mu\omega^{\Delta} + (1-\mu)\omega^{-\Delta} = \frac{\omega^{-1}}{\omega^{-1}-\omega}\omega^{\Delta} + \frac{\omega}{\omega-\omega^{-1}}\omega^{-\Delta} = \frac{1}{\omega-\omega^{-1}}\left(\omega^{1-\Delta} - \omega^{-(1-\Delta)}\right)$$

and one can think that ω collapses to 1 if the characteristic is 3. However, for real numbers (think of q as ω)

$$\lim_{q\to 1} \frac{q^{1-\Delta} - q^{-(1-\Delta)}}{q - q^{-1}} = 1 - \Delta\,.$$

Therefore, (6) can be though of as a limit of (9) when ω collapses to 1, as commented in the Introduction.

In case F is a field of characteristic $\neq 3$ but $\omega \notin F$ and α and β are nonzero scalars in F, according to Theorem 4 we consider the algebra with involution $(K_\omega^{\alpha,\beta}[x,y], I)$, where $K = F[\omega]$, $x^3 = \alpha$, $y^3 = \beta$, $yx = \omega xy$ and I is the K/F-involution fixing x and y. Then the elements $\omega^{-ij}x^iy^j$ verify that

$$I(\omega^{-ij}x^iy^j) = \omega^{-2ij}y^jx^i = \omega^{-ij}x^iy^j\,,$$

so that the set of trace zero elements fixed by I is

$$H(K_\omega^{\alpha,\beta}[x,y], I)_0 = F\text{-span}\langle \omega^{-ij}x^iy^j : 0 \le i,j \le 2,\ (i,j) \neq (0,0)\rangle\,.$$

And the $\diamond$ multiplication of these elements is given again by (9).

As a consequence of (6), (9) and (10), the basis

$$\{x_{ij} \overset{\text{def}}{=} -x^iy^j : -1 \le i,j \le 1,\ (i,j) \neq (0,0)\}$$

of the Okubo algebra $(F^{\alpha,\beta}[x,y]_0, *)$ in case the characteristic of F is 3 and the basis

$$\{x_{ij} \overset{\text{def}}{=} -\omega^{ij}x^iy^j : -1 \le i,j \le 1,\ (i,j) \neq (0,0)\}$$

of either $(F_\omega^{\alpha,\beta}[x,y]_0, *)$ or $(H(K_\omega^{\alpha,\beta}[x,y], I)_0, *)$ in case the characteristic of F is not 3 share the same multiplication table (which is exactly Table 1 in [**E**], with different name for the parameters). That is:

THEOREM 7. *For any Okubo algebra with isotropic norm over an arbitrary field (in particular any Okubo algebra over any field of characteristic* 3 *or of characteristic* $\neq 3$ *but containing the cubic roots of* 1*), there are nonzero scalars* $\alpha, \beta \in F$ *and a basis* $\{x_{ij} : -1 \le i,j \le 1,\ (i,j) \neq (0,0)\}$ *such that the multiplication table is:*

	$x_{1,0}$	$x_{-1,0}$	$x_{0,1}$	$x_{0,-1}$	$x_{1,1}$	$x_{-1,-1}$	$x_{-1,1}$	$x_{1,-1}$
$x_{1,0}$	$-\alpha x_{-1,0}$	0	0	$x_{1,-1}$	0	$x_{0,-1}$	0	$\alpha x_{-1,-1}$
$x_{-1,0}$	0	$-\alpha^{-1}x_{1,0}$	$x_{-1,1}$	0	$x_{0,1}$	0	$\alpha^{-1}x_{1,1}$	0
$x_{0,1}$	$x_{1,1}$	0	$-\beta x_{0,-1}$	0	$\beta x_{1,-1}$	0	0	$x_{1,0}$
$x_{0,-1}$	0	$x_{-1,-1}$	0	$-\beta^{-1}x_{0,1}$	0	$\beta^{-1}x_{-1,1}$	$x_{-1,0}$	0
$x_{1,1}$	$\alpha x_{-1,1}$	0	0	$x_{1,0}$	$-(\alpha\beta)x_{-1,-1}$	0	$\beta x_{0,-1}$	0
$x_{-1,-1}$	0	$\alpha^{-1}x_{1,-1}$	$x_{-1,0}$	0	0	$-(\alpha\beta)^{-1}x_{1,1}$	0	$\beta^{-1}x_{0,1}$
$x_{-1,1}$	$x_{0,1}$	0	$\beta x_{-1,-1}$	0	0	$\alpha^{-1}x_{1,0}$	$-\alpha^{-1}\beta x_{1,-1}$	0
$x_{1,-1}$	0	$x_{0,-1}$	0	$\beta^{-1}x_{1,1}$	$\alpha x_{-1,0}$	0	0	$-\alpha\beta^{-1}x_{-1,1}$

□

References

[E] A. Elduque, *Symmetric composition algebras*, J. Algebra **196** (1997), 283–300.

[EM1] A. Elduque and H.C. Myung, *On Okubo algebras*, Forty Years of Rochester Symposium: From Symmetries to Strings, A. Das, ed., World Scientific Publ., River Edge, New Jersey, 1990, pp. 299–310.

[EM2] ———, *Flexible composition algebras and Okubo algebras*, Commun. Algebra **19** (1991), 1197–1227.

[EM3] ———, *On flexible composition algebras*, Commun. Algebra **21** (1993), 2481–2505.

[EP] A. Elduque and J.M. Pérez, *Composition algebras with associative bilinear form*, Commun. Algebra **24** (1996), 1091–1116.

[F] J. R. Faulkner, *Finding octonion algebras in associative algebras*, Proc. Amer. Math. Soc. **104** (1988), 1027–1030.

[HK] D.E. Haile and M.A. Knus, *On Division Algebras of Degree 3 with Involution*, J. Algebra **184** (1996), 1073–1081.

[J] N. Jacobson, *Finite-Dimensional Division Algebras over Fields*, Springer–Verlag, Berlin-Heidelberg, 1996.

[KMRT] M.A. Knus, A.S Merkurjev, M. Rost and J.P. Tignol, *The Book of Involutions* (to appear).

[O] S. Okubo, *Pseudo-quaternion and pseudo-octonion algebras*, Hadronic J. **1** (1978), 1250–1278.

[OO1] S. Okubo and J.M. Osborn, *Algebras with nondegenerate associative symmetric bilinear form permitting composition*, Commun. Algebra **9** (1981), 1233–1261.

[OO2] ———, *Algebras with nondegenerate associative symmetric bilinear form permitting composition, II*, Commun. Algebra **9** (1981), 2015–2073.

[Pe] H. Petersson, *Eine Identität fünften Grades, der gewisse Isotope von Kompositions-Algebren genügen*, Math. Z. **109** (1969), 217–238.

[Pi] R.S. Pierce, *Associative Algebras*, Springer–Verlag, New York, 1982.

[ZSSS] K.A. Zhevlakov, A.M. Slin'ko, I.P. Shestakov and A.I. Shirshov, *Rings that are Nearly Associative*, Academic Press, New York, 1982.

Departamento de Matemáticas y Computación, Universidad de La Rioja. 26004 Logroño, Spain

Current address: Departamento de Matemáticas, Facultad de Ciencias, Universidad de Zaragoza. 50009 Zaragoza, Spain

E-mail address: `elduque@posta.unizar.es`

This page intentionally left blank

http://dx.doi.org/10.1090/conm/224/03189

Contemporary Mathematics
Volume **224**, 1999

Some new results on modular forms for $\mathrm{GL}(2, \mathbb{F}_q[T])$

Ernst-Ulrich Gekeler

Introduction.

The modular forms in question, i.e., Drinfeld modular forms, are analogues in positive characteristics of classical elliptic modular forms. They are rigid analytic functions defined on Drinfeld's upper half-place $\Omega = C - K_\infty$, where C is the completed algebraic closure of K_∞, the completion of a global function field K at some fixed place ∞.

In the present paper, we restrict to the simplest and most important case where $K = \mathbb{F}_q(T)$ is a rational function field and "∞" is the usual place at infinity, although most of the theory can be developed for general function fields in one variable over finite constant fields.

Let A be the subring of elements of K regular away from ∞, i.e., A is the polynomial ring $\mathbb{F}_q[T]$. It embeds discretely into K_∞ with compact quotient. Therefore, the sextuple $(A, K, K_\infty, C, \Omega, \mathrm{GL}(2, A))$ shares many properties (more than visible at a first sight) with $(\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, H^\pm = \mathbb{C} - \mathbb{R}, \mathrm{GL}(2, \mathbb{Z}))$. The most basic modular forms in the present context are the *Eisenstein series*

$$E_k(z) = \sum_{a,b \in A}{}' \frac{1}{(az+b)^k}$$

introduced by D. Goss in the seventies [13] [14]. In fact, E_k is a modular form of weight k for $\Gamma = \mathrm{GL}(2, A)$, non-zero if $0 < k \equiv 0 \pmod{q-1}$, and the two algebraically independent forms E_{q-1} and E_{q^2-1} generate the ring of all modular forms (with trivial type) for Γ. As in the classical case, such forms, their zeroes, relations, expansions around cusps, congruence properties etc. encode important parts of the arithmetic of K. They are directly related to Drinfeld modules (in particular, there exist analogues of the classical discriminant and invariant functions Δ and j) and, in a less obvious fashion, to elliptic curves over K (through some kind of Shimura-Taniyama-Weil correspondence [9]).

In the first part of this article (sect. 1-5, largely based on [6]), we expose

1991 Mathematics Subject Classification. Primary 11G09 11F11; secondary 11R58

Partially supported by DFG, Sonderprogramm "Algorithmische Zahlentheorie und Algebra"

known results about modular forms for Γ and introduce some technical tools. Here we omit most of the proofs and restrict to explaining the definitions and constructions. This part also provides the necessary background for the second part (sect. 6-8), whose results are new. In the second part, we investigate the zeroes of the Eisenstein series E_k. Such a series is called *special* if k has the form $q^j - 1$ for some j. The main results are (precise definitions are given below):

(A) (Prop. 6.7): If the zero z of E_k lies in the "fundamental domain" $\mathcal{F} = \{z \in \Omega \mid |z| = |z|_i \geq 1\}$ for Γ then $|z| = 1$. Equivalently, the j-invariant $j(z)$ of each zero of E_k satisfies $|j(z)| \leq q^q$.
This is similar to a result of Rankin and Swinnerton-Dyer [16] in the classical case.

(B) (Thm. 8.5): For each $z_0 \in \mathbb{F}_{q^{k+1}} - \mathbb{F}_q$, there exists a unique zero $z \in \mathcal{F}$ of the special Eisenstein series E_{q^k-1} that satisfies $|z - z_0| < 1$, and these are all the zeroes of E_{q^k-1} in $\mathcal{F}$. They are all simple, and their j-invariants are zero or of absolute value q^q.

(C) (Thm. 7.14, Thm. 8.12): Let L_k/K be the subfield of C generated by the $j(z)$, where $E_{q^k-1}(z) = 0$. Then $L_k \cdot K_\infty$ is the unramified extension of degree $k+1, 2, 1$ of K_∞ if $k \geq 4$, $k = 3$, $k \leq 2$, respectively. Further, L_k/K is unramified at finite primes of K of degree $d \geq k$.

Here (A) is rather simple and stated for completeness only, whereas (B) and (C) are deep. We also have similar results on the forms ∂E_{q^k-1} of weight q^k+1 and type 1, where $\partial : f \longmapsto f' + k\frac{\Delta'}{\Delta}f$ is the "Serre derivative" of a modular form of weight k.

Let $\varphi_k \in A[X]$ be the polynomial

$$\varphi_k(X) = \prod (X - j(z)),$$

where z runs through a system of Γ-representatives of zeroes z of E_{q^k-1} with $j(z) \neq 0$. Then L_k is the splitting field of φ_k, and it is conjectured that $\mathrm{Gal}(L_k/K)$ is the full symmetric group on the zeroes of φ_k, provided that $k \geq 4$. (For $k \leq 3$, the Galois group is smaller for trivial reasons.) Gunther Cornelissen has proved that φ_k is always irreducible, and he was also able to show that its Galois group is as conjectured at least if q is odd and k is even.

These results/conjectures shed new light on the classical situation, too. In the above-mentioned analogy, special Eisenstein series E_{q^k-1} ought to correspond to classical Eisenstein series E_{p-1} with a prime $p > 3$ and L_k to the field generated by the j-invariants of its zeroes. Numerical evidence (for $p \leq 89$) suggests that the polynomial

$$\varphi_p(X) = \prod_{\substack{j \text{ a zero of } E_{p-1} \\ j \neq 0, 1728}} (X - j(z))$$

is always irreducible with the full symmetric group as its Galois group. Furthermore, the numerator of its discriminant is highly divisible by (almost: the prime $l = 11$ seems to play a special role) all primes $l \leq \frac{p-1}{2}$, but also by some unpredictable larger primes l. Hence a flat analogy of e.g. (C) fails to hold in the classical case, and more work has to be done to understand φ_p.

It is a pleasure for me to thank the organizers of the KAIST conference for the invitation to lecture on the present material. I would also like to thank G. Cornelissen for extensive discussions as well as for help with some numerical calculations.

1. Notations.

The following notation will be used throughout.

(1.1)

$\mathbb{F}_q$	$=$	finite field with q elements, of characteristic p
A	$=$	$\mathbb{F}_q[T]$ the plynomial ring over $\mathbb{F}_q$ with quotient field $K = \mathbb{F}_q(T)$
K_∞	$=$	$\mathbb{F}_q((\pi))$ the completion of K at the infinite place ∞, with uniformizer $\pi = T^{-1}$, ring of integers $O_\infty = \mathbb{F}_q[[\pi]]$, normalized valuation $v:\ K_\infty \longrightarrow \mathbb{Z} \cup \{\infty\}$ and absolute value $\lvert x\rvert = q^{-v(x)}$
C	$=$	completed algebraic closure of K_∞, provided with the unique extension of "$\lvert\ .\ \rvert$", ring of integers $O_C = \{x \in C \mid \lvert x\rvert \leq 1\}$ and maximal ideal $\mathfrak{m}_C = \{x \in C \mid \lvert x\rvert < 1\}$
Ω	$=$	$C - K_\infty$ the Drinfeld upper half-plane, acted upon by
Γ	$=$	GL$(2, A)$.

Recall that C is algebraically closed with $\overline{\mathbb{F}}_q$, the algebraic closure of $\mathbb{F}_q$, as its residue class field. For $z \in C$ we define the *imaginary part* $|z|_i := \inf_{x \in K_\infty} |z - x|$ $= \min_{x \in K_\infty} |z - x|$. It satisfies

$$\left|\frac{az+b}{cz+d}\right|_i = \frac{|ad-bc|}{|cz+d|^2}|z|_i \quad \text{for } \begin{pmatrix} a\,b \\ c\,d \end{pmatrix} \in \mathrm{GL}(2, K_\infty). \tag{1.2}$$

The "upper half-plane" Ω is the set of C-points of a rigid analytic space defined over K_∞. In particular, the notion of holomorphic or meromorphic functions on Ω is defined. Typical admissible open subsets of Ω are the sets (in fact, affinoids)

$$D_n := \{z \in \Omega \mid q^{-(n+1)} \leq |z| = |z|_i \leq q^{-n}\}, \tag{1.3}$$

which together with their shifts $D_{n,x} := D_n + x$ ($n \in \mathbb{Z}$, $x \in K_\infty$) cover Ω. Typical holomorphic functions on Ω are rational functions in $z \in \Omega \hookrightarrow \mathbb{P}^1(C)$ without poles on Ω, or locally uniform (i.e., uniform on the $D_{n,x}$) limits of such.

We will adapt a naive point of view and simply write Ω, $D_{n,x}$ etc., the analytic structure being understood. More details can be found e.g. in [9], sect. 1.

2. Lattices [5] [15] [10].

A subset S of C is *discrete* if its intersection with each ball $B_r = \{z \in C \mid |z| \leq r\}$ is finite. An $\mathbb{F}_q$*-lattice* in C is a discrete $\mathbb{F}_q$-subspace, an A*-lattice* a discrete A-submodule. With each lattice $\Lambda \subset C$, we associate its exponential function

$$e_\Lambda(z) = z \prod_{\lambda \in \Lambda}{}' (1 - \frac{z}{\lambda}). \tag{2.1}$$

Here the $\prod'$ denotes the product over the non-zero elements of Λ; similar notation will be used for sums over Λ. The discreteness condition on Λ implies that the product (in arbitrary order) converges, uniformly on each B_r, to an entire function $e_\Lambda : C \longrightarrow C$. It is surjective, $\mathbb{F}_q$-linear, Λ-periodic, has constant derivative $e'_\Lambda(z) = 1$, and satisfies the identity of meromorphic functions on C:

$$t_\Lambda(z) := \frac{1}{e_\Lambda(z)} = \frac{e'_\Lambda(z)}{e_\Lambda(z)} = \sum_{\lambda \in \Lambda} \frac{1}{z - \lambda}. \tag{2.2}$$

(2.3) The above properties of e_Λ imply that it has an everywhere convergent series expansion $e_\Lambda(z) = \sum_{i \geq 0} \alpha_i z^{q^i}$. We call such functions $\mathbb{F}_q$-linear. It is immediately verified that the set of these is stable under composition. Let $\tau : C \longrightarrow C$ be the Frobenius map $z \longmapsto z^q$. Then e_Λ may be written as $e_\Lambda = \sum \alpha_i \tau^i$, and composition of entire $\mathbb{F}_q$-linear functions corresponds to multiplication in the non-commutative power series ring $C\{\{\tau\}\} = \{\text{formal series } \sum \alpha_i \tau^i \mid \alpha_i \in C\}$, where the usual rule $\tau c = c\tau$ for constants c is replaced by $\tau c = c^q \tau$. Actually, e_Λ belongs to the subring $C_{\mathrm{ent}}\{\{\tau\}\}$ of series $\sum \alpha_i \tau^i$ that satisfy $|\alpha_i| r^{q^i} \longrightarrow 0$ for all $r > 0$. Note that e_Λ is even a "polynomial" in τ if and only if $d := \dim_{\mathbb{F}_q} \Lambda < \infty$, in which case $\deg_\tau(e_\Lambda) = d$.

(2.4) For each $\mathbb{F}_q$-lattice Λ and $k \in \mathbb{N}$, we put

$$E_k(\Lambda) := \sum_{\lambda \in \Lambda}{}' \lambda^{-k},$$

the k-th *Eisenstein series* of Λ. It converges always, but vanishes identically if $k \not\equiv 0 \pmod{q-1}$. For further use, we note the identity

$$\frac{z}{e_\Lambda(z)} = -\sum_{k \geq 0} E_k(\Lambda) z^k, \tag{2.5}$$

which follows from (2.2) by an easy calculation. (Here and in the sequel, we use the convention $E_0(\Lambda) = -1$.) The function $e_\Lambda = 1 + \alpha_1 \tau + \cdots$ has a composition inverse

$$\log_\Lambda = \sum_{i \geq 0} \beta_i \tau^i$$

in $C\{\{\tau\}\}$, whose radius of convergence, regarded as a series $\sum \beta_i z^{q^i}$ in z, equals the *diameter* of Λ, $\mathrm{diam}(\lambda) := \min\{|\lambda| \mid 0 \neq \lambda \in \Lambda\}$. It is an amusing exercise to show

$$\beta_i = -E_{q^i-1}(\Lambda) \quad (i \geq 0). \tag{2.6}$$

2.7 Proposition. *Let Λ be an $\mathbb{F}_q$-lattice in C. There exists a uniquely determined series $G_k(X) = G_{k,\Lambda}(X)$ of polynomials over C ($k \in \mathbb{N}$) that satisfy the identity of meromorphic functions*

(i) $$\sum_{\lambda \in \Lambda} \frac{1}{(z-\lambda)^k} = G_{k,\Lambda}(t_\Lambda(z)).$$

The G_k have the following properties (putting $G_k = 0$ for $k \leq 0$):

(ii) $G_k = X(G_{k-1} + \alpha_1 G_{k-q} + \alpha_2 G_{k-q^2} + \cdots)$

(iii) G_k *is monic of degree* k

(iv) $G_k(0) = 0$

(v) $G_k = X^k$ *if* $1 \leq k \leq q$

(vi) $G_{pk} = (G_k)^p$

(vii) $X^2 G_k'(X) = kG_{k+1}$

(viii) $$\sum_{k \geq 0} G_k(X) u^k = \frac{uX}{1 - Xe_\Lambda(u)} \text{ in } C[[X,u]]$$

(ix) $$G_k(X) = \sum_{0 \leq i < j} \beta_i X^{q^j - q^i}, \text{ if } k = q^j - 1.$$

Here the α_i (β_i) are the coefficients of e_Λ ($\log_\Lambda$), respectively. The G_k are called the *Goss polynomials* of Λ. Items (i)-(vii) are due to David Goss ([14], ch. VI), the remaining appear in [6] sect. 3.

2.8 Remark. All the assertions made in the present section remain valid in an arbitrary field L containing $\mathbb{F}_q$ as long as only finite-dimensional $\mathbb{F}_q$-subspaces Λ of L are considered.

3. Drinfeld modules [15] [10].

In this section, Λ is an A-lattice of finite rank $r \in \mathbb{N}$. For $a \in A$, consider the commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Lambda & \longrightarrow & C & \xrightarrow{e_\Lambda} & C & \longrightarrow & 0 \\ & & \downarrow a & & \downarrow a & & \downarrow \Phi_a^\Lambda & & \\ 0 & \longrightarrow & \Lambda & \longrightarrow & C & \xrightarrow{e_\Lambda} & C & \longrightarrow & 0, \end{array} \tag{3.1}$$

where the left hand vertical maps are multiplication by a and ϕ_a^Λ is defined by the diagram, i.e., by the functional equation

$$e_\Lambda(az) = \phi_a^\Lambda(e_\Lambda(z)). \tag{3.2}$$

Then ϕ_a^Λ belongs to $C\{\tau\}$, the ring of "polynomials" in τ, and, for $a \neq 0$ of degree d, has the form

$$\phi_a^\Lambda = a + l_1(a,\Lambda)\tau + \cdots l_{rd}(a,\Lambda)\tau^{r\cdot d} \tag{3.3}$$

with $l_{rd}(a,\Lambda) \neq 0$, as we see by comparing coefficients in (3.2). The various ϕ_a^Λ commute in $C\{\tau\}$, and $a \longmapsto \phi_a^\Lambda$ defines a homomorphism ϕ^Λ of $\mathbb{F}_q$-algebras from A to $C\{\tau\}$. Now since $C\{\tau\}$ acts on $C = \mathbb{G}_a(C)$, we get a new structure of A-module on the additive group scheme $\mathbb{G}_a/C$, given by

$$a * z = \phi_a^\Lambda(z) \quad (z \in C).$$

Each structure of A-module on $\mathbb{G}_a/C$ given by an $\mathbb{F}_q$-algebra homomorphism $\phi : a \longmapsto \phi_a$ from A to $C\{\tau\}$ subject to (3.3) is called a *Drinfeld A-module of rank r* over C. Note that an $\mathbb{F}_q$-algebra homomorphism from $A = \mathbb{F}_q[T]$ to $C\{\tau\}$ is given through the image of T, which can be prescribed arbitrarily. Drinfeld modules may be defined over arbitrary fields provided with a structure as A-algebra. There are obvious notions of morphisms and isomorphisms of Drinfeld modules, and we have the following "Weierstraß uniformization" result due to Drinfeld [3].

3.4 Theorem. *Each Drinfeld A-module ϕ over C arises from an A-lattice Λ as above, and $\Lambda \longmapsto \phi^\Lambda$ induces an equivalence between the category of A-lattices of rank r in C (morphisms $c : \Lambda \longrightarrow \Lambda'$ are multipliers $c \in C$ such that $c\Lambda \subset \Lambda'$) and the category of Drinfeld A-modules of rank r over C.*

Between the coefficients $l_i(a,\Lambda)$ of ϕ_a^Λ and the Eisenstein series $E_j(\Lambda)$ associated to Λ, the following relation holds (see e.g. [6] 2.10):

$$a\ E_{q^k-1}(\Lambda) = \sum_{i+j=k} E_{q^i-1}(\Lambda) l_j(a,\Lambda)^{q^i}, \tag{3.5}$$

where as in (2.5), the convention $E_0(\Lambda) = -1$ is in force. It allows to recursively determine the E_{q^k-1} from the l_j and vice versa. As a consequence, the function $l_j(a, ?)$ on A-lattices has weight $q^j - 1$, i.e., for $c \in C^*$,

$$l_j(a, c\Lambda) = c^{1-q^j} l_j(a,\Lambda) \tag{3.6}$$

holds.

(3.7) We first consider in detail the case $\boxed{r = 1}$. Each rank-one A-lattice has the form $\Lambda = c \cdot A$ with some constant c. Correspondingly, a rank-one Drinfeld module $\phi = \phi^\Lambda$ is given by $\phi_T^\Lambda = T + l_1(T,\Lambda)\tau$. As results from (3.6), we can find a unique lattice $\Lambda = \bar{\pi}A$ such that its associated Drinfeld module $\rho := \phi^\Lambda$, the so-called *Carlitz module*, satisfies $\rho_T = T + \tau$. Here the period $\bar{\pi}$ is uniquely determined up to a $(q-1)$-th root of unity. We choose one such $\bar{\pi}$ and fix it once for all. We refer to [15] ch. 3 for a detailed study of ρ and the role it plays e.g. in the class field theory of K (which is similar to cyclotomic theory over the rationals $\mathbb{Q}$).

In order to describe e_Λ and $\log_\Lambda$ for $\Lambda = \bar{\pi}A$, we introduce some A-valued arithmetic functions.

$$\begin{array}{lrcll} (3.8) & [i] & := & T^{q^i} - T & (i \geq 0) \\ & D_i & := & [i][i-1]^q \cdots [1]^{q^{i-1}} & \\ & L_i & := & [i][i-1] \cdots [1] & (i \geq 1) \text{ and } D_0 = L_0 = 1. \end{array}$$

(The symbol L_i appears twice: as a field extension of K and as the above element of A. We are confident that no confusion occurs.) As is easily verified,

$$\begin{array}{rcll} [i] & = & \Pi f & (f \in A \text{ monic prime of degree } d|i) \\ D_i & = & \Pi f & (f \text{ monic of degree } i) \\ L_i & = & \text{l.c.m.}\{f\} & (f \text{ monic of degree } i). \end{array}$$

Furthermore, for $\Lambda = \bar{\pi}A$,

$$(3.9) \qquad e_\Lambda = \sum_{i \geq 0} \frac{1}{D_i} \tau^i \quad \text{and} \quad \log_\Lambda = \sum_{i \geq 0} \frac{(-1)^i}{L_i} \tau^i$$

holds. The $(q-1)$-th power of the period $\bar{\pi}$ may be expressed as

$$(3.10) \qquad \begin{aligned} \bar{\pi}^{q-1} &= [1]E_{q-1}(A) = (T^q - T) {\sum_{a \in A}}' a^{1-q} \\ &= -[1] \prod_{i \geq 1} (1 - \frac{[i]}{[i+1]})^{q-1} \\ &= -T^q \lim_{N \to \infty} {\prod_{\substack{a \in A \\ \deg\ a \leq N}}}' (\frac{a}{T^{\deg\ a}})^{q-1}, \end{aligned}$$

which are similar to well-known formulae for the classical counterpart $2\pi i$ of $\bar{\pi}$. (The first of these follows immediately from (3.5), the others are proven in [12] and [5] IV.4, respectively.) In particular,

$$|\bar{\pi}| = |T|^{\frac{q}{q-1}} = q^{\frac{q}{q-1}}.$$

(3.11) We finally define for $0 \neq a \in A$ the a-th *inverse cyclotomic polynomial*

$$f_a(X) := \rho_a(X^{-1}) X^{q^{\deg\ a}} \in A[X].$$

Here $\rho_a(X)$ is the (commutative) polynomial obtained from ρ_a by replacing τ^i through X^{q^i}. Then $f_a(X)$ has degree $|a| - 1$, leading coefficient a and absolute term $f_a(0) =$ leading coefficient of a as a polynomial in T. For example, $f_1(X) = 1$, $f_T(X) = TX^{q-1} + 1$, $f_{T^2}(X) = T^2X^{q^2-1} + (T^q + T)X^{q^2-q} + 1$. Writing

$$\rho_a(X) = \sum_{0 \le i \le d} l_i(a, \Lambda)X^{q^i}$$

with $d = \deg\ a$, we have $l_i \in A$ and $\deg\ l_i = (d - i)q^i$. Using the Newton polygon, we get the uniform bound $|\lambda| \le q^{\frac{1}{q-1}}$ for zeroes λ of $\rho_a(X)$. If now a is monic, $f_a(X) = \prod_{\rho_a(\lambda)=0} (1 - \lambda X)$, and finally by an easy estimate,

$$|f_a(x) - 1| \le \delta^{q^{d-1}(q-1)} \tag{3.12}$$

for all $x \in C$ with $|x| \le \delta \cdot q^{-\frac{1}{q-1}}$, $0 < \delta < 1$.

(3.13) Next, we consider the case $\boxed{r = 2}$. A rank-two A-lattice Λ has the form $\Lambda = A\omega_1 + A\omega_2$, where $\omega_1, \omega_2 \in C$ are K_∞-linearly independent. Multiplying by a suitable constant, we can assume $\Lambda = A\omega + A$, where $\omega \in \Omega$ is determined up to the action of $\Gamma = \mathrm{GL}(2, A)$. On the other hand, a rank-two Drinfeld A-module $\phi = \phi^\Lambda$ over C is given by $\phi_T = T + l_1(T, \Lambda)\tau + l_2(T, \Lambda)\tau^2$, which we write as

$$\phi_T = T + g(\Lambda)\tau + \Delta(\Lambda)\tau^2.$$

Two pairs (g, Δ) and (g', Δ') give rise to isomorphic Drinfeld modules ϕ and ϕ' if and only if $\frac{g^{q+1}}{\Delta} = \frac{g'^{q+1}}{\Delta'}$. We therefore define the j-invariant of ϕ as

$$j(\phi) = \frac{g^{q+1}}{\Delta}.$$

Putting $\Gamma \setminus \Omega$ for the set of orbits of Γ on Ω, we obtain bijections

(3.14)

$$\Gamma \setminus \Omega \xrightarrow{\cong} \left\{ \begin{array}{c} \text{classes of rank-two} \\ A\text{-lattices in } C, \\ \text{up to scaling} \end{array} \right\} \xrightarrow{\cong} \left\{ \begin{array}{c} \text{isomorphism classes} \\ \text{of rank-two Drinfeld} \\ A\text{-modules over } C \end{array} \right\} \xrightarrow{\cong} C,$$

given by $z \longmapsto \Lambda_z := Az + A$, $\Lambda \longmapsto \phi^\Lambda$, and $\phi \longmapsto j(\phi)$, respectively. We thus think of $j : \Gamma \setminus \Omega \xrightarrow{\cong} C$ as a moduli space for rank-two Drinfeld A-modules over C. Of course, the above reminds of the setting of (elliptic) modular forms for the group $\mathrm{SL}(2, \mathbb{Z})$, and the notation chosen is intended to underline the analogy.

4. Modular forms [14] [4] [5] [6].

Before formally defining modular forms for Γ, we describe the moduli space $\Gamma \setminus \Omega \xrightarrow{\cong} C \hookrightarrow \mathbb{P}^1(C)$ and a uniformizer around the "cusp" ∞. (Although the symbol "∞" is used twice for the infinite place of K and for the cusp, i.e., the point at infinity of $\mathbb{P}^1(C)$, the context will always distinguish the two meanings.)

(4.1) First note that γ permutes the subsets $D_{n,x}$ of Ω and acts with finite stabilizers. Therefore, the quotient of Ω by Γ exists in the category of analytic spaces, and has as C-points the point set $\Gamma \setminus \Omega$. We define an *elliptic point of* Γ as some $z \in \Omega$ such that $\Gamma_z := \{\gamma \in \Gamma \mid \gamma z = z\}$ is strictly larger than the generic stabilizer $\{\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right) \mid a \in \mathbb{F}_q^*\}$. We have:

(4.2) There is precisely one Γ-orbit of elliptic points, namely the orbit of $\mathbb{F}_{q^2} - \mathbb{F}_q \hookrightarrow \Omega$. For each elliptic point z, the stabilizer Γ_z is isomorphic with $\mathbb{F}_{q^2}^*$, a cyclic group of order $q^2 - 1$.

In other words, the projection $\Omega \longrightarrow \Gamma \setminus \Omega$ is unramified off elliptic points, and is ramified with index $q + 1 = \frac{q^2-1}{q-1}$ at the elliptic points. Going through the constructions of (3.14), we see that z is elliptic if and only if $j(z) = 0$.

(4.3) Next, let $c > 1$ and $\Omega_c = \{z \in C \mid |z|_i \geq c\}$. If c lies in the value group $q^{\mathbb{Q}}$ of C (which we always assume), Ω_c is an admissible open subspace of Ω. It follows from (1.2) that $\gamma(\Omega_c) \cap \Omega_c \neq \emptyset$ implies $\gamma \in \Gamma_\infty = \{\gamma \in \Gamma \mid \gamma\infty = \infty\} = \{\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in \Gamma\}$. Hence $\Gamma_\infty \setminus \Omega_c$ injects into $\Gamma \setminus \Omega$ as an admissible open subspace. We put

$$t(z) := \frac{1}{e_{\overline{\pi}A}(\overline{\pi}z)} = \overline{\pi}^{-1}\frac{1}{e_A(z)}, \tag{4.4}$$

which is holomorphic on Ω and invariant under shifts $z \longmapsto z + b$, $b \in A$.

4.5 Lemma. (i) *Let $z \in \Omega$ be such that $|z| = |z|_i = q^{d-\epsilon}$ with $0 \leq \epsilon < 1$, $d \in \mathbb{Z}$. Then*

$$\begin{aligned} \log_q |t(z)| \quad = \quad & -q^d(\tfrac{q}{q-1} - \epsilon) \qquad (d \geq 1) \\ & -d - (\tfrac{q}{q-1} - \epsilon) \quad (d \leq 0). \end{aligned}$$

(ii) *If $z \in \Omega$ has imaginary part $|z|_i \geq 1$, the absolute value $|t(z)|$ depends only on $|z|_i$ and satisfies*

$$|z|_i \leq -\log_q |t(z)| \leq c_0|z|_i$$

with some constant $c_0 > 1$ independent of z. Therefore t induces an isomorphism of $A \setminus \Omega_c$ with some pointed ball $B_r - \{0\}$ of radius $r = r(c)$.

Proof. [6] 5.5 + 5.6. $\square$

Now the transformations on Ω and Ω_c induced by Γ_∞ are products of shifts $z \longmapsto z + b$ $(b \in A)$ and multiplications $z \longmapsto az$ $(a \in \mathbb{F}_q^*)$. Furthermore, $t(az) = a^{-1}t(z)$, whence $t^{q-1} : \Gamma_\infty \setminus \Omega_c \xrightarrow{\cong} B_{r'} - \{0\}$ with $r' = r(c)^{q-1}$. Glueing the cusp ∞ to $\Gamma \setminus \Omega \xrightarrow{\cong} C$ therefore corresponds to filling in the missing point in our pointed balls, and $s = t^{q-1}$ may serve as a uniformizer around ∞. Here is the picture.

$$
\begin{array}{ccccccc}
B_{r'} - \{0\} & \xleftarrow[s]{\cong} & \Gamma_\infty \backslash \Omega_c & \hookrightarrow & \Gamma \backslash \Omega & \xrightarrow[j]{\cong} & C \\
\downarrow & & & & & & \downarrow \\
B_{r'} & & & \xrightarrow{s \mapsto s^{-1}} & & & \mathbb{P}^1(C)
\end{array} \tag{4.6}
$$

We may now make the following

4.7 Definition. *A modular form of weight k and type m for $\Gamma = \mathrm{GL}(2, A)$ is a function $f : \Omega \longrightarrow C$ that satisfies*

(i) $f(\gamma z) = \frac{(cz+d)^k}{(\det\ \gamma)^m} f(z) \quad (\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma)$;

(ii) *f is holomorphic on Ω;*

(iii) *f is holomorphic at infinity. That is, for $|z|_i$ large enough, f may be expanded as a convergent power series $f(z) = \sum a_i t^i(z)$.*

We define the order of f at ∞ as $\nu_\infty(f)$ = vanishing order of the power series in t. We further let $M_{k,m}$ be the C-vector space of modular forms of weight k and type m. Then $M_0 := \bigoplus_{k \geq 0} M_{k,0}$ and $M = \bigoplus_{k \geq 0,\ m(\bmod\ q-1)} M_{k,m}$ are C-algebras graded by $\mathbb{N}_0$ and $\mathbb{N}_0 \times \mathbb{Z}/(q-1)$, respectively.

4.8 Remarks. (i) Since $\det\ \gamma \in A^* = \mathbb{F}_q^*$, the type m depends only on $m \pmod{q-1}$.
(ii) If $m \equiv 0 \pmod{q-1}$, any f subject to condition (i) is invariant under Γ_∞ and therefore has an expansion with respect to $s = t^{q-1}$. This is not so in general.
(iii) The existence of a non-trivial modular form of weight k and type m implies that $k \equiv 2m \pmod{q-1}$, as results from looking at $\gamma = \left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$.
(iv) In general, the expansion $\sum a_i t^i$ of f will not converge on all of Ω. Nonetheless, the coefficients a_i determine f uniquely since Ω is connected as an analytic space. By abuse of language, we often write $f = \sum a_i t^i$.

Some examples of forms of type 0 have already appeared.

4.9 Examples. (i) Let $0 < k \equiv 0 \pmod{q-1}$. The Eisenstein series $E_k : z \longmapsto E_k(A_z + A) = \sum'_{a,b \in A} \frac{1}{(az+b)^k}$ is a non-zero element of $M_{k,0}$. Conditions (i) and (ii) of (4.7) are easily verified, and the series expansions are given e.g. in [13] sect. 2 and [6] 6.3.
(ii) Let $0 \neq a \in A$ and $i > 0$. The function $l_{i,a} : z \longmapsto l_i(a, Az + A)$ is a modular form of weight $q^i - 1$ and type zero. In particular, $g = l_{1,T} \in M_{q-1,0}$ and $\Delta = l_{2,T} \in M_{q^2-1,0}$. This may be seen, modulo (i), by expressing $l_{i,a}$ via (3.5) as an isobaric polynomial in the Eisenstein series E_{q^i-1}. E.g., $g = [1]E_{q-1}$, $\Delta = [2]E_{q^2-1} + [1]^q E_{q-1}^{q+1}$.

(iii) It is less easy to find examples of forms with non-trivial types. Here is one. Let H be the subgroup $\{\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)\}$ of Γ, and consider the *Poincaré series*

$$P_{k,m} = \sum_{\gamma \in H \backslash \Gamma} \frac{(cz+d)^k}{(\det\ \gamma)^m} t^m(\gamma z) \quad (\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)).$$

The sum is well-defined, since the γ-th term depends only on the class of γ in $H \setminus \Gamma$. It converges and gives rise to some $0 \neq P_{k,m} \in M_{k,m}$ provided that $k > 0$, $k \equiv 2m \pmod{q-1}$ and $m \leq \frac{k}{q+1}$.

For a modular form $0 \neq f$ and $z \in \Omega$, we let $\nu_z(f)$ be the vanishing order of f at z, which depends only on the orbit of z. The next result is similar to Théorème 3 in ch. II of [17] and may be proved by a rigid analytic analogue of contour integration [11] pp. 93-95; a different proof is given in [5] V.5.

4.10 Theorem. *For $0 \neq f \in M_{k,m}$, the following relation holds:*

$$\sum_{z \in \Gamma \backslash \Omega}{}^{\star} \nu_z(f) + \frac{\nu_e(f)}{q+1} + \frac{\nu_\infty(f)}{q-1} = \frac{k}{q^2-1},$$

where the left hand sum $\sum^\star$ is over the non-elliptic Γ-orbits in Ω and e is some fixed elliptic point.

Putting $h := P_{q+1,1}$, we obtain the vanishing orders given in the table

(4.11)

	ν_e	ν_z, z non-elliptic	ν_∞
g	1	0	0
h	0	0	1
Δ	0	0	$q-1$

Also, E_{q^2-1} has precisely one zero z mod Γ, which is non-elliptic, and corresponds to $j(z) = [1]$. Further, $M_{0,0} = C$, $h^{q-1} = \text{const.}\Delta$, and the next result is an easy consequence.

4.12 Corollary. (i) (*D. Goss* [14]) $M_0 = C[g, \Delta]$,
(ii) $M = C[g, h]$,
where $\{g, \Delta\}$ resp. $\{g, h\}$ are algebraically independent.

The t-expansions of these forms and also of the Eisenstein series may be effectively calculated and turn out to be A-valued after a trivial normalization. We first state the result for Δ.

4.13 Theorem. *$\Delta(z)$ has the product expansion, which converges locally uniformly for $|t| < q^{-\frac{1}{q-1}}$:*

$$\overline{\pi}^{1-q^2}\Delta(z) = -t^{q-1} \prod_{a \in A \text{ monic}} f_a(t)^{(q^2-1)(q-1)}.$$

The formula is proved in [4]. It is similar to the product $q\prod(1-q^n)^{24}$ for the elliptic discriminant: even the exponents $(q^2-1)(q-1)$ and 24 have a common interpretation through values of the zeta functions of K and $\mathbb{Q}$, respectively ([5] VI.4). The radius of convergence comes out from (3.12). Note that, in view of $f_a(t) = 1 + o(t^{q^{\deg\, a-1}(q-1)})$, the product converges formally in the power series ring $A[[t]]$. Hence the coefficients of $\overline{\pi}^{1-q^2}\Delta(z)$ lie in A. A similar assertion is true for the Eisenstein series.

4.14 Theorem. *Let $k \in \mathbb{N}$ be divisible by $q-1$. Then*

$$\overline{\pi}^{-k}E_k = \sum_{i\geq 0} a_i t^i \quad \textit{with certain } a_i \in A\ (i \geq 1) \textit{ and } 0 \neq a_0 \in K.$$

A more precise description of the t-expansion of E_k is given in [6] 6.3. In particular

$$\overline{\pi}^{1-q}g = \overline{\pi}^{1-q}[1]E_{q-1} \in A[[t]].$$

This motivates to rescale our basic modular forms g, Δ by putting

$$g_{\text{new}} := \overline{\pi}^{1-q}g_{\text{old}},\ \Delta_{\text{new}} := \overline{\pi}^{1-q^2}\Delta_{\text{old}}. \tag{4.15}$$

Only this new normalization will be used from now on.

5. Integrality and congruence properties.

(5.1) Let f be a holomorphic A-invariant function on Ω, e.g. a modular form. We define the differential operator θ as $f \longmapsto \theta f := \overline{\pi}^{-1}\frac{df}{dz}$, which on t-expansions is $-t^2\frac{d}{dt}$, as results from (2.2). We further put

$$E := \frac{\theta\Delta}{\Delta} \text{ and } \partial_k f := \theta f + kEf \quad (f \in M_{k,m}).$$

The relevant properties of E and ∂_k are collected as follows. Proofs are given in [6] sect. 8.

5.2 Proposition. (i) *E satisfies the functional equation*

$$E(\gamma z) = \frac{(cz+d)^2}{\det\,\gamma}E(z) - \frac{c}{\overline{\pi}\,\det\,\gamma}(cz+d) \quad \textit{under } \gamma = \left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right) \in \Gamma.$$

(ii)
$$E(z) = \sum_{a\in A \text{ monic}} at(az) = \overline{\pi}^{-1}\sum_{a \text{ monic}} a \sum_{b\in A}\frac{1}{az+b}.$$

5.3 Proposition. (i) $f \in M_{k,m} \Rightarrow \partial_k f \in M_{k+2,m+1}$

(ii) $f_i \in M_{k_i,m_i}$ $(i=1,2) \Rightarrow \partial_{k_1+k_2}(f_1\cdot f_2) = \partial_{k_1}(f_1)f_2 + f_1\partial_{k_2}(f_2)$

We therefore regard $\partial = (\partial_k)$ as a differential operator of weight two on the graded C-algebra M. Now the spaces of $f \in M_{q+1,1}$ (resp. $f \in M_{q^2-1,0}$)

with $\nu_\infty(f) > 0$ have dimension one, which gives the following identities up to multiplicative constants. These constants are determined by comparing leading terms.

5.4 Theorem ([6] Thm. 9.1). *$\partial g = h$ and $h^{q-1} = -\Delta$.*

In the next table, extracted from [6] sect. 10, we give the first few terms of these functions.

5.5 Table.

	expansion with respect to $s = t^{q-1}$
g	$1 - [1]s + [1]s^{q^2-q+1} - [1]s^{q^2} - [1]^2 s^{q^2+1} + o(s^{2q^2-2q+1})$
h/t	$-1 - s^{q-1} + [1]s^q - s^{2q-2} + 2[1]s^{2q-1} - [1]^2 s^{2q} + o(s^{3q-3})$
Δ	$-s + s^q - [1]s^{q+1} - s^{q^2-q+1} + s^{q^2} + o(s^{q^2+1})$
E/t	$1 + s^{q-1} + s^{2q-2} - [1]s^{2q-1} + o(s^{3q-3})$

We define $M_{k,m}(A)$, $M_0(A)$, $M(A)$ to be the respective A-modules of modular forms having t-expansions with A-coefficients. By the above, $h \in M_{q+1,1}(A)$, and from (4.12)-(4.14) we derive:

5.6 Corollary. *$M_{k,m}(A)$ is an A-structure on the C-vector space $M_{k,m}$. Furthermore, $M_0(A) = A[g, \Delta]$ and $M(A) = A[g, h]$.*

It is convenient to also scale the special Eisenstein series of weight $q^k - 1$ as follows. For $k \geq 0$ define

$$g_k := (-1)^{k+1} \bar{\pi}^{1-q^k} L_k E_{q^k-1}. \tag{5.7}$$

Combining some of the preceding material ((2.6), (3.5), (3.9), 4.14)), we arrive at the following description of g_k.

5.8 Proposition. *g_k has absolute term 1 and coefficients in A, and satisfies the recursion*

$$g_k = g_{k-1} g^{q^{k-1}} - [k-1] g_{k-2} \Delta^{q^{k-2}} \quad (k \geq 2)$$

with $g_0 = 1$, $g_1 = g$.

For what follows, we fix a prime $\mathfrak{p}$ of A of degree d and with residue class field $\mathbb{F}_\mathfrak{p} = A/\mathfrak{p}$. Reduction (mod $\mathfrak{p}$) and everything derived from it will be denoted by ($\tilde{\ }$). We consider congruences (mod $\mathfrak{p}$) of modular forms, i.e., of their t-expansions.

5.9 Proposition ([6] 6.11). *For $k \geq 0$, we have*

$$g_{k+d}(t) \equiv g_k(t^{q^d}) \pmod{\mathfrak{p}}.$$

In particular, $g_d \equiv 1 \pmod{\mathfrak{p}}$.

Next, we let $A_{(\mathfrak{p})}$ be the (non-completed) localization of A at $\mathfrak{p}$ and $M_{(\mathfrak{p})}$ the subring of $M(A)\otimes K$ of forms with $\mathfrak{p}$-integral coefficients. We want to determine the image $\tilde{M}$ of the canonical map

$$\begin{aligned} M_{(\mathfrak{p})} \hookrightarrow A_{(\mathfrak{p})}[[t]] &\longrightarrow \mathbb{F}_{\mathfrak{p}}[[t]] \\ f &\longmapsto \tilde{f}. \end{aligned}$$

In order to do so, we need the polynomials $A_k(X,Y)$, $A_k^*(X,Z)$ over A well-defined through the conditions

$$A_k(g,\Delta) = g_k = A_k^*(g,h). \tag{5.10}$$

Let ϕ be the generic Drinfeld module over $A[g,\Delta]$ defined by

$$\phi_T = T + g\tau + \Delta\tau^2,$$

where g and Δ are considered as indeterminates. If for the moment p is the monic generator of $\mathfrak{p}$, we write

$$\phi_p = \sum_{0\le i\le 2d} l_{i,p}\tau^i,$$

where $l_{i,p} = F_{i,\mathfrak{p}}(g,\Delta)$ with some polynomial $F_i = F_{i,\mathfrak{p}} \in A[X,Y]$. The properties of A_k, A_k^*, F_k given below are consequences from (5.4), (5.8), (5.9) and the commutation rule $\phi_p \circ \phi_T = \phi_T \circ \phi_p$ in $A[g,\Delta]\{\tau\}$.

5.11 Proposition. (i) *$A_k(X,Y)$, $A_k^*(X,Z)$ and $F_k(X,Y)$ are isobaric of weight q^k-1, where the variables X, Y, Z have weights $q-1$, q^2-1, $q+1$, respectively.*
(ii) $A_k(X,-Z^{q-1}) = A_k^*(X,Z)$

(iii) $A_0 = 1$, $A_1 = X$, $A_k = A_{k-1}X^{q^{k-1}} - [k-1]A_{k-2}Y^{q^{k-2}} \quad (k\ge 2)$

(iv) $F_0 = p$, $F_1 = \frac{p^q-p}{[1]}X$,

$$[k]F_k = XF_{k-1}^q - X^{q^{k-1}}F_{k-1} + YF_{k-2}^{q^2} - Y^{q^{k-2}}F_{k-2} \quad (k\ge 2).$$

5.12 Proposition. $A_{k+d} \equiv A_k^{q^d}\cdot A_d \pmod{\mathfrak{p}}$

We are especially interested in the polynomial $F_d(X,Y)$ and its reduction $\tilde{F}_d(X,Y)$ (essentially the "Hasse invariant of rank-two Drinfeld modules in characteristic $\mathfrak{p}$"), whose meaning we briefly describe. Recall that $(\tilde{\ })$ is reduction (mod $\mathfrak{p}$). Regarding g,Δ still as indeterminates, but now over $\mathbb{F}_{\mathfrak{p}}$,

$$\tilde{\phi}_T = \tilde{T} + g\tau + \Delta\tau^2 \in \mathbb{F}_{\mathfrak{p}}(g,\Delta)\{\tau\}$$

defines a rank-two Drinfeld module $\tilde{\phi}$ on the A-field $\mathbb{F}_{\mathfrak{p}}(g,\Delta)$ of characteristic $\mathfrak{p}$. Inserting specific values g_0,Δ_0 for g,Δ yields a Drinfeld module, say $\phi^{(g_0,\Delta_0)}$, over the field they generate. The fact that $\tilde{F}_d(g_0,\Delta_0) = 0$ now says that $\phi^{(g_0,\Delta_0)}$ is supersingular [7]. This implies e.g. that $j(\phi^{(g_0,\Delta_0)}) = \frac{g_0^{q+1}}{\Delta_0}$ lies in the quadratic extension of $\mathbb{F}_\mathfrak{p}$.

Let $\epsilon : \mathbb{F}_\mathfrak{p}[X,Y] \longrightarrow \mathbb{F}_\mathfrak{p}[[t]]$ and $\epsilon^* : \mathbb{F}_\mathfrak{p}[X,Z] \longrightarrow \mathbb{F}_\mathfrak{p}[[t]]$ be the homomorphisms that map X, Y, Z to the expansions (mod $\mathfrak{p}$) $\tilde{g}$, $\tilde{\Delta}$, $\tilde{h}$ of g, Δ, h respectively. We can now answer the question about $\tilde{M}$ asked above.

5.13 Theorem ([6] 12.1). (i) $\tilde{A}_d = \tilde{F}_{d,\mathfrak{p}}$, *i.e.*, $A_d \equiv F_{d,\mathfrak{p}} \pmod{\mathfrak{p}}$.
(ii) *The kernel of ϵ is the principal ideal in $\mathbb{F}_\mathfrak{p}[X,Y]$ generated by $\tilde{A}_d(X,Y) - 1$. Similarly,* $\ker \epsilon^* = (\tilde{A}_d^*(X,Z) - 1)$. *Hence $\tilde{M}_0 = \mathbb{F}_\mathfrak{p}[X,Y]/(\tilde{A}_d(X,Y) - 1)$ and $\tilde{M} = \mathbb{F}_\mathfrak{p}[X,Z]/(\tilde{A}_d^*(X,Z) - 1)$.*

5.14 Remark. Assertion (i) states a certain relation between the special Eisenstein series g_d and supersingular j-invariants for rank-two Drinfeld A-modules in characteristic $\mathfrak{p}$, where $\mathfrak{p}$ is a prime of degree d. Checking supersingularity is most easily performed using the polynomial $\tilde{A}_d$, whose calculation is considerably simpler than the one of $\tilde{F}_{d,\mathfrak{p}}$, and depends only on d but not on $\mathfrak{p}$ itself.

Note also that $\tilde{F}_{d,\mathfrak{p}}(X,Y) - 1 \in \ker \epsilon$ means that the t-expansion of $l_{d,p}$ is congruent to the constant 1 (mod $\mathfrak{p}$).

The rings $\tilde{M}_0$ and $\tilde{M}$ are further discussed in [6] sect. 12. These rings are normal, i.e., Dedekind rings, and their spectra are $\mathfrak{p}$-fibers of certain modular curves.

6. Zeroes of Eisenstein series.

(6.1) In this section, we consider the set $\{z \in \Omega \mid E_k(z) = 0\}$ of zeroes of E_k on Ω, where k is divisible by $q - 1$. It is stable under the action of Γ, and consists therefore of the full reciprocal image of a subset of C under $j : \Omega \longrightarrow C$. Such $z \in \Omega$ or their j-invariants $j(z)$ are referred to as z-zeroes or j-zeroes of E_k, respectively. From (4.10) we see that the set of j-zeroes is finite.

6.2 Lemma. *Let $e \in \Omega$ be an elliptic point. Then E_k vanishes in e if and only if k is not divisible by $q^2 - 1$.*

Proof. The "if" part follows from (4.10) and $\nu_\infty(E_k) = 0$ (or directly from the automorphy condition applied to a suitable $\gamma \in \Gamma_e$). Suppose $k \equiv 0 \pmod{q^2 - 1}$. Without restriction, $e \in \mathbb{F}_{q^2}$. Then $E_k(e) = \sum_{a \in A^{(2)}} a^{-k} = E_k(A^{(2)})$ with $A^{(2)} = \mathbb{F}_{q^2}[T]$, and the assertion follows from the next lemma upon replacing q by q^2. $\square$

6.3 Lemma. *Let $k \in \mathbb{N}$ be divisible by $q - 1$. Then $E_k(A) \neq 0$.*

Proof. In K_∞, we have (mod π) : $E_k(A) \equiv \sum_{a \in \mathbb{F}_q^*} a^{-k} = \sum_{a \in \mathbb{F}_q^*} 1 = -1$. $\square$

We next put

$$\text{(6.4)} \qquad \mathcal{F} = \{z \in \Omega \mid |z| = |z|_i \geq 1\} \text{ and } \mathcal{F}_0 = \{z \in \Omega \mid |z| = |z|_i = 1\},$$

which are admissible open subsets of Ω. We further define a sequence of subgroups Γ_i of Γ as follows:

$$\Gamma_0 = \mathrm{GL}(2, \mathbb{F}_q),\ \Gamma_i = \{\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in \Gamma \mid a, d \in \mathbb{F}_q^*,\ \deg\ b \leq i\},\ i \geq 1.$$

Then $\Gamma_\infty =$ stabilizer of $\infty \in \mathbb{P}^1(K) = \bigcup_{i \geq 1} \Gamma_i$.

$\mathcal{F}$ is as close to a fundamental domain for Γ on Ω as is possible in our situation.

6.5 Proposition. (i) *Each element of* Ω *is* Γ*-equivalent to some element of* $\mathcal{F}$. (ii) *Let* $z, z' = \gamma z$ $(\gamma \in \Gamma)$ *be* Γ*-equivalent in* $\mathcal{F}$, $k := [\log_q |z|]$ *the greatest integer less or equal to* $\log_q |z|$. *Then* $\gamma \in \Gamma_k$. *In particular,* $|z'| = |z| = |z|_i = |z'|_i$.

Proof. (i) Let $z \in \Omega$ be given, and suppose that $|z|_i < 1$. Applying some $\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma_\infty$, we can achieve that also $|z| < 1$. If $\log_q |z| \notin \mathbb{Z}$ then $|z| = |z|_i$, hence $|z^{-1}|_i = |z^{-1}| = |z|^{-1} = |z|_i^{-1} > 1$ and $z^{-1} = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) z \in \mathcal{F}$. If $\log_q |z| \in \mathbb{Z}$, the formula $|z^{-1}|_i = |z|^{-2}|z|_i$ shows that $|z^{-1}| \geq |z^{-1}|_i \geq q^2 |z|_i$. After a finite number of steps we thus arrive at some $z' = \gamma z$ with $|z'|_i \geq 1$. Again applying some $\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma_\infty$ if necessary, we get $|z'| = |z'|_i \geq 1$.
(ii) This is a consequence of (1.2) and $|cz + d| = \max\{|c||z|, |d|\}$ for $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$. $\square$

The next result is proved in [8] Thm. 2.17.

6.6 Theorem. *For* $z \in \mathcal{F}$, *we have*

$$\begin{array}{rcll} \log_q |j(z)| & = & q^d(q - \epsilon(q-1)) & \text{if } |z| = |z|_i > 1 \\ & \leq & q & \text{if } |z| = |z|_i = 1, \end{array}$$

where, as in (4.5), $|z| = |z|_i = q^{d-\epsilon}$ *with* $d \in \mathbb{N}$ *and* $0 \leq \epsilon < 1$.

Note that $\log_q |j(z)|$ only depends on $|z|_i$ as long as $|z|_i > 1$. Further, $\log_q |j(z)| = q|z|_i$ if $\log_q |z|_i \in \mathbb{N}$, and its values for non-integral $\log_q |z|_i$ interpolate linearly.

6.7 Proposition. *Let* $k \in \mathbb{N}$ *be divisible by* $q - 1$. *The Eisenstein series* E_k *satisfies* $|E_k(z)| \leq 1$ *for* $z \in \mathcal{F}$ *with equality if* $z \notin \mathcal{F}_0$. *In particular, the set of* z*-zeroes of* E_k *is contained in* $\mathcal{F}_0$. *Each* j*-zero* $j(t)$ *satisfies* $|j(z)| \leq q^q$.

Proof. For $a, b \in A$ and $z \in \mathcal{F}$, we have $|az + b| = \max\{|az|, |b|\} \geq 1$, from which $|E_k(z)| \leq 1$ results. If moreover $z \notin \mathcal{F}_0$, $|az + b| > 1$ for $(a, b) \neq (0, c)$ with $c \in \mathbb{F}_q$. Hence

$$|E_k(z)| = |\sum_{a,b \in A} \frac{1}{(az+b)^k}| = |\sum_{c \in \mathbb{F}_q^*} \frac{1}{c^k}| = 1.$$

The last statement follows from (6.6). $\square$

6.8 Remark. The zeroes of Eisenstein series in general fail to be simple, for essentially trivial reasons. Let for example $k = a(q-1)$ with $1 \leq a \leq q$. From dim $M_{k,0} = 1$, $E_k = \text{const.}\ E_{q-1}^a$ (in fact, $E_k = (-1)^{a+1}E_{q-1}^a$), and thus has an a-fold zero at elliptic points. Other multiple zeroes arise, of course, from $E_{pk} = E_k^p$ ($p = \text{char}(\mathbb{F}_q)$). A less trivial example is given in (6.12).

(6.9) We next discuss how to calculate the E_k. Recall that $E_k(z) = E_k(\Lambda_z)$ with $\Lambda_z = Az + A$, and so the identities of sect. 2 may be applied. Write e_z for the exponential function e_{Λ_z} associated to Λ_z by (2.1) and $\log_z$ for its composition inverse. They have expansions

$$e_z(w) = \sum_{i \geq 0} \alpha_i(z) w^{q^i}, \quad \log_z(w) = \sum \beta_i(z) w^{q^i},$$

where the coefficients α_i, β_i are holomorphic in z (actually, modular forms of weight $q^i - 1$ and type 0). From

$$w = \frac{w}{e_z(w)} e_z(w) = (-\sum_{i \geq 0} E_i(z) w^i)(\sum_{j \geq 0} \alpha_j(z) w^{q^j}),$$

we get the relation, valid for $k \geq 1$:

$$E_k(z) + \alpha_1(z) E_{k+1-q} + \alpha_2(z) E_{k+1-q^2} + \cdots = 0, \tag{6.10}$$

where as usual, $E_0 = -1$ and $E_k = 0$ if $k < 0$. It allows recursive calculation of the E_k from the α_j, which in turn are determined through the β_j, i.e., special Eisenstein series. Viz.,

$$\sum_{i+j=k} \alpha_i \beta_j^{q^i} = 0 \quad (k \geq 1). \tag{6.11}$$

We illustrate this by the following example.

6.12 Example. Let $k < q^3 - 1$ be divisible by $q - 1$. From (6.10),

$$E_k = -\alpha_1 E_{k+1-q} - \alpha_2 E_{k+1-q^2}.$$

Further

$$\alpha_1 = -\beta_1 = E_{q-1}, \quad \alpha_2 = -\beta_2 + \beta_1^{q+1} = E_{q^2-1} + E_{q-1}^{q+1},$$

thus

$$E_k = -E_{q-1}E_{k+1-q} - E_{q^2-1}E_{k+1-q^2} - E_{q-1}^{q+1}E_{k+1-q^2}.$$

Similar recurrence formulae may be written down for larger k. More specifically, consider $k = 2(q^2 - 1)$. We have

$$\begin{aligned} E_{2(q^2-1)} &= -E_{q-1}(-E_{q-1}E_{2q^2-2q} - E_{q^2-1}E_{q^2-q} - E_{q-1}^{q+1}E_{q^2-q}) \\ &\quad -E_{q^2-1}^2 - E_{q-1}^{q+1}E_{q^2-1} \\ &= -E_{q^2-1}^2, \end{aligned}$$

using $E_{qi} = E_i^q$ and $E_{2(q-1)} = -E_{q-1}^2$. This somewhat mysterious identity is not forced by dimension reasons since dim $M_{2(q^2-1),0} = 3$. It would be interesting to know which subscripts k give rise to similar identities, i.e., for which tuples $k_1, \dots, k_s, l_1, \dots, l_t$ subject to $\sum k_i = \sum l_j$, we have a relation $\prod E_{k_i} = \prod E_{l_j}$ up to sign.

7. The polynomials φ_k and ψ_k.

In the present section, strongly influenced from [1], we study in more detail the special Eisenstein series E_{q^k-1} or rather the $g_k = (-1)^{k+1}\overline{\pi}^{1-q^k} L_k E_{q^k-1}$.

We first define the one-variable version of the polynomial $A_k(X, Y)$ of (5.10).

7.1 Lemma. *A_k, considered as a polynomial in X, is monic of degree $(q^k-1)/(q-1)$. It is not divisible by X if k is even, and exactly once divisible by X if k is odd.*

Proof. Obvious from (5.11). □

For what follows, we let $\chi, \lambda, \mu : \mathbb{N} \longrightarrow \mathbb{N}_0$ be defined by

$$(7.2) \qquad \begin{aligned} \chi(k) &= 0 \quad \text{for even and } \chi(k) = 1 \text{ for odd } k \\ \lambda(k) &= \frac{q^{k-1} + (-1)^k}{q+1} \\ \mu(k) &= \frac{q^k - q^{\chi(k)}}{q^2 - 1}. \end{aligned}$$

We further put

$$\varphi_k = \frac{A_k(X,Y)}{X^{\chi(k)} Y^{\mu(k)}}.$$

By the lemma, φ_k is a monic polynomial of degree $\mu(k)$ in $\frac{X^{q+1}}{Y}$. By abuse of notation, we also use "X" as the indeterminate of $\varphi_k = \varphi_k(X)$. Its crucial property (which follows directly from its construction) is

$$(7.3) \qquad g_k = g^{\chi(k)} \Delta^{\mu(k)} \varphi_k(j).$$

Further, for non-elliptic $z \in \Omega$, we have the equivalence

$$\varphi_k(j(z)) = 0 \Leftrightarrow g_k(z) = 0.$$

7.4 Proposition. *We have $\varphi_0 = \varphi_1 = 1$ and for $k \geq 2$*

$$\varphi_k(X) = X^{\lambda(k)} \varphi_{k-1}(X) - [k-1] \varphi_{k-2}(X).$$

Proof. Translation of (5.11) (iii). □

Note that the quantity $\lambda(k)$ is strictly larger than $\mu(k-2) = \deg\ \varphi_{k-2}$, and therefore no cancellation takes place in the formula.

7.5 Example. The first few φ_k are $\varphi_0 = \varphi_1 = 1$, $\varphi_2 = X - [1]$,

$$\begin{aligned}
\varphi_3 &= X^q - [1]X^{q-1} - [2] \\
\varphi_4 &= X^{q^2+1} - [1]X^{q^2} - [2]X^{q^2-q+1} - [3]X + [1][3] \\
\varphi_5 &= X^{q^3+q} - [1]X^{q^3+q-1} - [2]X^{q^3} - [3]X^{q^3-q^2+q} \\
&\quad +[1][3]X^{q^3-q^2+q-1} - [4]X^q + [1][4]X^{q-1} + [2][4].
\end{aligned}$$

As in section 5, we let $\mathfrak{p}$ be a prime of A of degree d with residue field $\mathbb{F}_\mathfrak{p}$ and reduction map $x \longmapsto \tilde{x}$. Translating (5.12) (or directly using induction from (7.4)) yields

7.6 Proposition. *For $k \geq 0$, φ_k satisfies the congruence*

$$\varphi_{k+d}(X) \equiv X^{\chi(k)\lambda(d+1)}\varphi_k^{q^d}\varphi_d \pmod{\mathfrak{p}}. \quad \square$$

7.7 Theorem. (i) *The polynomial φ_d is square-free. Hence $\varphi_d(X) = \prod(X-j)$, where j runs over the non-elliptic j-zeroes of g_d.*
(ii) *All the z-zeroes of g_d (and thus of E_{q^d-1}) are simple.*

Proof. (i) It is shown in [6] 11.7 that the polynomial $\tilde{F}_{d,\mathfrak{p}}$ of (5.10) is square-free, hence also its dehomogenized version $\tilde{F}_{d,\mathfrak{p}}(X,Y)/Y^m X^{\deg - m(q^2-1))/(q-1)}$, which is a polynomial $f(\frac{X^{q+1}}{Y})$ in $\frac{X^{q+1}}{Y}$. Here $\deg = \deg\ \tilde{F}_{d,\mathfrak{p}} = q^d - 1$ and $m = \max\{i \mid i(q^2-1) \leq \deg\}$. But $\tilde{F}_{d,\mathfrak{p}} = \tilde{A}_d$ (5.13), and so $\tilde{\varphi}_d(X) = f(X)$ is square-free, too, as well as $\varphi_d(X)$ itself.
(ii) Let $z_0 \in \Omega$ be non-elliptic. Since the j-invariant $j : \Omega \longrightarrow C$ is unramified in z_0, we have $\mathrm{ord}_{z_0} g_d(z) = \mathrm{ord}_{j(z_0)}\varphi_d(j)$, which is ≤ 1 by (i). Let now e be an elliptic point. From (6.2) we see that $g_d(e) = 0$ if and only if d is odd. The precise vanishing order $\nu_e(g_d) = 1$ (for d odd) results from (i) and (4.10), since $\#\{j \neq 0 \mid j \text{ a } j\text{-zero of } g_d\} = \deg\ \varphi_d = \mu(d) = \frac{\text{weight of } g_d}{q^2-1} - \frac{1}{q+1}$. $\square$

7.8 Remarks. (i) As the proof shows, $\tilde{\varphi}_d(X) = \prod(X-j)$, where j runs through the supersingular invariants $j \neq 0$ of rank-two Drinfeld modules in characteristic $\mathfrak{p}$. Hence the j-zeroes of g_d provide a canonical lift of these to the generic characteristic. This also gives a canonical way of identifying the sets $\sum(\mathfrak{p})$ of supersingular invariants in different characteristics $\mathfrak{p}$ of the same degree d.
(ii) An alternative proof of the theorem, which avoids the above congruence and supersingularity considerations, may be given as follows ([5] VII.3, [1] I 3.4): Suppose $z_0 \in \mathcal{F}$ is a zero of E_{q^d-1}. Then we know from (6.7) that $|z_0| = |z_0|_i = 1$. Hence for $a, b \in A$, $|az_0 + b| = \max\{|a|, |b|\}$, and we can estimate the terms in $\frac{d}{dz}E_{q^d-1}(z_0) = \sum_{a,b}{}' \frac{a}{(az_0+b)^{q^d}}$, which eventually yields $\frac{d}{dz}E_{q^d-1}(z_0) \neq 0$.

We already know from (6.7) and (7.3) that the roots of $\varphi_k(X)$, i.e., the non-zero j-roots of g_k, are $\leq q^q$ in absolute value. In fact, equality holds.

7.9 Proposition. *All the roots x of $\varphi_k(X)$ satisfy $|x| = q^q$.*

Proof. It suffices to verify that the Newton polygon of φ_k over K_∞ is a straight line with slope q. More explicitly, write

$$\varphi_k = \sum_{0 \leq i \leq \mu(k)} a_{k,i} X^{\mu(k)-i}.$$

Then it is straightforward from (7.4) that

(i) $-v(\varphi_k(0)) = \deg(\varphi_k(0)) = q \cdot \deg\ \varphi_k$ and

(ii) $-v(a_{k,i}) = \deg(a_{k,i}) \leq q^i$ for all i,

which yields the result. $\square$

7.10 Questions/Remarks. Concerning the polynomials φ_k and their splitting fields L_k over K, several natural questions arise, which have obvious analogues for classical Eisenstein series over $\mathbb{Q}$.
(i) Is φ_k always irreducible?
(ii) Is the Galois group $\mathrm{Gal}(\varphi_k)$ the full symmetric group?
(iii) Which places of K are ramified in L_k, and what is the discriminant $D_{L_k/K}$?

The "classical" counterpart for φ_k is (for a natural prime $p > 3$)

$$\varphi_p(X) = \prod (X - j),$$

where j runs through the non-elliptic (i.e., $j \neq 0, 1728$) j-zeroes of $E_{p-1}(z) = \sum_{a,b\in\mathbb{Z}}{}' \frac{1}{(az+b)^{p-1}}$. For $p < 89$ (for all p?), φ_p is irreducible over $\mathbb{Q}$ with the full symmetric group $S_{\deg\ \varphi_p}$ as its Galois group, as has been checked by G. Cornelissen, using MAPLE. In our function field situation, we have: φ_k is irreducible over K. Furthermore, $\mathrm{Gal}(\varphi_k) = S_{\deg\ \varphi_k}$ at least if $k \geq 4$ is even and q is odd [2]. The case $k = 3$ is degenerate and yields the affine group $\{\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) \mid a \in \mathbb{F}_q^*,\ b \in \mathbb{F}_q\}$ over $\mathbb{F}_q$ as Galois group of φ_3 ([1] I.6.2). For $k \leq 2$, $\deg\ \varphi_k \leq 1$. Question (iii) will be dealed with below; see also (8.11) and (8.12).

7.11 Definition. *For $k \in \mathbb{N}$, put*

$$\mathcal{D}_k = \prod_{0<i<k} [i]^{\mu(k)-\mu(i)-\chi(k-i)}.$$

Based on numerical calculations, G. Cornelissen conjectured that, up to a constant in $\mathbb{F}_q^*$, $\mathcal{D}_k = \mathrm{disc}(\varphi_k)$. A first step into this direction is

7.12 Proposition. $|\mathrm{disc}(\varphi_k)| \leq |\mathcal{D}_k|$.

Proof ([1] I.7.3; beware of misprints!). We have

$$(*) \qquad |\mathrm{disc}(\varphi_k)| = \prod_{\substack{x \neq y \\ \varphi_k(x)=0=\varphi_k(y)}} |x-y| \leq \prod_{x\neq y} q^q = q^{q\mu(k)(\mu(k)-1)}.$$

After a lengthy but elementary calculation,

$$|\mathcal{D}_k| = \prod_{0<i<k} q^{q^i(\mu(k)-\mu(i)-\chi(k-i))}$$

evaluates to the right hand side of (*), which gives the result. □

7.13 Example (*loc. cit.* 7.2). $\pm\mathrm{disc}(\varphi_3) = \mathcal{D}_3$

Proof. $\varphi_3(X) = X^q - [1]X^{q-1} - [2]$, hence the equalities up to sign

$$\mathrm{disc}(\varphi_3) = \prod_{\varphi_3(x)=0} \varphi_3'(x) = \prod_x [1]x^{q-2} = [1]^q[2]^{q-2} = \mathcal{D}_3. \quad \square$$

We next show that $\mathrm{disc}(\varphi_k)$ and $\mathcal{D}_k$ have the same finite prime divisors.

7.14 Theorem. *Let $\mathfrak{p}$ be a prime of A of degree d and $k \geq 3$. The reduction $\tilde{\varphi}_k$ of φ_k (mod $\mathfrak{p}$) has multiple roots if $k > d$ (except for $(q,d,k) = (2,2,3)$) and is square-free for $k \leq d$.*

Proof. The assertion follows for $k > d$ from (7.6) and for $k = d$ from the proof of (7.7), i.e., the fact that $\tilde{\varphi}_d$ is the square-free supersingular polynomial. For the case $k < d$ (actually, $k \leq d$: we therefore get a second proof for $k = d$), we use a variant of the argument given in [6] Thm. 12.6.

It suffices to show that the plane affine curve over $\mathbb{F}_\mathfrak{p}$ defined by $A_k(X,Y) = 0$ is non-singular off $(X,Y) = (0,0)$, as long as $k \leq d$. Here and in the remainder of the proof, we suppress the ($\tilde{}$) for "reduction mod $\mathfrak{p}$". This is checked directly for $k = 1$ or 2. ($A_1 = X$, $A_2 = X^{q+1} - [1]Y$.) For $k \geq 3$, we have

$$\begin{aligned}
\frac{\partial}{\partial X}A_k(X,Y) &= \frac{\partial}{\partial X}A_{k-1}\cdot X^{q^{k-1}} - [k-1]\frac{\partial}{\partial X}A_{k-2}\cdot Y^{q^{k-2}} \\
\frac{\partial}{\partial Y}A_k(X,Y) &= \frac{\partial}{\partial Y}A_{k-1}\cdot X^{q^{k-1}} - [k-1]\frac{\partial}{\partial Y}A_{k-2}\cdot Y^{q^{k-2}}.
\end{aligned}$$

Hence

$$(*) \qquad \frac{\partial}{\partial X}A_k(X,Y) = 0 = \frac{\partial}{\partial Y}A_k(X,Y)$$

is equivalent with the matrix equation

$$(**) \qquad \begin{pmatrix} \frac{\partial}{\partial X}A_{k-1} & \frac{\partial}{\partial X}A_{k-2} \\ \frac{\partial}{\partial Y}A_{k-1} & \frac{\partial}{\partial Y}A_{k-2} \end{pmatrix} \begin{pmatrix} X^{q^{k-1}} \\ -[k-1]Y^{q^{k-2}} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

If V_k denotes the 2×2-determinant in (**), an elementary calculation left to the reader yields

$$V_3 = [1],\ V_{k+1} = [k-1]Y^{q^{k-2}}\cdot V_k \quad (k \geq 3).$$

Taking into account that "$A_k(X,0) = 0 \Rightarrow X = 0$" (7.1), we now use induction to prove the statement

$$S(k): \quad \text{"(*) implies } (X,Y) = (0,0)\text{"}.$$

This turns out to hold as long as $[k-1] \not\equiv 0 \pmod{\mathfrak{p}}$, i.e., as long as $k \leq d$ (3.8). The proof is finished. $\square$

Comparing with the definition of $\mathcal{D}_k$, we see that $\mathcal{D}_k$ and $\operatorname{disc}(\varphi_k)$ have the same finite prime divisors. In particular, the splitting field L_k of φ_k is unramified at places $\mathfrak{p}$ of A of degree $d \geq k$.

Similar considerations that led us to the properties of the zeroes of g_k may also be applied to the functions

$$h_k := \partial g_k. \tag{7.15}$$

7.16 Proposition. (i) *The two series* (h_k) *and* $({}_1h_k)$ *(where* ${}_1h_k := \frac{h_k}{h_1}$*) satisfy the same recursion*

$$h_k = h_{k-1} \cdot g^{q^{k-1}} - [1]h_{k-2}\Delta^{q^{k-2}} \quad (k \geq 2)$$

as the series (g_k)*, with initial conditions* $h_0 = 0$*,* $h_1 = h$ *and* ${}_1h_0 = 0$*,* ${}_1h_1 = 1$*, respectively.*
(ii) ${}_1h_1 = {}_2h_k^q$ *with some* ${}_2h_k \in M_{q^k-1,0}$ *that satisfies*

$$\begin{aligned} {}_2h_k &= {}_2h_{k-1}g^{q^{k-2}} - [k-1]_2^{q^{-1}} h_{k-2}\Delta^{q^{k-3}} \quad (k \geq 2) \\ {}_2h_0 &= 0, \quad {}_2h_1 = 1. \end{aligned}$$

Proof. Immediate from applying the differential operator ∂ to (5.8), and using the fact that taking q-th roots is well-defined and additive. $\square$

Note that ${}_2h_k$ has its coefficients in $A[T^{q^{-1}}] = \mathbb{F}_q[T^{q^{-1}}]$.

Let now $B_k(X,Z) \in A[X,Z]$ be the unique polynomial such that $B_k(g,h) = h_k$. From (5.10) and $\partial h = 0$, we have

$$B_k(X,Z) = \frac{\partial}{\partial X} A_k^*(X,Z)Z = \frac{\partial}{\partial X} A_k(X, -Z^{q-1})Z,$$

where $\frac{\partial}{\partial X} A_k(X, -Z^{q-1})$ is homogeneous of weight $q^k - q$. (As usual, the weights of X and Z are $q-1$ and $q+1$, respectively.) The largest power of $Y := -Z^{q-1}$ of weight $\leq q^k - q$ is $Y^{\mu(k)-\chi(k+1)}$, and

$$\frac{\frac{\partial}{\partial X} A_k(X,Y)}{Y^{\mu(k)-\chi(k+1)}} = \text{polynomial in } \frac{X^{q+1}}{Y} \text{ times } X^{q\chi(k+1)}.$$

We therefore define the polynomial ψ_k by

$$\psi_k\left(\frac{X^{q+1}}{Y}\right) = \frac{B_k(X,Z)}{Y^{\mu(k)-\chi(k+1)} \cdot X^{q\chi(k+1)} \cdot Z}, \tag{7.17}$$

which is similar to the polynomial φ_k of (7.2). It has the properties analogous to (7.3) and (7.4):

$$h_k = g^{q\chi(k+1)} \cdot \Delta^{\mu(k)-\chi(k+1)} \cdot h \cdot \psi_k(j) \tag{7.18}$$

and for non-elliptic $z \in \Omega$,

$$\psi_k(j(z)) = 0 \Leftrightarrow h_k(z) = 0;$$

$$\begin{aligned} &\psi_0 = \psi_1 = 1, \text{ and for } k \geq 2, \\ &\psi_k(X) = X^{\lambda(k)-(-1)^k}\psi_{k-1}(X) - [k-1]\psi_{k-2}(X). \end{aligned} \tag{7.19}$$

The first few of them are $\psi_2 = 1$, $\psi_3 = X^q - [2]$,

$$\begin{aligned} \psi_4 &= X^{q^2} - [2]X^{q^2-q} - [3] \\ \psi_5 &= X^{q^3+q} - [2]X^{q^3} - [3]X^{q^3-q^2+q} - [4]X^q + [2][4]. \end{aligned}$$

Also, one shows without difficulty:

(7.20) ψ_k is monic of degree $\deg\ \psi_k = \deg\ \phi_k - \chi(k+1) = \mu(k) - \chi(k+1)$ and $\deg(\psi_k(0)) = q \cdot \deg\ \psi_k$. Further, writing $\psi_k(X) = \sum a_{k,i}X^{\deg\ \psi_k - i}$ with $a_i \in A$, we have $\deg\ a_{k,i} \leq qi$. Hence again the Newton polygon of ψ_k is a straight line of slope q, and the next result follows.

7.21 Proposition. *All the roots x of $\psi_k(X)$ and hence all the j-zeroes $x \neq 0$ of $h_k = \partial g_k$ satisfy $|x| = q^q$.* $\square$

7.22 Remark. The ψ_k are q-th powers of polynomials with coefficients in $\mathbb{F}_q[T^{q^{-1}}]$. Since for non-elliptic z, $\nu_z(h_k) = \mathrm{ord}_{j(z)}\psi_k(j)$, this is in keeping with the fact that all the $\nu_z(h_k)$ are divisible by q. We shall see later (8.14) that $\nu_z(h_k)$ actually equals q for all zeroes z of h_k. We also note that the present ψ_k slightly differ from those ψ_k^C defined in [1]; the relation is $\psi_k^C(X) = X^{\chi(k+1)}\psi_k(X)$.

8. Location of zeroes of special Eisenstein series and of their Serre derivatives.

We already know that all the zeroes $z \in \mathcal{F}$ of g_k and h_k satisfy $z \in \mathcal{F}_0$, i.e., $|z| = |z|_i = 1$, with $|j(z)| = 0$ or q^q. Here we investigate how the zeroes are distributed in $\mathcal{F}_0$. First note that C has $\overline{\mathbb{F}}_q$, the algebraic closure of $\mathbb{F}_q$, as its residue class field. For $z \in O_C = \{z \in C \mid |z| \leq 1\}$, we have

$$\begin{aligned} z \in \mathcal{F}_0 \quad &\Leftrightarrow \quad \exists\ z_0 \in \overline{\mathbb{F}}_q - \mathbb{F}_q \text{ such that } |z - z_0| < 1 \\ &\Leftrightarrow \quad \mathrm{red}(z) \notin \mathbb{F}_q, \end{aligned} \tag{8.1}$$

where $\mathrm{red} : O_C \longrightarrow O_C/\mathfrak{m}_C = \overline{\mathbb{F}}_q$ is the reduction map. The idea is to approximate $E_k(z)$ by the truncated series

$$\begin{aligned} \tilde{E}_k(z) &= \sideset{}{'}\sum_{a,b\in\mathbb{F}_q} \frac{1}{(az+b)^k} \quad \text{and} \\ \overline{\pi}t(z) &= e_A^{-1}(z) = \sum_{a\in A} \frac{1}{z-a} \end{aligned} \tag{8.2}$$

by

$$\tilde{t}(z) = e_{\mathbb{F}_q}^{-1}(z) = \sum_{a \in \mathbb{F}_q} \frac{1}{z-a},$$

which at the same time may be considered as reductions mod $\mathfrak{m}_C$ of E_k, e_A^{-1}, respectively. We therefore deal first with these "finite Eisenstein series", i.e., lattice sums over finite-dimensional $\mathbb{F}_q$-lattices.

8.3 Proposition. *Let k be divisible by $q-1$. Then as rational functions,*

$$\tilde{E}_k(z) = -(1 + G_k(\tilde{t})),$$

where $G_k(X)$ is the k-th Goss polynomial attached to the $\mathbb{F}_q$-lattice $\mathbb{F}_q$. We have

$$G_k(X) = \sum_{0 \le i \le (k-1)/q} \binom{k-1-i(q-1)}{i} (-1)^i X^{k-i(q-1)},$$

and in particular,

$$G_{q^k-1}(X) = \sum_{0 \le i < k} X^{q^k - q^i}.$$

Proof.

$$\begin{aligned}
\tilde{E}_k(z) &= {\sum_{b \in \mathbb{F}_q}}' b^{-k} + {\sum_{a \in \mathbb{F}_q}}' \sum_{b \in \mathbb{F}_q} \frac{1}{(az+b)^k} = -1 + {\sum_a}' \sum_b \frac{1}{(z+b/a)^k} \\
&= -1 - \sum_b \frac{1}{(z+b)^k} = -1 - G_k(\tilde{t}) \text{ by (2.7) (i).}
\end{aligned}$$

Furthermore,

$$\sum_{k \ge 0} G_k(X) u^k = \frac{uX}{1 - X e_{\mathbb{F}_q}(u)} = \frac{uX}{1 - X(u - u^q)},$$

which yields the stated $G_k(X)$ upon expanding the geometric series. Analyzing the binomial coefficients in $G_l(X)$ for l of the special form $l = q^k - 1$ (or applying (2.7) (ix), combined with $\log_{\mathbb{F}_q}(z) = \sum_{i \ge 0} z^{q^i}$) gives the last formula. □

8.4 Proposition. *For $z \in \mathcal{F}_0$ we have:*

$$\tilde{E}_{q^k-1}(z) = 0 \Leftrightarrow z \in \mathbb{F}_{q^{k+1}} - \mathbb{F}_q,$$

and all the roots are simple.

Proof. Let $z \in \mathcal{F}_0$. Then

$$\tilde{E}_{q^k-1}(z) = 0 \Leftrightarrow 1 + \sum_{0 \le i < k} \tilde{t}(z)^{q^k - q^i} = 0$$

$$\Leftrightarrow \sum_{0 \le i \le k} e_{\mathbb{F}_q}^{q^i}(z) = 0 \text{ (since } z \notin \mathbb{F}_q \text{ and therefore } \tilde{t}(z) \text{ is finite and non-zero)}$$

$\Leftrightarrow z = z^{q^{k+1}}$, as $e_{\mathbb{F}_q}(z) = z - z^q$.

Using again (2.7), parts (vi) and (vii), and $\frac{d}{dz}\tilde{t}(z) = -\tilde{t}^2(z)$, we have for $z_0 \in \mathbb{F}_{q^{k+1}} - \mathbb{F}_q$, $\tilde{t}_0 = \tilde{t}(z_0)$:

$$\frac{d}{dz}\tilde{E}_{q^k-1}(z) = -G'_{q^k+1}(\tilde{t}_0)\tilde{t}_0^2 = G_{q^k}(\tilde{t}_0) = \tilde{t}_0^{q^k} \neq 0,$$

i.e., the simplicity of the roots. $\square$

We now come back to $E_{q^k-1} = \sum'_{a,b\in A} \frac{1}{(az+b)^{q^k-1}}$ itself. Let $z \in \mathcal{F}_0$ be a zero. If at least one of a, b is non-constant, the term $(az+b)^{1-q^k}$ is less than 1 in absolute value. Hence, modulo $\mathfrak{m}_C$,

$$0 = E_{q^k-1}(z) \equiv \sum_{a,b\in\mathbb{F}_q}{}' \frac{1}{(az+b)^{q^k-1}} = \tilde{E}_{q^k-1}(z),$$

i.e., $z \equiv z_0 \in \mathbb{F}_{q^{k+1}} - \mathbb{F}_q$. On the other hand, given $z_0 \in \mathbb{F}_{q^{k+1}} - \mathbb{F}_q$, we have $E_{q^k-1}(z_0)| < 1$ and $|\frac{d}{dz}E_{q^k-1}(z_0)| = |\frac{d}{dz}\tilde{E}_{q^k-1}(z_0)| = 1$, hence by Hensel's lemma, there exists a unique zero z of E_{q^k-1} congruent to z_0. We have therefore proved the following theorem.

8.5 Theorem. *For each $z_0 \in \mathbb{F}_{q^{k+1}} - \mathbb{F}_q$, there exists a unique zero $z \in \mathcal{F}_0$ of E_{q^k-1} that satisfies $|z - z_0| < 1$, and these are all the zeroes of E_{q^k-1} in $\mathcal{F}$.* $\square$

Note that the above also gives an independent proof of the simplicity of zeroes of special Eisenstein series.

8.6 Corollary. *Let $z \in \mathcal{F}_0$ have* $\mathrm{red}(z) = z_0 \in \overline{\mathbb{F}}_q - \mathbb{F}_q$. *Then*

$$\begin{aligned} |g_k(z)| &= 1, \quad \text{if } z_0 \notin \mathbb{F}_{q^{k+1}} \\ &< 1, \quad \text{if } z_0 \in \mathbb{F}_{q^{k+1}}. \end{aligned}$$

Proof. The constant comparing E_{q^k-1} and $g_k = (-1)^{k+1}\overline{\pi}^{1-q^k}L_k \cdot E_{q^k-1}$ has absolute value 1. The result now follows from $|E_{q^k-1}(z)| \leq 1$ and $|E_{q^k-1}(z)| < 1$ $\Leftrightarrow \tilde{E}_{q^k-1}(z_0) = 0$. $\square$

8.7 Corollary. *In the same situation,*

$$\begin{aligned} |j(z)| &= q^q, \quad \text{if } z_0 \notin \mathbb{F}_{q^2} \\ &< q^q, \quad \text{if } z_0 \in \mathbb{F}_{q^2}. \end{aligned}$$

Proof. This follows from $j = \frac{g^{q+1}}{\Delta}$ and $|\Delta| = q^{-q}$ uniformly on $\mathcal{F}_0$ ([8] 2.13, where the equivalent formula $\log_q |\Delta_{\mathrm{old}}| = q^2$ is given). $\square$

For the convenience of the reader, we give a list with the logarithms of absolute values of the relevant functions on $\mathcal{F}_0$.

8.8. Table

f	$\log_q \lvert f\rvert$ on $\mathcal{F}_0$	$\log_q \lvert f(z)\rvert$ depending on $z_0 = \mathrm{red}(z)$
$\overline{\pi}$	$\frac{q}{q-1}$	
$t = \overline{\pi}^{-1} e_A^{-1}, h$	$-\frac{q}{q-1}$	
$e_A^{-1}, \tilde{t}$	0	
E_k	≤ 0	< 0 iff $\tilde{E}_k(z_0) = 0$
$g_k, E_{q^k-1}, \tilde{E}_{q^k-1}$	≤ 0	< 0 iff $z_0 \in \mathbb{F}_{q^{k+1}}$
Δ	$-q$	
Δ_{old}	q^2	
g	≤ 0	< 0 iff $z_0 \in \mathbb{F}_{q^2}$
j	$\leq q$	$< q$ iff $z_0 \in \mathbb{F}_{q^2}$

8.9 Proposition. *Let $\tilde{z}$ be the coordinate on $\mathbb{P}^1/\mathbb{F}_q$, and consider $\tilde{t} = \sum_{a\in\mathbb{F}_q} \frac{1}{\tilde{z}-a}$ $= \frac{1}{\tilde{z}-\tilde{z}^q}$ and $\tilde{j} := \frac{(1+\tilde{t}^{q-1})^{q+1}}{\tilde{t}^{q-1}}$ as rational functions on $\mathbb{P}^1$. Then $\tilde{j}$ is invariant under the action of $\Gamma_0 = \mathrm{GL}(2,\mathbb{F}_q)$ on $\mathbb{P}^1$ and identifies the quotient $\Gamma_0 \setminus \mathbb{P}^1$ with $\mathbb{P}^1$.*

Proof. It is immediate that $\tilde{j}$ is invariant under matrices of the form $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$ since $\tilde{t}(a\tilde{z}) = a^{-1}\tilde{t}(\tilde{z})$. A small calculation gives the invariance under $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, hence $\tilde{j}$ is invariant under Γ_0, which is generated by matrices of that shape. As a function in $\tilde{z}$, $\tilde{j}$ has degree $q^3 - q = \#\mathrm{PGL}(2,\mathbb{F}_q)$, thus $\mathbb{F}_q(\tilde{j})$ is the fixed field of Γ_0 in $\mathbb{F}_q(\tilde{z})$. Therefore, $\tilde{j}$ defines a birational morphism from $\Gamma_0 \setminus \mathbb{P}^1$ to $\mathbb{P}^1$, which is an isomorphism since the target $\mathbb{P}^1$ is normal. $\square$

8.10 Theorem. *Let z, w be zeroes of g_k in $\mathcal{F}_0$, $z_0 = \mathrm{red}(z)$, $w_0 = \mathrm{red}(w)$. Then*

$$\begin{aligned} |j(z) - j(w)| &= 0, \quad \text{if } z_0, w_0 \text{ are equivalent under } \Gamma_0 = \mathrm{GL}(2,\mathbb{F}_q) \\ &= q^q \quad \text{otherwise.} \end{aligned}$$

Proof. In the first case, also z and w are Γ_0-equivalent by Theorem 8.5, whence $j(z) = j(w)$.
For the second case, we take a closer look on the behavior of j on $\mathcal{F}_0$. We have $j = \frac{g^{q+1}}{\Delta}$, where $\Delta = -t^{q-1} \prod_{a\in A \text{ monic}} f_a(t)^{(q^2-1)(q-1)}$. Now the infinite product $P(z) = \prod \cdots$ converges and satisfies $|P(z)-1| < 1$ on $\mathcal{F}_0$, as follows from (3.12) and (4.5). Hence on $\mathcal{F}_0$, the following congruences mod $\mathfrak{m}_C$ hold:

$$\begin{aligned} \overline{\pi}^{q-1}\Delta(z) &= e_A^{1-q}(z)P(z) \equiv e_{\mathbb{F}_q}(z)^{1-q} = \tilde{t}(z)^{q-1}, \\ g &= \overline{\pi}^{1-q}[1]E_{q-1}(z) \equiv E_{q-1}(z) \quad (\text{since } \overline{\pi}^{1-q}[1] \text{ is a 1-unit}) \\ &\equiv \tilde{E}_{q-1}(z) = -(1+\tilde{t}(z)^{q-1}) \quad \text{by (8.3), and further} \\ \overline{\pi}^{1-q}j(z) &\equiv (1+\tilde{t}(z)^{q-1})^{q+1}\tilde{t}(z)^{1-q} \equiv (1+\tilde{t}(z_0)^{q-1})^{q+1}\tilde{t}(z_0)^{1-q} = \tilde{j}(z_0). \end{aligned}$$

We see from (8.9) that Γ_0-inequivalent points z_0, w_0 give rise to different $\tilde{j}(z_0) \neq$

$\tilde{j}(w_0)$. Thus finally $|\overline{\pi}^{1-q}j(z) - \overline{\pi}^{1-q}j(w)| = 1$ and $|j(z) - j(w)| = |\overline{\pi}^{q-1}| = q^q$. $\square$

8.11 Corollary. *The inequality of Proposition* 7.12 *is in fact an equality, i.e.,* $|\mathrm{disc}(\varphi_k)| = |\mathcal{D}_k|$.

Proof. Immediate from (8.10) and the proof of (7.12). $\square$

8.12 Theorem. *Let L_k/K be the splitting field of φ_k, that is, the field extension generated by the j-zeroes of g_k. Then $L_k \cdot K_\infty$ is the unramified extension of K_∞ of degree $k+1, 2, 1$ if $k \geq 4$, $k = 3$, $k = 1, 2$, respectively.*

Proof. The assertion is trivial if $k = 1, 2$, thus suppose $k \geq 3$. We have $L_k \cdot K_\infty = K_\infty(j(z) \mid E_{q^k-1}(z) = 0)$. Let $z_0 \in \mathbb{F}_{q^{k+1}} - \mathbb{F}_q$ and $K_\infty^{(k+1)} = K_\infty(w_0 \mid w_0 \in \mathbb{F}_{q^{k+1}})$ be the unramified extension of degree $k+1$. The expansion of E_{q^k-1} around z_0 has coefficients in $K_\infty^{(k+1)}$, as follows from developing

$$\frac{1}{(az+b)^{q^k-1}} = \left[\frac{1}{(az_0+b)(1+\frac{a(z-z_0)}{az_0+b})}\right]^{q^k-1}$$ into a geometric series in $z - z_0$

and rearranging terms. Hence the zero z of E_{q^k-1} close to z_0 actually lies in $K_\infty^{(k+1)}$. For the same reason, $t(z)^{q-1} = \overline{\pi}^{1-q}e_A(z)^{1-q}$ and $j(z) =$ convergent Laurent series in $t(z)^{q-1}$ with coefficients in $A \subset K_\infty$ lie in $K_\infty^{(k+1)}$. In view of $\overline{\pi}^{1-q}j(z) \equiv \tilde{j}(z)$ (see (8.9)), it now suffices to show:

$k \geq 4$: The field extension $\mathbb{F}_q(S)$ generated over $\mathbb{F}_q$ by the value set $S = \tilde{j}(\mathbb{F}_{q^{k+1}} - \mathbb{F}_q)$ of $\tilde{j} : \mathbb{F}_{q^{k+1}} - \mathbb{F}_q \longrightarrow \mathbb{F}_{q^{k+1}}$ equals $\mathbb{F}_{q^{k+1}}$;

$k = 3$: $\varphi_3(X) = X^q - [1]X^{q-1} - [2]$ has $K_\infty^{(2)}$ as its splitting field.

Now $\tilde{j}$, being of degree $q^3 - q$, has image S of cardinality $\#(S) \geq \frac{q^{k+1}-q}{q^3-q} > q^{k-2}$. For $k > 4$, $\#(S)^2 > \#\mathbb{F}_{q^{k+1}}$, hence $\mathbb{F}_q(S) = \mathbb{F}_{q^{k+1}}$, and this also holds for $k = 4$ since $k+1 = 5$ is prime. If $k = 3$,

$$-T^{-q^2}X^q\varphi_3(\frac{T^q}{X}) = (1 - T^{1-q^2})X^q + (1 - T^{1-q})X - 1 \equiv X^q + X - 1 =: \eta(X)$$

has the same splitting field as $\varphi_3(X)$. But $\eta(X) = \prod(X - e)$, where e runs through the elements of $\mathbb{F}_{q^2}$ with trace 1. Its splitting field over $\mathbb{F}_q$ therefore equals $\mathbb{F}_{q^2}$, which gives $K_\infty^{(2)}$ for the splitting field of φ_3 over K_∞. $\square$

The present result, together with (8.11) and Theorem 7.14 strongly suggests that in fact $\mathrm{disc}(\varphi_k) = \mathcal{D}_k$, possibly up to a constant in $\mathbb{F}_q^*$. We cannot resist here to present the following table, suitable to catalyse some meditation. It contains the numerators of the discriminants of the polynomials φ_p (see (7.10)) in the range $29 \leq p \leq 79$, i.e., those $p \neq 83$ where $2 \leq \deg\ \varphi_p \leq 6$.

Note that, in contrast with our $\varphi_k \in A[X]$, $\varphi_p \in \mathbb{Q}[X]$, and denominators actually occur. So its discriminant is in general not an integer. The numbers

c_k are k-digit integers without small prime factors, which we didn't attempt to further factorize.

8.13 Table (G. Cornelissen/MAPLE).

p	deg φ_p	num(disc(φ_p))
29	2	$2^{14} \cdot 3^9 \cdot 5^5 \cdot 7^3 \cdot 13^2 \cdot 281827873$
31	2	$2^{21} \cdot 3^9 \cdot 5^5 \cdot 7^4 \cdot 13^2 \cdot 39468318601$
37	3	$2^{46} \cdot 3^{30} \cdot 5^{15} \cdot 7^{12} \cdot 11^2 \cdot 13^6 \cdot 17^2 \cdot 19^2 \cdot c_{13} \cdot c_{21}$
41	3	$2^{47} \cdot 3^{25} \cdot 5^{19} \cdot 7^9 \cdot 11^4 \cdot 13^6 \cdot 17^2 \cdot 19^2 \cdot 2137 \cdot c_{34}$
43	3	$2^{48} \cdot 3^{24} \cdot 5^{15} \cdot 7^{14} \cdot 13^6 \cdot 17^2 \cdot 19^2 \cdot 97 \cdot 223 \cdot c_{15} \cdot c_{23}$
47	3	$2^{48} \cdot 3^{27} \cdot 5^{15} \cdot 7^9 \cdot 11^2 \cdot 13^6 \cdot 17^2 \cdot 19^2 \cdot c_{48}$
53	4	$2^{92} \cdot 3^{53} \cdot 5^{30} \cdot 7^{21} \cdot 11^4 \cdot 13^9 \cdot 17^6 \cdot 19^2 \cdot 23^2 \cdot 67 \cdot 73$
		$\cdot 127 \cdot 1481 \cdot c_{81}$
59	4	$2^{107} \cdot 3^{51} \cdot 5^{31} \cdot 7^{21} \cdot 11^6 \cdot 13^{12} \cdot 17^6 \cdot 19^6 \cdot 23^2 \cdot c_{102}$
61	5	$2^{156} \cdot 3^{86} \cdot 5^{55} \cdot 7^{35} \cdot 11^{18} \cdot 13^{20} \cdot 17^6 \cdot 19^9 \cdot 23^2 \cdot 29^4 \cdot 31^4$
		$\cdot 3037 \cdot c_{160}$
67	5	$2^{160} \cdot 3^{85} \cdot 5^{51} \cdot 7^{35} \cdot 11^{13} \cdot 13^{20} \cdot 17^6 \cdot 19^6 \cdot 23^6 \cdot 29^4 \cdot 31^4$
		$\cdot 79 \cdot 1987 \cdot 21467 \cdot c_{175}$
71	5	$2^{160} \cdot 3^{86} \cdot 5^{51} \cdot 7^{33} \cdot 11^{19} \cdot 13^{20} \cdot 17^{12} \cdot 19^6 \cdot 23^6 \cdot 29^4 \cdot 31^4$
		$\cdot 127 \cdot 313 \cdot 6311 \cdot 29837 \cdot c_{180}$
73	6	$2^{242} \cdot 3^{136} \cdot 5^{70} \cdot 7^{53} \cdot 11^{18} \cdot 13^{30} \cdot 17^{15} \cdot 19^{16} \cdot 23^8 \cdot 29^4 \cdot 31^6$
		$\cdot 37^6 \cdot 1867 \cdot c_{272}$
79	6	$2^{240} \cdot 3^{129} \cdot 5^{77} \cdot 7^{53} \cdot 11^{22} \cdot 13^{25} \cdot 17^{14} \cdot 19^{14} \cdot 23^6 \cdot 29^4 \cdot 31^4$
		$\cdot 37^6 \cdot 53 \cdot 3319 \cdot c_{283}$

The reader will observe that all the primes $l \leq \frac{p-1}{2}$ (with the possible exception of $l = 11$) occur to a high power in num(disc(φ_p)), which is a weak analogy of the behavior of disc(φ_k) $\in A$. However, we can neither prove this fact (?), nor do we understand the larger prime divisors l that appear.

Some of the results about zeroes of g_k have analogues for h_k resp. ∂E_{q^k-1}.

8.14 Theorem. *For each $z_0 \in \mathbb{F}_{q^k} - \mathbb{F}_q$, there exists a unique zero $z \in \mathcal{F}_0$ of h_k that satisfies $|z - z_0| < 1$, these are all the zeroes of h_k in $\mathcal{F}$, and they have multiplicity q.*

Proof. We start with two simple estimates.

Let $z \in \mathcal{F}_0$, $a, b \in A$. Then

(i) deg $a > 0 \Rightarrow |\overline{\pi} at(az)| < 1$

(ii) $\max\{\deg\ a, \deg\ b\} > 0 \Rightarrow \left|\frac{a}{(az+b)^{q^k}}\right| < 1$.

The second of these is trivial, and the first follows from (4.5).

For $z \in \mathcal{F}_0$,

$$\begin{aligned}\overline{\pi}\partial E_{q^k-1}(z) &= \tfrac{d}{dz}\sum_{a,b\in A}{}'\frac{1}{(az+b)^{q^k-1}} - \overline{\pi}E\sum_{a,b\in A}{}'\frac{1}{(az+b)^{q^k-1}}\\ &= \sum_{a,b}{}'\frac{a}{(az+b)^{q^k}} - \overline{\pi}\sum_{a\in A \text{ monic}} at(az)\sum_{a,b}{}'\frac{1}{(az+b)^{q^k-1}},\end{aligned}$$

which has absolute value ≤ 1. Modulo $\mathfrak{m}_C$,

$$\begin{aligned}\overline{\pi}\sum_{a \text{ monic}} at(az) &\equiv \overline{\pi}t(z) \quad \text{by (8.15) (i))}\\ &= e_A^{-1}(z) = \sum_{a\in A}\frac{1}{z-a} \equiv \sum_{a\in\mathbb{F}_q}\frac{1}{z-a} = \tilde{t}(z),\end{aligned}$$

and in the double sums $\displaystyle\sum_{a,b}{}'$, only terms with $(a,b)\in\mathbb{F}_q\times\mathbb{F}_q$ contribute to the congruence. Hence

$$\begin{aligned}\overline{\pi}\partial E_{q^k-1}(z) &\equiv \sum_{a,b\in\mathbb{F}_q}{}'\frac{a}{(az+b)^{q^k}} - \tilde{t}(z)\tilde{E}_{q^k-1}(z)\\ &= \sum_{a\in\mathbb{F}_q}{}'a\tilde{t}(az)^{q^k} - \tilde{t}(z)\tilde{E}_{q^k-1}(z).\end{aligned}$$

Now $\tilde{t}(az) = a^{-1}\tilde{t}(z)$, hence by the formula for G_{q^k-1} given in (8.3), the above equals

$$\begin{aligned}-\tilde{t}(z)^{q^k} - \tilde{t}(z)\left[-1-\sum_{0\leq i<k}\tilde{t}(z)^{q^k-q^i}\right] &= \sum_{0<i\leq k}\tilde{t}(z)^{q^k-q^i+1}\\ \equiv \sum_{0<i\leq k}\tilde{t}(z_0)^{q^k-q^i+1}, &\quad \text{if } z_0 = \mathrm{red}(z)\in\mathbb{F}_q.\end{aligned}$$

Suppose that $h_k(z) = 0 = \overline{\pi}\partial E_{q^k-1}(z)$. Then

$$0 = \sum_{0<i\leq k}\tilde{t}(z_0)^{-q^i} = \sum_{0<i\leq k} e_{\mathbb{F}_q}(z_0)^{q^i} = z_0^q - z_0^{q^{k+1}}, \text{ i.e., } z_0\in\mathcal{F}_{q^k}.$$

On the other hand, $\mathrm{red}(z) = z_0 \in \mathbb{F}_{q^k}$ implies that $|\overline{\pi}\partial E_{q^k-1}(z_0)| < 1$, from which we will derive the existence of a q-fold zero z with $z\equiv z_0$. Since $|\tilde{t}| = 1$ on $\mathcal{F}_0$,

$$\tilde{t}^{-1}\overline{\pi}\partial E_{q^k-1} \equiv \sum_{0<i\leq k}\tilde{t}^{q^k-q^i} = {}_2\tilde{h}_k^q,$$

where ${}_2\tilde{h}_k := \displaystyle\sum_{0\leq i<k}\tilde{t}^{q^{k-1}-q^i}$ has zeroes at $z = z_0 \in \mathbb{F}_{q^k} - \mathbb{F}_q$, in fact, simple zeroes, as follows from the proof of (8.4). Up to a suitable scaling, ${}_2\tilde{h}_k$ is the

reduction of the function ${}_2h_k$ of (7.16). Hence the simple zeroes of ${}_2\tilde{h}_k$ may be uniquely lifted to simple zeroes of ${}_2h_k$ in $\mathcal{F}_0$, i.e., to zeroes of multiplicity q of $h_k = \text{const.}\ \partial E_{q^k-1}$. This finishes the proof. $\square$.

Using similar methods, we get the following analogues of results (8.6), (8.10) and (8.12) for the zeroes of h_k. We leave details to the reader.

(8.15) For $z \in \mathcal{F}_0$ with $\mathrm{red}(z) = z_0 \in \overline{\mathbb{F}}_q - \mathbb{F}_q$,

$$\begin{array}{rcll} |h_k(z)| & = & 1, & \text{if } z_0 \notin \mathbb{F}_{q^k} \\ & < & 1, & \text{if } z_0 \in \mathbb{F}_{q^k}. \end{array}$$

(8.16) Let z, w be zeroes of h_k in $\mathcal{F}_0$ with reductions z_0, w_0. Then

$$\begin{array}{rcll} |j(z) - j(w)| & = & 0, & \text{if } z_0, w_0 \text{ are equivalent under } \Gamma_0 = \mathrm{GL}(2, \mathbb{F}_q) \\ & = & q^q & \text{otherwise.} \end{array}$$

(8.17) Let M_k/K be the splitting field of ψ_k. Then $M_k \cdot K_\infty$ is the unramified extension of degree k of $K_\infty(T^{q^{-1}})$ if $k \geq 5$, of degree 2 if $k = 4$, it equals $K_\infty(T^{q^{-1}})$ if $k = 3$, and K_∞ if $k = 1, 2$.

8.18 Remark. As is apparent from the preceding, the functions $\tilde{t}$, $\tilde{E}_k$, $\tilde{j}$ etc., as rational functions of $\Omega/\mathbb{F}_q := \overline{\mathbb{F}}_q - \mathbb{F} \hookrightarrow \mathbb{P}^1(\overline{\mathbb{F}}_q)$, may be regarded as the reductions (up to scaling) of the functions t, E_k, j, ... on Ω. They are modular with respect to the action of Γ_0 on $\Omega/\mathbb{F}_q$. Proposition (8.3) describes the $\tilde{t}$-expansion of the Eisenstein series $\tilde{E}_k$, and (8.9) gives the modular uniformization of $\Gamma_0 \setminus (\Omega/\mathbb{F}_q)$. In fact, an important part of our present results on Drinfeld modular forms evolves from the investigation of functions on the "finite upper half-plane" $\Omega/\mathbb{F}_q$. Hence the theory of such "finite modular forms" is at least not empty. A systematic study of them will be given elsewhere.

References

[1] G. Cornelissen: Geometric properties of modular forms over rational function fields. Thesis. Gent 1997.

[2] G. Cornelissen: The field of definition of the divisor of Eisenstein series for $\mathbb{F}_q(T)$, in preparation.

[3] V.G. Drinfeld: Elliptic modules (russian), Math. Sbornik **94** (1974), 594-627; english translation: Math. USSR-Sbornik **23** (1976), 561-592.

[4] E.-U. Gekeler: A product expansion for the discriminant function of Drinfeld modules of rank two, J. Numb. Th. **21** (1985), 135-140.

[5] E.-U. Gekeler: Drinfeld modular curves, Lect. Notes Math. **1231**, Springer 1986.

[6] E.-U. Gekeler: On the coefficients of Drinfeld modular forms, Invent. Math. **93** (1988), 667-700.

[7] E.-U. Gekeler: On finite Drinfeld modules, J. Alg. **141** (1991), 187-203.

[8] E.-U. Gekeler: On the Drinfeld discriminant function, Comp. Math. **106** (1997), 181-202.

[9] E.-U. Gekeler, M. Reversat: Jacobians of Drinfeld modular curves. J. reine angew. Math. **476** (1996), 27-93.

[10] E.-U. Gekeler, M. van der Put, M. Reversat, J. van Geel (eds.): Drinfeld modules, modular schemes and applications, World Scientific 1997.

[11] L. Gerritzen, M. van der Put: Schottky groups and Mumford curves, Lect. Notes Math. **817**, Springer 1980.

[12] D. Goss: Von Staudt for $\mathbb{F}_q[T]$, Duke Math. J. **45** (1978), 885-910.

[13] D. Goss: π-adic Eisenstein series for function fields, Comp. Math. **41** (1980), 3-38.

[14] D. Goss: The algebraist's upper half-plane, Bull. AMS NS 2 (1980), 391-415.

[15] D. Goss: Basic structures of function field arithmetic, Ergeb. d. Math. **35**, Springer 1996.

[16] F.K.C. Rankin, H.P.F. Swinnerton-Dyer: On the zeroes of Eisenstein series, Bull. London Math. Soc **2** (1970), 169-170.

[17] J-P. Serre: Cours d'arithmétique, PUF, Paris 1970.

Ernst-Ulrich Gekeler
Fachbereich 9 Mathematik
Universität des Saarlandes
66041 Saarbrücken
Germany

gekeler@math.uni-sb.de

This page intentionally left blank

http://dx.doi.org/10.1090/conm/224/03187

Contemporary Mathematics
Volume 224, 1999

Counting jump optimal linear extensions of some posets

Hyung Chan Jung

1. Introduction

Let P be a finite poset and let $|P|$ be the *number of vertices* in P. A *subposet* of P is a subset of P with the induced order. A *chain* C in P is a subposet of P which is a linear order. The *length* of the chain C is $|C| - 1$. A poset is *ranked* if every maximal chain has the same length. A *linear extension* of a poset P is a linear order $L = x_1, x_2, \ldots, x_n$ of the elements of P such that $x_i < x_j$ in P implies $i < j$. Let $\mathcal{L}(P)$ be the set of all linear extensions of P. Szpilrajn [**13**] showed that $\mathcal{L}(P)$ is not empty.

Let P, Q be two disjoint posets. The *disjoint sum* $P + Q$ of P and Q is the poset on $P \cup Q$ such that $x < y$ if and only if $x, y \in P$ and $x < y$ in P or $x, y \in Q$ and $x < y$ in Q. The *linear sum* $P \oplus Q$ of P and Q is obtained from $P + Q$ by adding the relation $x < y$ for all $x \in P$ and $y \in Q$.

Throughout this section, L denotes an arbitrary linear extension of P. Let $a, b \in P$ with $a < b$. Then b *covers* a, denoted $a \prec b$, provided that for any $c \in P$, $a < c \leq b$ implies that $c = b$. A (P, L)-*chain* is a maximal sequence of elements $z_1, z_2, \ldots, z_k$ such that $z_1 \prec z_2 \prec \cdots \prec z_k$ in both L and P. Let $c(L)$ be the number of (P, L)-chains in L.

A consecutive pair (x_i, x_{i+1}) of elements in L is a *jump* (or *setup*) of P in L if x_i is not comparable to x_{i+1} in P. The jumps induce a decomposition $L = C_1 \oplus \cdots \oplus C_m$ of L into (P, L)-chains $C_1, \ldots, C_m$ where $m = c(L)$ and $(\max C_i, \min C_{i+1})$ is a jump of P in L for $i = 1, \ldots, m - 1$. Let $s(L, P)$ be the number of jumps of P in L and let $s(P)$ be the minimum of $s(L, P)$ over all linear extensions L of P. The number $s(P)$ is called the *jump number* of P. If $s(L, P) = s(P)$ then L is called a *(jump) optimal linear extension* of P. We denote the set of all optimal linear extensions of P by $\mathcal{O}(P)$. The *width* $\omega(P)$ of P is the maximal number of elements of an *antichain* (mutually incomparable elements) of P. Chein and Habib [**2**] introduced several aspects of jump number. Dilworth [**3**] showed that $\omega(P)$ equals the minimum number of chains in a partition of P into chains. Since for any linear extension L of P the number of (P, L)-chains is at least as large as the minimum number of chains in a chain partition of P, it follows from Dilworth's

1991 *Mathematics Subject Classification.* Primary 06A07; Secondary 05A15.

Research partially supported by KOSEF-RCAA and partially by Korean Ministry of Education through Research Fund grant BSRI-97-1438.

theorem that

$$s(P) \geq \omega(P) - 1. \tag{1}$$

If equality holds in (1), then P is called a *Dilworth poset* or simply a *D-poset.* More discussion about D-posets is given in [**12**].

A poset P is *cover N-free* if P does not contain *cover* $N = \{x_1 < y_1, x_2 \prec y_1, x_2 < y_2\}$ as a subposet. A *cycle (on 2n elements)* is a partially ordered set $\{a_{2n} > a_n, a_{2n} > a_1, a_{n+i} > a_i, a_{n+i} > a_{i+1}$ for $i = 1, \ldots, n-1\}$. A poset P is cycle-free if P does not contain cycle as a subposet. Proposition 1.1 and Lemma 1.2 give properties of cycle-free posets and *cover N-free* posets.

PROPOSITION 1.1 (DUFFUS, RIVAL AND WINKLER [**4**]). *If P is cycle-free, then*

$$s(P) = \omega(P) - 1.$$

LEMMA 1.2 (EL-ZAHAR AND RIVAL [**6**]). *If P is cover N-free, then for any antichain $\{a_1, \ldots, a_n\}$ in P there is $L \in \mathcal{O}(P)$ such that $a_1 < \cdots < a_n$ in L.*

In this paper, we will count the number of optimal linear extensions of some finite posets. It is clear that $|\mathcal{O}(P)| \leq |\mathcal{L}(P)|$.

2. Direct Counting

By direct counting, Jung [**8**] counted optimal linear extensions of some basic posets :

A k-chain $\underline{k}$ is a chain of length $k-1$. We get easily $s(\underline{a_1} + \cdots + \underline{a_n}) = n - 1$ and

$$|\mathcal{O}(\underline{a_1} + \cdots + \underline{a_n})| = n!.$$

Let $I_m = 1 + \cdots + 1$ (m times). We define a *complete multipartite poset* to be a poset $M(m_1, \ldots, m_n) = I_{m_1} \oplus \cdots \oplus I_{m_n}$. Then we get $(M(m_1, \ldots, m_n)) = m_1 + \cdots + m_n - n$ and

$$|\mathcal{O}(M(m_1, \ldots, m_n))| = m_1! m_2! \cdots m_n!. \tag{2}$$

Especially, $K_{m,n} = M(m,n)$ is called a *complete bipartite poset.* Then from (2), we get

$$|\mathcal{O}(K_{m,n})| = m!n!.$$

An *upward* [*downward*] *rooted tree* T_u [T_d] is a poset whose diagram is an upward [downward] rooted tree. Let $T = T_u$ or T_d. Then we get $s(T) = \omega(T) - 1$ and

$$|\mathcal{O}(T)| = \omega(T)!. \tag{3}$$

A *fence* (or *zigzag*) on n elements is a poset $F_n = \{a_1 < a_2, a_2 > a_3, \ldots\}$. We get $s(F_n) = \lceil \frac{n}{2} \rceil - 1$ and

$$|\mathcal{O}(F_n)| = \begin{cases} 1, & \text{if } n = 1 \text{ or even} \\ 2^{(n-1)/2}, & \text{otherwise.} \end{cases}$$

For intergers n, k with $n \geq 0$ and $k \geq 0$, the *general crown* S_n^k is the poset of unit length with $n+k$ minimal elements $x_1, \ldots, x_{n+k}$ and $n+k$ maximal elements

$y_1, \dots, y_{n+k}$. The order on S_n^k is defined by $x_i < y_j$ iff $j \notin \{i, i+1, \dots, i+k\}$, where addition is modulo $n+k$. Then we get $s(S_n^k) = 2n+k-3$ and

$$|\mathcal{O}(S_n^k)| = 2^k(n+k)\{(n-1)!\}^2. \tag{4}$$

A *standard poset on n elements* S_n is defined to be S_n^0. From (4), we get

$$|\mathcal{O}(S_n)| = n!(n-1)!.$$

Let $N = \{x_1 < y_1, x_2 < y_1, x_2 < y_2\}$ be a poset. The linear orders $L_1 = x_1x_2y_1y_2$, $L_2 = x_1x_2y_2y_1$, $L_3 = x_2x_1y_1y_2$, $L_4 = x_2x_1y_2y_1$, $L_5 = x_2y_2x_1y_1$ are all the possible linear extensions of N. Thus $|\mathcal{L}(N)|$=5. Also, $s(N)$=1 and only L_5 is the optimal linear extension of N, that is,

$$|\mathcal{O}(N)| = 1. \tag{5}$$

Let C_{2n} be a cycle on $2n$ elements. By direct counting, we get $|\mathcal{O}(C_{2n})| = n \cdot 2^{n-1}$.

El-Zahar and Rival [**5**] shows that $s(P_1+P_2) = s(P_1)+s(P_2)+1$ and $s(P_1 \oplus P_2) = s(P_1) + s(P_2)$ for finite posets P_1, P_2. This motivates the following theorem:

THEOREM 2.1. *Let P_1, P_2 be finite posets. Then*
(a) $|\mathcal{O}(P_1+P_2)| = \frac{(s(P_1)+s(P_2)+2)!}{(s(P_1)+1)!s(s(P_2)+1)!}|\mathcal{O}(P_1)| \cdot |\mathcal{O}(P_2)|$,
(b) $|\mathcal{O}(P_1 \oplus P_2)| = |\mathcal{O}(P_1)| \cdot |\mathcal{O}(P_2)|$.

PROOF. (*a*) Let $L_1 \in \mathcal{O}(P_1)$ and $L_2 \in \mathcal{O}(P_2)$. Then $c(L_1) = s(P_1)+1$ and $c(L_2) = s(P_2)+1$. Let L be a linear sums of (P_1, L_1)-chains and (P_2, L_2)-chains such that $L[P_1] = L_1$ and $L[P_2] = L_2$. Then $L \in \mathcal{O}(P_1+P_2)$. All the possible number of the above L is

$$\binom{c(L_1)+c(L_2)}{c(L_1)} = \binom{s(P_1)+s(P_2)+2}{s(P_1)+1}.$$

This holds for every $L_1 \in \mathcal{O}(P_1)$ and for every $L_2 \in \mathcal{O}(P_2)$. Thus

$$|\mathcal{O}(P_1+P_2)| \geq \binom{s(P_1)+s(P_2)+2}{s(P_1)+1}|\mathcal{O}(P_1)| \cdot |\mathcal{O}(P_2)|.$$

On the other hand, if $L \in \mathcal{O}(P_1+P_2)$ then $L[P_1] \in \mathcal{O}(P_1)$ and $L[P_2] \in \mathcal{O}(P_2)$. Thus L is a linear sums of $(P_1, L[P_1])$-chains and $(P_2, L[P_2])$-chains. This completes the proof of (*a*).
(*b*) Let $L_i \in \mathcal{O}(P_i)$ for $i = 1, 2$. Since $L_1 \oplus L_2 \in \mathcal{O}(P_1 \oplus P_2)$, we get $|\mathcal{O}(P_1 \oplus P_2)| \geq |\mathcal{O}(P_1)| \cdot |\mathcal{O}(P_2)|$. For any $L \in \mathcal{O}(P_1 \oplus P_2)$, every elements of P_1 precedes every elements of P_2. Also, $L[P_i] \in \mathcal{O}(P_i)$ for $i = 1, 2$. Thus $L = L[P_1] \oplus L[P_2]$, and so $|\mathcal{O}(P_1 \oplus P_2)| \leq |\mathcal{O}(P_1)| \cdot |\mathcal{O}(P_2)|$. This proves (*b*).

Let $V = \{y_1 > x_1, y_2 > x_1\}$. Then $|\mathcal{O}(V)| = 2$ and we get $|\mathcal{O}(N)| = 1$ from (5), and we get $|\mathcal{O}(V+N)| = 12$ by Theorem 2.1 (a). Also, by applying Theorem 2.1, we get (2).

A poset P is called *series parallel* if it can be constructed from singletons using the operations of disjoint sum (+) and linear sum ($\oplus$). By Theorem 2.1, we can easily count the number of optimal linear extensions of any series parallel posets.

Note the difference between N and cover N. Rival[10] showed that *a finite poset is series parallel if and only if it contains no subset isomorphic to N.*

Thus if a finite poset P contains no subset isomorphic to N then we can count the number of optimal linear extensions of P.

For example, let $P_0 = 1 \oplus ((1 \oplus (1+1)) + (1 \oplus (1+1+1)))$. Then we can get $|\mathcal{O}(P_0)| = 120$ by Theorem 2.1.

3. Structure Counting

Let P be a poset, and Q be a subposet of P. For any $L \in \mathcal{L}(P)$ we let $L[Q]$ be a subposet of L which is also a linear extension of Q.

THEOREM 3.1. *If P is cycle-free, then*

$$|\mathcal{O}(P)| \leq \omega(P)!. \tag{6}$$

Moreover, equality holds in (6) if P is cycle-free and cover N-free.

PROOF. Let $n = \omega(P)$, and $A = \{x_1, \ldots, x_n\}$ be a maximum size antichain. Assume that the following (7) is true:

(7) if P is cycle-free and $L_1 \neq L_2$ where $L_1, L_2 \in \mathcal{O}(P)$ then $L_1[A] \neq L_2[A]$.

Then $|\mathcal{O}(P)| = |\{L[A] : L \in \mathcal{O}(P)\}| \leq |A|! = n!$ and we get (6).
To prove (7) we will show that if $L_1[A] = L_2[A]$ then $L_1 = L_2$.
Suppose $L_1 \neq L_2$. Choose the first different elements $y_1 \in L_1$ and $y_2 \in L_2$. Since y_1, y_2 are the first different elements, $y_1 < y_2$ in L_1 and $y_2 < y_1$ in L_2. So y_1 and y_2 are incomparable in P. Now choose a (P, L_1)-chain C_i^1 which contains y_1, and a (P, L_2)-chain C_j^2 which contains y_2. Since P is cycle-free, $c(L) = \omega(P)$ for any $L \in \mathcal{O}(P)$ by Proposition 1.1, and so any (P, L)-chain contains exactly one x_i for some i. Thus we can choose $x_i \in C_i^1$ and $x_j \in C_j^2$. Now since $L_1[A] = L_2[A]$, we get $x_i = x_j$, and so $i = j$.
In P since y_1 and y_2 are incomparable either $y_1 < x_i$ and $y_2 < x_i$ or $y_1 > x_i$ and $y_2 > x_i$. If $y_1 < x_i$ and $y_2 < x_i$ hold, $y_2 < x_i$ implies that C_i^1 follows y_2 in L_1, and thus $y_2 < y_1$ in L_1, which is a contradiction. So $y_1 > x_i$ and $y_2 > x_i$ in P.
Now consider (P, L_1)-chains. Since $y_1 > x_i$ in C_i^1, there exists a (P, L_1)-chain $C_{l_1}^1$ which contains y_2 and x_{l_1}. But x_i and x_{l_1} are incomparable, thus $y_2 > x_{l_1}$. Since $y_2 > x_i$, C_i^1 precedes $C_{l_1}^1$ in L_1. Thus $x_i < x_{l_1}$ in $L_1[A]$. Similarly, consider (P, L_2)-chains. Since $y_2 > x_i$ in C_i^2, there exists a (P, L_2)-chain $C_{l_2}^2$ which contains y_1 and x_{l_2}. But x_i and x_{l_2} are incomparable, thus $y_1 > x_{l_2}$. Since $y_1 > x_i$, C_i^2 precedes $C_{l_2}^2$ in L_2. Thus $x_i < x_{l_2}$ in $L_2[A]$.
Since P is cycle-free, $l_1 \neq l_2$. Now $y_1 > x_{l_2}$ in P implies C_i^1 follows (P, L_1)-chain $C_{l_2}^1$ which contains x_{l_2} in L_1. Thus $x_{l_2} < x_i < x_{l_1}$ in $L_1[A]$. Also, $y_2 > x_{l_1}$ in P implies C_i^2 follows (P, L_2)-chain $C_{l_1}^2$ which contains x_{l_1} in L_2. So we get $x_{l_1} < x_i < x_{l_2}$ in $L_2[A]$. Hence $L_1[A] \neq L_2[A]$, which is a contradiction. Thus (7) holds, and (6) is proved.

Assume that P is *cover N-free* and cycle-free. Since P is *cover N-free*, by Lemma 1.2, for any $x_{i_1} \ldots x_{i_n}$ there is $L \in \mathcal{O}(P)$ such that $x_{i_1} < \ldots < x_{i_n}$ in L. Thus $|A|! \leq |\mathcal{O}(P)|$. Since P is also cycle-free, (6) holds. Hence $|\mathcal{O}(P)| = \omega(P)!$.

For $n \geq 5$, $|\mathcal{O}(C_{2n})| = n \cdot 2^{n-1} < n! = \omega(C_{2n})!$ Since C_{2n} is a cycle, this shows that the converse of Theorem 3.1 is false. A poset $K = \{x_1 < x_2 < x_3, y_1 <$

$y_2 < y_3, y_1 < x_2 < y_3, y_2 < x_3, y_1 < x_3, x_1 < y_3\}$ contains cycle and cover N. But $|\mathcal{O}(K)| = \omega(K)! = 2$ holds. This shows that Theorem 3.1 is the best possible result. By applying Theorem 3.1 we get (3) easily, and (5) is an example of inequality in (6).

Let $N_* = \{x_1 < y_1, x_2 < z < y_1, x_2 < y_2\}$ be a poset. Then since N_* contains N as a subset, it is not series parallel. Thus we cannot apply Theorem 2.1 to get $|\mathcal{O}(N_*)|$. But by Theorem 3.1, we get $|\mathcal{O}(N_*)| = 6$.

Let P, Q be two posets. The *direct product* $P \times Q$ of P and Q is the poset on $\{(p,q) : p \in P, q \in Q\}$ where $(a,b) \leq (c,d)$ if and only if $a \leq c$ in P and $b \leq d$ in Q. Let P^n be $P \times \cdots \times P$ (n times).

PROPOSITION 3.2. *Let P be a finite poset. Then every (P,L)-chain has length at most $k-1$ for all linear extension L of P if and only if $s(P \times \underline{k}) = |P| - 1$.*

PROOF. Suppose that every (P,L)-chain has length at most $k-1$ for all linear extension L of P. Let L_* be any optimal linear extension of $P \times \underline{k}$. Then any $(P \times \underline{k}, L_*)$-chain has length at most $k-1$. Otherwise, let C be a $(P \times \underline{k}, L_*)$-chain which has length at least k. Let $(p_2, l_2) = \max C$ and $(p_1, l_1) = \min C$. Then $p_2 \geq p_1$ and $l_2 \geq l_1$. If $p_2 = p_1$ or $l_2 = l_1$ then $|C| \leq k$, which contradicts the fact that the length of $|C|$ is at least k. Thus $p_2 > p_1$ and $l_2 > l_1$. Note that (p_1, l_2) and (p_2, l_1) are incomparable. So one of the (p_1, l_2) and (p_2, l_1) is not in C, say (p_1, l_2). In L_*, since $(p_1, l_1) < (p_1, l_2)$, C precedes (p_1, l_2), which contradicts $(p_1, l_2) < (p_2, l_2)$. Thus in L_*, since $(p_1, l_2) < (p_2, l_2)$, (p_1, l_2) precedes C, which also contradicts $(p_1, l_1) < (p_1, l_2)$. Hence every $(P \times \underline{k}, L_*)$-chain has length at most $k-1$. Now we get $s(P \times \underline{k}) \geq \frac{|P \times \underline{k}|}{|\underline{k}|} - 1 = |P| - 1$. Let $L^* = \oplus(\{p\} \times \underline{k} : p$ ordered as in some linear extension l of $P)$. Since $s(L^*, P \times \underline{k}) = |P| - 1$, $s(P \times \underline{k}) = |P| - 1$.

Conversely, suppose that $s(P \times \underline{k}) = |P| - 1$ holds. If there exists a linear extension L such that some (P,L)-chain C has length at least k, without loss of generality we may assume $L = C_1 \oplus \cdots \oplus C_{i-1} \oplus C \oplus C_{i+1} \oplus \cdots \oplus C_n$. Now construct a linear extension l_* as follows: $l_* = (\oplus(\{p\} \times \underline{k} :\ p$ ordered as in $C_1 \oplus \cdots \oplus C_{i-1}))\oplus(\oplus_{i=1}^{k}(C \times \{i\}) \oplus (\oplus(\{p\} \times \underline{k} :\ p$ ordered as in $C_{i+1} \oplus \cdots \oplus C_n))$. Since $s(l_*, P \times \underline{k}) < |P| - 1$, we get a contradiction. This completes the proof.

COROLLARY 3.3 (JUNG [**7**]). *Let the maximum size of a chain in a ranked poset P be at most k. Let $C(a) = \{(a,i) : i = 1, \ldots, k\}$ for all $a \in P$. Choose a linear extension L of P, and let $L_* = \oplus C(a)$ where $C(a)$ is arranged just like the order of a in L. Then L_* is an optimal linear extension of $P \times \underline{k}$, and $s(P \times \underline{k}) = |P| - 1$.*

We consider the poset $\underline{a_1} \times \cdots \times \underline{a_n}$ where $a_1, \ldots, a_n$ are positive integers. We assume that $a_i \geq 2$ for $i = 1, \ldots, n$ and let $a^* = \max\{a_1, \ldots, a_n\}$. Without loss of generality, we assume that $a^* = a_n$. Define $C(b_1, \ldots, b_{n-1}) = \{(b_1, \ldots, b_{n-1}, i) : 1 \leq i \leq a^*\}$. Then $C(b_1, \ldots, b_{n-1})$ is a chain of length $a^* - 1$ for any $b_1, \ldots, b_{n-1}$ where $1 \leq b_j \leq a_j$ for $j = 1, \ldots, n-1$.

COROLLARY 3.4 (JUNG [**7**]). *Let $L^* = \oplus C(b_1, \ldots, b_{n-1})$ where the $(b_1, \ldots, b_{n-1})$ are in lexicographic order. Then $L^* \in \mathcal{O}(\underline{a_1} \times \cdots \times \underline{a_n})$ and*

$$s(\underline{a_1} \times \cdots \times \underline{a_n}) = \left(\prod_{i=1}^{n} a_i\right)/a^* - 1.$$

PROPOSITION 3.5. *Let P be a finite poset. Then every (P, L)-chain has length less than $k-1$ for all linear extension L of P if and only if $\mathcal{O}(P \times \underline{k}) = \{L : L = \oplus(\{p\} \times \underline{k} :$ p ordered as in a linear extension l of P $)\}$.*

PROOF. If every (P, L)-chain has length less than $k-1$ for all linear extension L of P, then we get easily

$$\mathcal{O}(P \times \underline{k}) = \{L : L = \oplus(\{p\} \times \underline{k} : \ p \text{ ordered as in a linear extension } l \text{ of } P\ )\}.$$

Suppose converse is not true. Then there exists a linear extension $L = C_1 \oplus \cdots \oplus C_{i-1} \oplus C_i \oplus C_{i+1} \oplus \cdots \oplus C_n$ of P such that the length of C_i is at least $k-1$. Now define $L_* = [\oplus(\{p\} \times \underline{k} : p$ ordered as in $C_1 \oplus \cdots \oplus C_{i-1})] \oplus [\oplus(C_i \times \{j\} : j = 1, \ldots, k)] \oplus [\oplus(\{p\} \times \underline{k} : p$ ordered as in $C_{i+1} \oplus \cdots \oplus C_n)]$. If the length of C_i is at least k, then $s(L_*, P \times \underline{k}) = \sum_{j=1}^{i-1} |C_j| + k + \sum_{j=i+1}^{n} |C_j| - 1 < |P| - 1$, which contradict Proposition 3.2. If the length of C_i equals $k-1$, then $s(L_*, P \times \underline{k}) = \sum_{j=1}^{i-1} |C_j| + k + \sum_{j=i+1}^{n} |C_j| - 1 = |P| - 1$. Thus $L_* \in \mathcal{O}(P \times \underline{k})$, which contradicts $\mathcal{O}(P \times \underline{k}) = \{L : L = \oplus(\{p\} \times \underline{k} :$ p ordered as in a linear extension l of P $)\}$.

THEOREM 3.6. *Let P be a finite poset. Then every (P, L)-chain has length less than $k-1$ for all linear extension L of P if and only if $|\mathcal{O}(P \times \underline{k})| = |\mathcal{L}(P)|$.*

PROOF. Let $L_1 \in \mathcal{O}(P \times \underline{k})$. Since $s(P \times \underline{k}) = |P| - 1$, every $(P \times \underline{k}, L_1)$-chain has length $k-1$. Thus $L_1 = \oplus(\{p\} \times \underline{k} : p$ ordered as in some linear extension l_1 of $P)$. So $|\mathcal{O}(P \times \underline{k})| \leq |\mathcal{L}(P)|$. On the other hand, for any linear extension L of P we get an optimal linear extension $\oplus(\{p\} \times \underline{k} : p$ ordered as in $L)$. Hence $|\mathcal{O}(P \times \underline{k})| \geq |\mathcal{L}(P)|$.

COROLLARY 3.7. *Suppose P is either (i) a poset whose maximum size of a chain is less than k or (ii) products of chains each of which has length less than k-1. Then*

$$|\mathcal{O}(P \times \underline{k})| = |\mathcal{L}(P)|.$$

4. Concluding Remarks

There are some unsolved problems in counting optimal linear extensions.

PROBLEM 4.1. *Characterize P where P is not bipartite if $|\mathcal{O}(P)| = k$ for $k = 1, 2, 3$.*

PROBLEM 4.2. *Count the number of optimal linear extensions of products of finite chains.*

We denote the set of maximal [minimal] elements of a poset P by $Max(P)$ [$Min(P)$]. Let $\mathcal{F}_{2n}$ be the family of bipartite posets P such that if $Max(P) = \{a_1, a_2, \ldots, a_n\}$ and $Min(P) = \{b_1, b_2, \ldots, b_n\}$, then $b_1 < a_1, a_1 > b_2, b_2 < a_2, \ldots, b_n < a_n$ with possible comparabilities $a_i > b_j$ for some i, j where $1 \leq i < j-1 \leq n-1$. Note that for bipartite posets Problem 4.1 is partially solved by Y.J. Yoon [**14**]: *A bipartite poset P has a unique optimal linear extension if and only if $P \in \mathcal{F}_{2n}$ for some n.* Later H.C. Jung [**9**] extends this idea and characterized bipartite posets with two optimal linear extensions.

Also, Problem 4.2 is partially solved by H.C. Jung [8]: $|\mathcal{O}(\underline{m}^n)| \geq \prod_{k=1}^{n} k^{m^{n-k}}$, and let $a_1 = \ldots = a_i > a_{i+1} \geq a_{i+2} \geq \cdots \geq a_n$, then $|\mathcal{O}(\underline{a_1} \times \cdots \times \underline{a_n})| \geq |\mathcal{O}(\underline{a_1} \times \cdots \times \underline{a_i})|^{a_{i+1} \cdots a_n} |\mathcal{L}(\underline{a_{i+1}} \times \cdots \times \underline{a_n})|$.

References

[1] G. Brightwell and P. Winkler, *Counting linear extensions*, Order **8** (1991), 225–242.

[2] M. Chein and M. Habib, *The jump number of dags and posets: an introduction*, Ann. Disc. Math. **9** (1980), 189–194.

[3] R. P. Dilworth, *A decomposition theorem for partially ordered sets*, Ann. of Math. **51** (1950), 161–166.

[4] D. Duffus, I. Rival and P. Winkler, *Minimizing setups for cycle-free ordered sets*, Proc. Amer. Math. Soc. **85** (1982), 509–513.

[5] M.H.El-Zahar and I. Rival, *Examples of jump-critical ordered sets*, SIAM J. Alg. Disc. Meth. **6** (1985), 143–156.

[6] M.H.El-Zahar and I. Rival, *Greedy linear extensions to minimize jumps*, Disc. Appl. Math. **11** (1995), 143–156.

[7] H.C. Jung, *On the products of some posets:jump number, greediness*, Ars Combinatoria **40** (1995), 101–120.

[8] H.C. Jung, *Lower bounds of the number of jump optimal linear extensions : products of some chains*, Bull. Korean Math. Soc. **32** (1995), 171–177.

[9] H.C. Jung, *Bipartite posets with two optimal linear extensions*, Kyungpook Math. J. **37** (1997), 279–284.

[10] I. Rival, *Linear Extensions of Finite Ordered Sets*, Ann. of Disc. Math. **23** (1984), 355–370.

[11] I. Rival, *Stories about order and the letter N (en)*, Contemporary Math. **57** (1986), 263–285.

[12] M. M. Syslo, *Remarks on Dilworth partially ordered sets*, Proc. of the WG's 85(H. Noltemeier, ed.), Trauner Verlag, Linz, 1985, pp. 355–362.

[13] E. Szpilrajn, *Sur l'extension de l'ordre partiel*, Fund. Math. **16** (1930), 386–389.

[14] Y.J. Yoon, *Bipartite posets with a unique jump optimal linear*, Bull. Korean Math. Soc. **33** (1996), 393–395.

Liberal Arts and Sciences, Korea University of Technology and Education
Byungchon, Chonan, Chungnam, 330-860, Korea

E-mail address: `hcjung@kitenms.kite.ac.kr`

This page intentionally left blank

http://dx.doi.org/10.1090/conm/224/03195

Contemporary Mathematics
Volume **224**, 1999

The Irreducible Representations of Categories

Masashi Kosuda

ABSTRACT. The author constructs the irreducible representations of the Hecke category and the Jones category using the irreducible representations of the centralizers of the mixed tensor representations of quantum groups $\mathcal{U}_q(gl_n(\mathbf{C})$ and using the irreducible representations of the Jones algebra respectively. The irreducible representations of the former category give the HOMFLY invariants of oriented tangles and those of the latter category give the Jones invariants of non oriented tangles. In this article, the author will explain how an irreducible representation of a category becomes completely reducible and apply this to the Hecke category and the Jones category.

Introduction

In this article, we construct irreducible representations of two categories. One is the Hecke category which is obtained from the category of oriented arcs and circles in $\mathbf{R}^2 \times [0,1]$. The other is the Jones category which is obtained from the category of disjoint arcs in $\mathbf{R} \times [0,1]$. These categories are defined in Section 1.

The composition of morphisms is regarded as a product of a category. However, we cannot necessarily define the product between every two elements of the category unlike the case of groups. Nevertheless, some categories have presentations by their generators and relations [**T**] just like groups. The Hecke category and the Jones category have such a property. In other words, we can define these categories by their generators and relations.

A linear representation of a category is a functor from the category to the category of linear maps. Since the Hecke category and the Jones category are defined by the generators and the relations, to define the representations of these two categories, we have only to define functors so that they preserve the relations of each category.

The purpose of this article is to construct the *irreducible* representations of these two categories. An irreducible representation of category is a functor which has no proper subfunctors. (See Section 2.)

The following are the main results. (Theorem 0.3 and Theorem 0.4 are due to his paper [**Y**].)

1991 *Mathematics Subject Classification.* Primary 57M25, 17B37, 18D10; Secondary 05E10.
The author was supported in part by Yukawa Foundation.

THEOREM 0.1. *Let $q \in \mathbf{C}$ be a non zero parameter which is not a root of unity and let $a \in \mathbf{C}$ be another non zero parameter which is not a power of q. Then arbitrary representation of the Hecke category $\mathcal{H} = \mathcal{H}(\mathbf{C}; a^{-1}, q - q^{-1})$ is completely reducible.*

THEOREM 0.2. *Let $\Lambda_{k,l}$ be a set of pairs of partitions defined by*

$$\Lambda_{k,l} = \coprod_{m=0}^{\min(k,l)} \{[\alpha, \beta]; \alpha, \beta \text{ partitions}, |\alpha| = k - m, |\beta| = l - m\}$$

and put

$$\Lambda = \bigcup_{r=0}^{\infty} \Big(\bigcup_{\substack{k \geq 0,\ l \geq 0 \\ k+l=r}} \Lambda_{k,l} \Big) = \coprod_{p=-\infty}^{\infty} \Big(\bigcup_{\substack{k \geq 0,\ l \geq 0 \\ k-l=p}} \Lambda_{k,l} \Big).$$

We fix parameters $q, a \in \mathbf{C}$ so that they satisfy the conditions in Theorem 0.1. Then for the Hecke category $\mathcal{H} = \mathcal{H}(\mathbf{C}; a, q - q^{-1})$ the following hold.

1. *For any pair of partitions $\gamma \in \Lambda$, there exists an irreducible representation $\mathbf{P}^{\gamma}$ of $\mathcal{H}$.*
2. *For $\gamma_1, \gamma_2 \in \Lambda$, the irreducible representations $\mathbf{P}^{\gamma_1}$ and $\mathbf{P}^{\gamma_2}$ of $\mathcal{H}$ are equivalent if and only if $\gamma_1 = \gamma_2$.*
3. *Conversely, for any irreducible representation $\mathbf{P}$ of $\mathcal{H}$, there exists a pair of partition $\gamma \in \Lambda$ such that $\mathbf{P}$ and $\mathbf{P}^{\gamma}$ are equivalent.*

THEOREM 0.3. *(Yoshioka) Let $q \in \mathbf{C}$ be a non zero parameter which is not a root of unity. Then arbitrary representation of the Jones category $\mathcal{J} = \mathcal{J}(\mathbf{C}; q)$ is completely reducible.*

THEOREM 0.4. *(Yoshioka) Let $q \in \mathbf{C}$ be a non zero parameter which is not a root of unity. Then for the Jones category $\mathcal{J} = \mathcal{J}(\mathbf{C}; q)$ the following hold.*

1. *For any non negative integer l, there exists an irreducible representation $\mathbf{Rep}_l$ of $\mathcal{J}$.*
2. *For non negative integers l_1 and l_2, the irreducible representations $\mathbf{Rep}_{l_1}$ and $\mathbf{Rep}_{l_2}$ of $\mathcal{J}$ are equivalent if and only if $l_1 = l_2$.*
3. *Conversely, for any irreducible representation $\mathbf{Rep}$ of $\mathcal{J}$, there exists an integer l such that $\mathbf{Rep}$ and $\mathbf{Rep}_l$ are equivalent.*

In order to prove Theorem 0.1 and Theorem 0.3, we use Theorem 2.8. (The papers [**K, Y**] give full details of the proof.)

We will define the above representations $\{\mathbf{P}^{\gamma}\}$ and $\{\mathbf{Rep}_l\}$ in Section 3 using a family of Bratteli diagrams. The fact that these families of representations satisfy Theorem 0.2 and Theorem 0.4 respectively is proved using Theorem 2.7. (The details are also in the papers [**K, Y**].)

The notion of the irreducible representation was introduced by Neretin [**N**] and formulated by Yoshioka in his Master's thesis [**Y**].

This article is organized as follows. In Section 1 we give the definitions of the Hecke category and the Jones category. In Section 2 we introduce the notion of the irreducible representations of (small) categories according to the papers [**K, N, Y**] and show conditions for a category to be completely reducible. In Section 3 we define a complete set of irreducible representations $\{\mathbf{P}^{\gamma}\}$ of the Hecke category and in Section 4 we define a complete set of irreducible representations $\{\mathbf{Rep}_l\}$ of the Jones category.

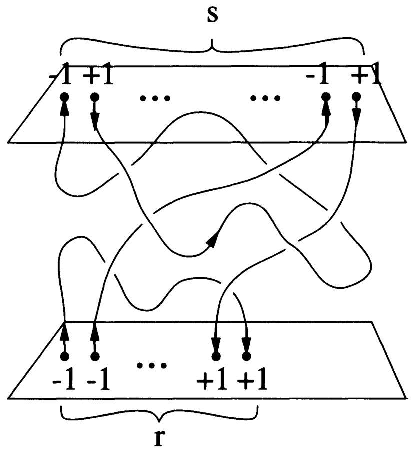


FIGURE 1. An oriented tangle

1. The Hecke category and the Jones category

Let r and s be non-negative integers. An oriented (r, s)-*tangle* T is a finite set of disjoint oriented arcs and circles properly embedded (up to isotopy) in $\mathbf{R}^2 \times [0,1]$ such that

$$\partial T = \{(i,0,0)|i = 1,2,\dots,r\} \cup \{(j,0,1)|j = 1,2,\dots,s\},$$

and such that T is perpendicular to $\mathbf{R}^2 \times \{0\}$ and $\mathbf{R}^2 \times \{1\}$ at every boundary point of ∂T. (See Figure 1.) With each (r, s)-tangle T, we associate two sequences, $\partial_- T = (\epsilon_1(T), \epsilon_2(T), \dots, \epsilon_r(T))$ and $\partial^+ T = (\epsilon^1(T), \epsilon^2(T), \dots, \epsilon^s(T))$, consisting of ± 1. Here $\epsilon_i(T) = +1$ if the tangent vector of T at $(i, 0, 0)$ is outward with respect to $\mathbf{R}^2 \times [0,1]$ and $\epsilon_i(T) = -1$ otherwise. Similarly $\epsilon^j(T) = -1$ if the tangent vector of T at $(j, 0, 1)$ is outward and $\epsilon^j(T) = +1$ otherwise. If $r = 0$ (resp. $s = 0$), then $\partial_- T$ (resp. $\partial^+ T$) is the empty set $\emptyset$. We can easily find that if $\sum_1^r \epsilon_i(T) \neq \sum_1^s \epsilon^j(T)$ then there exist no (r, s)-tangles.

Before defining the Hecke category, we define the category $\mathcal{OTA}$ of oriented tangles. The *objects* of $\mathcal{OTA}$ are defined as the sequences $\{(\epsilon_1, \dots \epsilon_r)|r = 0, 1, \dots\}$ with $\epsilon_i = \pm 1$ including the empty sequence and denoted by $Ob(\mathcal{OTA})$. A *morphism* from $\epsilon = (\epsilon_1, \dots, \epsilon_r)$ to $\epsilon' = (\epsilon'_1, \dots, \epsilon'_s)$ is a $\mathbf{C}$-linear combination of oriented (r, s)-tangles in which each tangle T satisfies $\partial_- T = \epsilon$ and $\partial^+ T = \epsilon'$. The set of morphisms from ϵ to ϵ' is denoted by $Mor_{\mathcal{OTA}}(\epsilon, \epsilon')$. We define the composition product $T_1 \circ T_2$ of tangles T_1 and T_2 by placing T_1 on T_2, gluing the corresponding boundaries and shrinking half along the vertical axis. (Figure 2.) The composition $T_1 \circ T_2$ is defined only when $\partial_- T_1 = \partial^+ T_2$. The composition product will be extended $\mathbf{C}$-linearly.

Slightly changing the argument in Turaev's paper [**T**], we will find that every oriented tangle T can be presented by a composition product of special tangles as in Figure 3. In other words, these special tangles are generators of $\mathcal{OTA}$. We also find that there are relations as in Figure 4 together with the "commuting relations" as in Figure 5 among the generators. (See their paper [**ADO, O, T**].) Conversely, we can define $\mathcal{OTA}$ by these generators and relations.

Keeping the above fact in mind, we define the Hecke category.

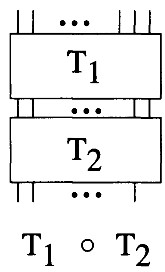


FIGURE 2. Product of tangles

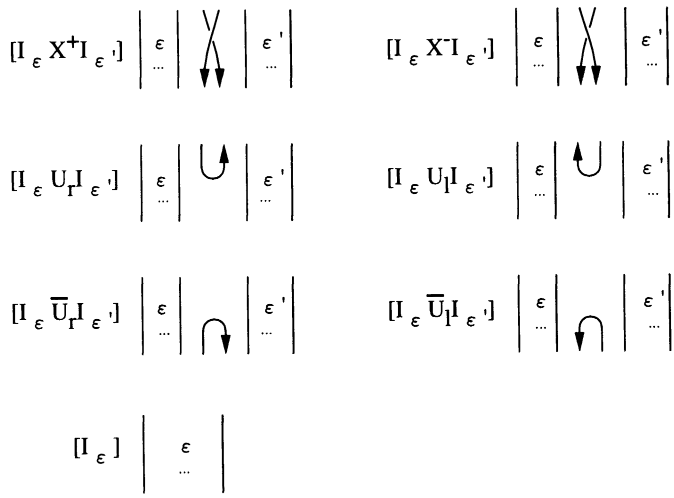


FIGURE 3. Special tangles (generators of the Hecke category)

DEFINITION 1.1. Let $Ob(\mathcal{H}(\mathbf{C};a^{-1},q-q^{-1}))=\{(\epsilon_1,\dots\epsilon_r)|r=0,1,\dots\}$ with $\epsilon_i=+1$ or -1 including the empty sequence be the objects of $\mathcal{H}(\mathbf{C};a^{-1},q-q^{-1})$. Let $[I_\epsilon]$ be the identity morphism on $\epsilon\in Ob(\mathcal{H}(\mathbf{C};a^{-1},q-q^{-1}))$. Then *the Hecke category $\mathcal{H}=\mathcal{H}(\mathbf{C};a^{-1},q-q^{-1})$ corresponding to the field $\mathbf{C}$ and the parameters* $a,q\in\mathbf{C}$ is defined by the generators:

$$\begin{array}{ccccccc}
[I_\epsilon X^+I_{\epsilon'}],[I_\epsilon X^-I_{\epsilon'}] & : & (\epsilon,+1,+1,\epsilon') & \rightarrow & (\epsilon,+1,+1,\epsilon'), & (\epsilon,\epsilon'\in Ob(\mathcal{H})),\\
[I_\epsilon U_rI_{\epsilon'}],[I_\epsilon U_lI_{\epsilon'}] & : & (\epsilon,\epsilon') & \rightarrow & (\epsilon,\pm1,\mp1,\epsilon'), & (\epsilon,\epsilon'\in Ob(\mathcal{H})),\\
[I_\epsilon \bar{U}_rI_{\epsilon'}],[I_\epsilon \bar{U}_lI_{\epsilon'}] & : & (\epsilon,\mp1,\pm1,\epsilon') & \rightarrow & (\epsilon,\epsilon'), & (\epsilon,\epsilon'\in Ob(\mathcal{H})),\\
[I_\epsilon] & : & \epsilon & \rightarrow & \epsilon, & (\epsilon\in Ob(\mathcal{H}))
\end{array}$$

and the commuting relations:

$$[I_afI_{(b,w,c)}]\circ[I_{(a,x,b)}gI_c]=[I_{(a,y,b)}gI_c]\circ[I_afI_{(b,z,c)}]$$

for $f:x\rightarrow y$, $g:z\rightarrow w$, $f,g\in\{X^+,X^-,U_r,U_l,\bar{U}_r,\bar{U}_l\}$ and $a,b,c\in Ob(\mathcal{H})$, and the following relations:

1. $[I_\epsilon\bar{U}_lI_{(+1,\epsilon')}]\circ[I_{(\epsilon,+1)}U_lI_{\epsilon'}]=[I_{(\epsilon,+1,\epsilon')}]=[I_{(\epsilon,+1)}\bar{U}_rI_{\epsilon'}]\circ[I_\epsilon U_rI_{(+1,\epsilon')}]$,
   $[I_{(\epsilon,-1)}\bar{U}_lI_{\epsilon'}]\circ[I_\epsilon U_lI_{(-1,\epsilon')}]=[I_{(\epsilon,-1,\epsilon')}]=[I_\epsilon\bar{U}_rI_{(-1,\epsilon')}]\circ[I_{(\epsilon,-1)}U_rI_{\epsilon'}]$,
2. $[I_{(\epsilon,-1,-1)}\bar{U}_lI_{\epsilon'}]\circ[I_{(\epsilon,-1,-1,+1)}\bar{U}_lI_{(-1,\epsilon')}]\circ[I_{(\epsilon,-1,-1)}X^\pm I_{(-1,-1,\epsilon')}]$
   $\circ[I_{(\epsilon,-1)}U_lI_{(+1,-1,-1,\epsilon')}]\circ[I_\epsilon U_lI_{(-1,-1,\epsilon')}]$

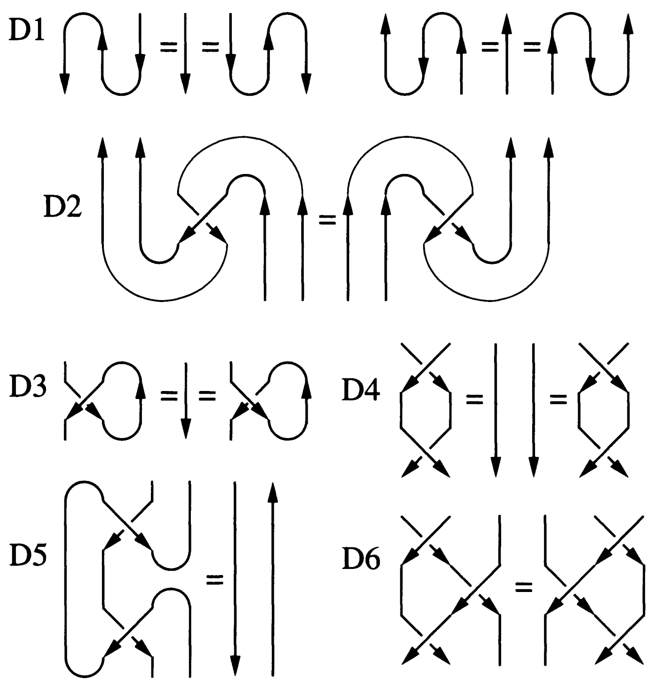


FIGURE 4. Relations

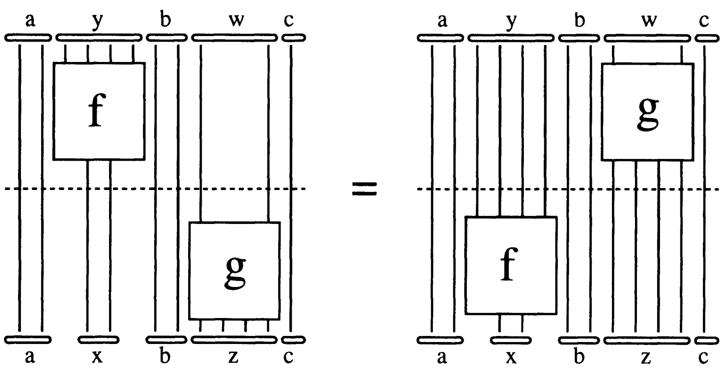


FIGURE 5. Commuting relations

$= [I_\epsilon \bar{U}_r I_{(-1,-1,\epsilon')}] \circ [I_{(\epsilon,-1)} \bar{U}_r I_{(+1,-1,-1,\epsilon')}] \circ [I_{(\epsilon,-1,-1)} X^{\pm} I_{(-1,-1,\epsilon')}]$
$\circ [I_{(\epsilon,-1,-1,+1)} U_r I_{(-1,\epsilon')}] \circ [I_{(\epsilon,-1,-1)} U_r I_{\epsilon'}]$,

3. $[I_{(\epsilon,+1)} \bar{U}_l I_{\epsilon'}] \circ [I_\epsilon X^+ I_{(-1,\epsilon')}] \circ [I_{(\epsilon,+1)} U_r I_{\epsilon'}]$
$= [I_{(\epsilon,+1,\epsilon')}]$
$= [I_{(\epsilon,+1)} \bar{U}_l I_{\epsilon'}] \circ [I_\epsilon X^- I_{(-1,\epsilon')}] \circ [I_{(\epsilon,+1)} U_r I_{\epsilon'}]$,
4. $[I_\epsilon X^+ I_{\epsilon'}] \circ [I_\epsilon X^- I_{\epsilon'}] = [I_{(\epsilon,+1,+1,\epsilon')}] = [I_\epsilon X^- I_{\epsilon'}] \circ [I_\epsilon X^+ I_{\epsilon'}]$,
5. $[I_\epsilon T^- I_{\epsilon'}] \circ [I_\epsilon Y^+ I_{\epsilon'}] = [I_{(\epsilon,+1,-1,\epsilon')}]$,
where $[I_\epsilon T^- I_{\epsilon'}] = [I_\epsilon \bar{U}_r I_{(+1,-1,\epsilon')}] \circ [I_{(\epsilon,-1)} X^- I_{(-1,\epsilon')}] \circ [I_{(\epsilon,-1,+1)} U_r I_{\epsilon'}]$
and $[I_\epsilon Y^+ I_{\epsilon'}] = [I_{(\epsilon,-1,+1)} \bar{U}_l I_{\epsilon'}] \circ [I_{(\epsilon,-1)} X^+ I_{(-1,\epsilon')}] \circ [I_\epsilon U_l I_{(+1,-1,\epsilon')}]$,

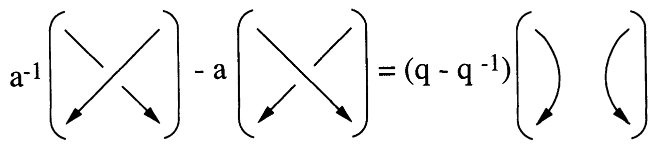


FIGURE 6. The skein relation

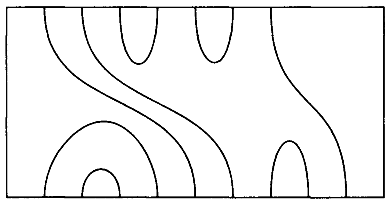


FIGURE 7. (m, n)-diagram

6. $[I_\epsilon X^+ I_{(+1,\epsilon')}] \circ [I_{(\epsilon,+1)} X^+ I_{\epsilon'}] \circ [I_\epsilon X^+ I_{(+1,\epsilon')}]$
$= [I_{(\epsilon,+1)} X^+ I_{\epsilon'}] \circ [I_\epsilon X^+ I_{(+1,\epsilon')}] \circ [I_{(\epsilon,+1)} X^+ I_{\epsilon'}]$,

together with the following *skein* relation (pictured in Figure 6):

$$a^{-1}[I_\epsilon X^+ I_{\epsilon'}] - a[I_\epsilon X^- I_{\epsilon'}] = (q - q)^{-1}[I_{(\epsilon,+1,+1,\epsilon')}],$$

for any pair of objects $\epsilon, \epsilon' \in Ob(\mathcal{H})$.

Note that the restriction of the Hecke category on an object ϵ makes an algebra $\mathcal{H}(\epsilon, \epsilon) = Mor_{\mathcal{H}}(\epsilon, \epsilon)$. The algebra structure of $\mathcal{H}(\epsilon, \epsilon)$ is intensively studied in the papers[**BCHLLS, KM**].

Next we define the Jones category. Let m and n be non-negative integers. We suppose that $m + n$ is divisible by 2. An *(m, n)-diagram D* is defined as a finite set of disjoint arcs properly embedded (up to isotopy) in $\mathbf{R} \times [0, 1]$ such that

$$\partial D = \{(i, 0) | i = 1, 2, \ldots, m\} \cup \{(j, 1) | j = 1, 2, \ldots, n\},$$

and such that D is perpendicular to $\mathbf{R} \times \{0\}$ and $\mathbf{R} \times \{1\}$ at every boundary point of ∂D. (See Figure 7.)

The *objects* of $\mathcal{J}$ are defined as the set of non negative integers and denoted by $Ob(\mathcal{J})$. A *morphism* from m to n is defined as a $\mathbf{C}$-linear combination of (m, n)-diagrams. The set of morphisms from m to n is denoted by $Mor_{\mathcal{J}}(m, n)$. If $m + n$ is not divisible by 2, we understand that $Mor_{\mathcal{J}}(m, n) = \{0\}$. Let $q \in \mathbf{C}$ be a non zero parameter. We define the composition product $D_1 \circ D_2$ of (m, n)-diagrams D_1 and D_2 just like the composition product of tangles. However, if we have p closed circles in the picture $D_1 \circ D_2$, then we remove the circles and multiply by β^p. Here $\beta = q + q^{-1}$. (See Figure 8.) The composition $D_1 \circ D_2$ is defined only when $\partial_- D_1 = \partial^+ D_2$. It will be extended $\mathbf{C}$-linearly.

Similarly to the case of the Hecke category, we can define the Jones category by generators and relations. (See Figure 9.)

DEFINITION 1.2. Let $Ob(\mathcal{J}(\mathbf{C}; q)) = \{0, 1, 2, \cdots\}$ be the objects of $\mathcal{J}(\mathbf{C}; q)$. Namely, $Ob(\mathcal{J}(\mathbf{C}; q))$ is a set of non negative integers. Let $[I_n] \in Mor_{\mathcal{J}(\mathbf{C};q)}(n, n)$ be the identity morphism on $n \in Ob(\mathcal{J}(\mathbf{C}; q))$. Then *the Jones category $\mathcal{J} = \mathcal{J}(\mathbf{C}; q)$* corresponding to the field $\mathbf{C}$ and the parameter $q \in \mathbf{C}$ is defined by the

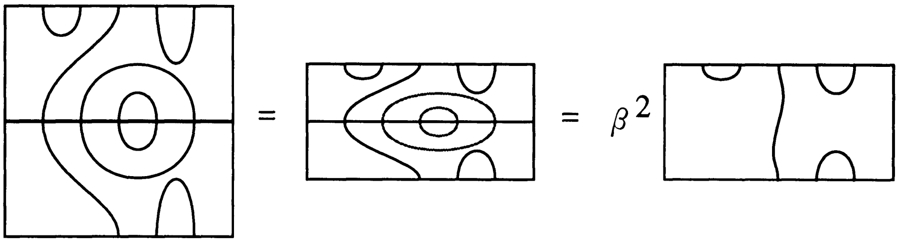


FIGURE 8. Product of (m, n)-diagram

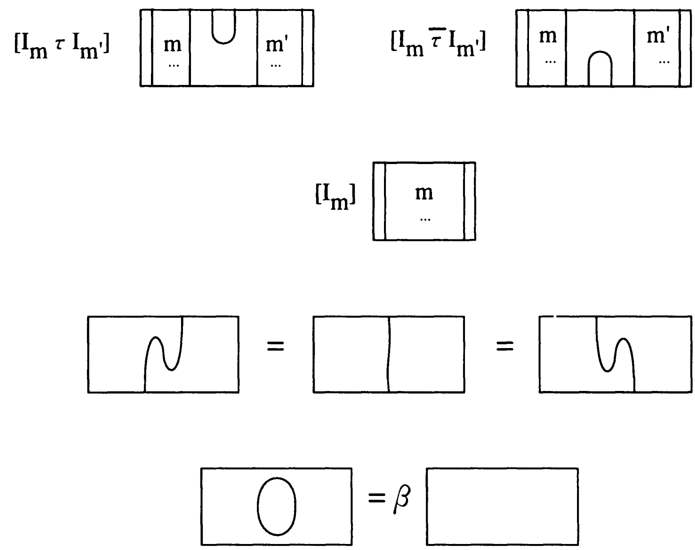


FIGURE 9. Generators and relations of the Jones category

generators:

$$\begin{array}{rcccll} [I_m\tau I_{m'}] & : & m+m' & \longrightarrow & m+m'+2 & (m, m' \in Ob(\mathcal{J})), \\ [I_m\bar{\tau} I_{m'}] & : & m+m'+2 & \longrightarrow & m+m' & (m, m' \in Ob(\mathcal{J})), \\ [I_m] & : & m & \longrightarrow & m & (m \in Ob(\mathcal{J})) \end{array}$$

and the commuting relations:

$$[I_a f I_{b+w+c}] \circ [I_{a+x+b} g I_c] = [I_{a+y+b} g I_c] \circ [I_a f I_{(b+z+c)}]$$

for $f : x \longrightarrow y$, $g : z \longrightarrow w$, $f, g \in \{\tau, \bar{\tau}\}$ and $a, b, c, \in Ob(\mathcal{J})$, and the following relations:

1. $[I_m\bar{\tau} I_{1+m'}] \circ [I_{m+1}\tau I_{m'}] = [I_{m+1+m'}] = [I_{m+1}\bar{\tau} I_{m'}] \circ [I_m \tau I_{1+m'}]$,
2. $[I_m\bar{\tau} I_{m'}] \circ [I_m\tau I_{m'}] = \beta[I_{m+m'}]$,

for any pair of objects $m, m' \in Ob(\mathcal{J})$.

2. Representations of categories

In this section, we introduce the notion of irreducible representations of categories according to the papers [**N**] and [**Y**]. Throughout this section, we consider the following category $\mathcal{A}$. Let K be a field. Suppose that a category $\mathcal{A}$ has the set of objects $Ob(\mathcal{A})$ which is non empty. This means we only consider small categories. For any pair of objects $x, y \in Ob(\mathcal{A})$, the set of morphisms $Mor_{\mathcal{A}}(x,y)$ is a finite dimensional K-vector space. For any triple of objects $x, y, z \in Ob(\mathcal{A})$, the composition of morphisms $Mor_{\mathcal{A}}(y,z) \times Mor_{\mathcal{A}}(x,y) \to Mor_{\mathcal{A}}(x,z)$ are bilinear.

In the following we denote $Mor_{\mathcal{A}}(x,y)$ by $\mathcal{A}(x,y)$. By the definition of the category $\mathcal{A}$, we find that $\mathcal{A}(x,x)$ is a K-algebra for any object $x \in Ob(\mathcal{A})$. We use the notation $\mathcal{V}_{ect}$ to denote the category of finite dimensional K-vector spaces.

DEFINITION 2.1. Let $\mathbf{F}$ be a covariant functor from a category $\mathcal{A}$ to the category $\mathcal{V}_{ect}$. For a pair of objects $x, y \in Ob(\mathcal{A})$, if the correspondence $\alpha \in \mathcal{A}(x,y)$ to $\mathbf{F}(\alpha) \in \mathcal{V}_{ect}$ is K-linear, then we call $\mathbf{F}$ a (linear) representation of the category $\mathcal{A}$.

For the above functor $\mathbf{F}$, we put $\mathcal{V} = \{V_x = \mathbf{F}(x) | x \in Ob(\mathcal{A})\}$. The representation $\mathbf{F}$ is sometimes denoted by $(\mathbf{F}, \mathcal{V})$. The zero representation $\mathbf{O}$ is one of the representations of the category $\mathcal{A}$. It is defined by the functor which maps each object $x \in Ob(\mathcal{A})$ to $\{0\}$.

Two representations $\mathbf{F} = (\mathbf{F}, \mathcal{V} = \{V_x\})$ and $\mathbf{G} = (\mathbf{G}, \mathcal{W} = \{W_x\})$ of $\mathcal{A}$ are *equivalent*, if they are natural equivalent. In other words, there exists a family of K-isomorphisms $\{\phi_x : V_x \to W_x\}$ such that $\mathbf{G}(\alpha) \circ \phi_x = \phi_y \circ \mathbf{F}(\alpha)$ for each pair of objects x, y and for each morphism $\alpha \in \mathcal{A}(x,y)$.

These representations are extensions of the notion of those of K-algebras. In fact, for $x \in Ob(\mathcal{A})$ and $\alpha \in \mathcal{A}(x,x)$, the correspondence $\alpha \mapsto \mathbf{F}(\alpha)$ defines a K-linear map $\mathcal{A}(x,x) \to \mathrm{Hom}_K(V_x, V_x)$ which preserves the composition of morphisms. We denote the representation (as K-algebra) of $\mathcal{A}(x,x)$ by $F_x = (F_x, V_x)$ and call it the *restriction* of $\mathbf{F}$ on $\mathcal{A}(x,x)$ or restriction of $\mathbf{F}$ on x.

DEFINITION 2.2. Let $\mathbf{F} = (\mathbf{F}, \mathcal{V})$ and $\mathbf{G} = (\mathbf{G}, \mathcal{W})$ be representations of a category $\mathcal{A}$. If there exists a family of injective K-linear maps $\{\iota_x : W_x \to V_x\}$ such that $\mathbf{F}(\alpha) \circ \iota_x = \iota_y \circ \mathbf{G}(\alpha)$ holds for each pair of objects x, y and for each morphism $\alpha \in \mathcal{A}(x,y)$, then we call $\mathbf{G}$ a *subrepresentation* of $\mathbf{F}$.

DEFINITION 2.3. If a representation $\mathbf{F}$ has no subrepresentations except $\mathbf{F}$ itself and $\mathbf{O}$, we call it *irreducible.* (The zero representation $\mathbf{O}$ is, by definition, not irreducible.) If a representation $\mathbf{F}$ can be decomposed into a direct sum of irreducible representations, we call it *completely reducible.* Here a direct sum $\oplus_{i\in I}\mathbf{F}_i$ of representations $\mathbf{F}_i = (\mathbf{F}_i, \mathcal{V}_i = \{V_{i,x} | x \in Ob(\mathcal{A})\})$ is defined as follows:

$$\begin{aligned}
\sum_{i\in I} \dim_K V_{i,x} &< \infty, \quad \text{for } x \in Ob(\mathcal{A}), \\
\left(\bigoplus_{i\in I} \mathbf{F}_i\right)(x) &= \bigoplus_{i\in I} V_{i,x} \quad \text{for } x \in Ob(\mathcal{A}), \\
\left(\bigoplus_{i\in I} \mathbf{F}_i\right)(\alpha) &= \bigoplus_{i\in I} \mathbf{F}_i(\alpha) : \bigoplus_{i,x} V_{i,x} \mapsto \bigoplus_{i\in I} V_{i,y} \\
&\qquad \text{for } x, y \in Ob(\mathcal{A}) \text{ and } \alpha \in \mathcal{A}(x,y).
\end{aligned}$$

LEMMA 2.4. *Let $\mathbf{F} = (\mathbf{F}, \mathcal{V})$ be a representation of a category $\mathcal{A}$. If a representation $G = (G, W)$ of the algebra $\mathcal{A}(x,x)$ is a subrepresentation of $F_x = (F_x, V_x)$, then there exists a subrepresentation $\mathbf{G} = (\mathbf{G}, \mathcal{W})$ of $\mathbf{F}$ such that the restriction of $\mathbf{G}$ on $\mathcal{A}(x,x)$ is equivalent to G.*

PROOF. Define a functor $\mathbf{G} = (\mathbf{G}, \mathcal{W})$ as follows:

1. $\mathbf{G}(x) = W_x = W$,
2. $\mathbf{G}(y) = W_y = \mathbf{F}(\mathcal{A}(x, y))W$ for $y \in Ob(\mathcal{A})$,
3. $\mathbf{G}(\alpha) = \mathbf{F}(\alpha)|_{W_{x'}}$ for $x', y' \in Ob(\mathcal{A}), \alpha \in \mathcal{A}(x', y')$.

Then we have

$$\begin{aligned} \mathbf{G}(\alpha)(W_{x'}) &= \mathbf{G}(\alpha)(\mathbf{F}(\mathcal{A}(x, x'))W) \\ &= \mathbf{F}(\alpha \circ \mathcal{A}(x, x'))W \\ &\subset \mathbf{F}(\mathcal{A}(x, y'))W \\ &= W_{y'}. \end{aligned}$$

□

We call the functor $\mathbf{G}$ which is defined as above the *cyclic hull* of G with respect to $\mathbf{F}$.

LEMMA 2.5. *Let $\mathbf{F}$ be an irreducible representation of a category $\mathcal{A}$. For an object $x \in Ob(\mathcal{A})$, the restriction $F_x = (F_x, V_x)$ of $\mathbf{F}$ on $\mathcal{A}(x, x)$ defines an irreducible representation or the zero representation of $\mathcal{A}(x, x)$.*

PROOF. Suppose that we have $V_x \neq \{0\}$. If there exists a proper non zero subrepresentation $F'_x = (F'_x, V'_x)$ of F_x, the cyclic hull $\mathbf{F}'$ of F'_x with respect to $\mathbf{F}$ is not equivalent to $\mathbf{F}$ nor $\mathbf{O}$. This contradicts that $\mathbf{F}$ is irreducible . □

For an irreducible representation we have the following lemma.

LEMMA 2.6. *Let $\mathbf{F}$ be an irreducible representation of a category $\mathcal{A}$. For a pair of objects $x, y \in Ob(\mathcal{A})$, if $V_x \neq \{0\}$ and $V_y \neq \{0\}$, then there exists a morphism $\alpha \in \mathcal{A}(x, y)$ such that $\mathbf{F}(\alpha) : V_x \to V_y$ is non zero.*

PROOF. Suppose that $\mathbf{F}(\mathcal{A}(x, y)) = \{0\}$. Define $(\mathbf{F}', \mathcal{V}' = \{V'_z\})$ as follows:

- $V'_z = \mathbf{F}(\mathcal{A}(x, z))V_x$ for each object $z \in Ob(\mathcal{A})$,
- $\mathbf{F}'(\alpha) = \mathbf{F}(\alpha)|_{V'_z} : V'_z \to V'_w$ for $z, w \in Ob(\mathcal{A})$ and for $\alpha \in \mathcal{A}(z, w)$.

Since $V_y \neq \{0\}$ and $V'_y = \{0\}$ by the definition, $(\mathbf{F}', \mathcal{V}')$ becomes a proper subrepresentation of $\mathbf{F}$. This contradicts that $\mathbf{F}$ is irreducible. □

THEOREM 2.7. *Let $\mathbf{F} = (\mathbf{F}, \mathcal{V})$ and $\mathbf{G} = (\mathbf{G}, \mathcal{W})$ be irreducible representations of a category $\mathcal{A}$. If V_x and W_x are equivalent as $\mathcal{A}(x, x)$-module for some object $x \in Ob(\mathcal{A})$ and if they are not equal to $\{0\}$, then $\mathbf{F}$ and $\mathbf{G}$ are equivalent as representations of the category.*

THEOREM 2.8. *Suppose that a category $\mathcal{A}$ satisfies the following further conditions.*

1. *$Ob(\mathcal{A})$ is a well-ordered set.*
2. *For any object $x \in Ob(\mathcal{A})$, all the finite dimensional representations of the K-algebra $\mathcal{A}(x, x)$ are completely reducible.*
3. *If objects $x, y \in Ob(\mathcal{A})$ satisfy $x \leq y$ and $\mathcal{A}(x, y) \neq \{0\}$, then $\mathcal{A}(y, x) \neq \{0\}$ and there exist morphisms $\tau_y \in \mathcal{A}(y, x)$ and $\tau'_y \in \mathcal{A}(x, y)$ such that $1_x = \tau_y \circ \tau'_y$, where 1_x is the unit of $\mathcal{A}(x, x)$.*

Then an arbitrary representation $\mathbf{F} = (\mathbf{F}, \mathcal{V})$ of $\mathcal{A}$ is completely reducible.

For the proof of the above two theorems, see the papers [**K, N, Y**].

3. Irreducible representations of the Hecke category

In this section we define linear maps $\{\mathbf{P}^\gamma = (\mathbf{P}^\gamma, \mathcal{L}^\gamma)\}$ from $\mathcal{H}$ to categories of linear spaces $\{\mathcal{L}^\gamma\}$. These linear maps define all the irreducible representations of the Hecke category $\mathcal{H}$. Let $q \in \mathbf{C}$ be a non zero parameter which is not a root of unity and let $a \in \mathbf{C}$ be another non zero parameter which is not a power of q. (See the condition in Theorem 0.1.) Let $\mathcal{H} = \mathcal{H}(\mathbf{C}; a^{-1}, q - q^{-1})$ be the Hecke category corresponding to $\mathbf{C}$, a^{-1} and $q - q^{-1}$.

Categories $\{\mathcal{L}^\gamma\}$ are defined over $\mathbf{C}$. The objects of $\mathcal{L}^\gamma$ are $\mathbf{C}$-vector spaces $\{\mathbf{C}\Omega(\epsilon)^\gamma | \epsilon \in Ob(\mathcal{H})\}$ and the morphisms of $\mathcal{L}^\gamma$ are the linear maps between two objects of $\mathcal{L}^\gamma$.

We define the set $\Omega(\epsilon)^\gamma$ according to the paper [**S**] by Stembridge.

Let $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_n)$ be an integer sequence, and define $|\lambda| = \lambda_1 + \lambda_2 + \cdots + \lambda_n$. We call that λ is a *staircase* if the sequence is weakly decreasing. In particular we call that λ is a *partition* of N if the sequence is non negative, weakly decreasing, and $|\lambda| = N$. Two partitions $(\lambda_1, \lambda_2, \cdots, \lambda_n)$ and $(\lambda_1, \lambda_2, \cdots, \lambda_n, 0)$ are considered to be the same. The *length* $l(\lambda)$ of λ is the number of nonzero terms in λ. Let $\emptyset$ be the null partition (the partition of 0). Every partition λ has the dual partition $\lambda^* = (\lambda'_1, \ldots \lambda'_{\lambda_1})$, where $\lambda'_i = \mathrm{Card}\{j | \lambda_j \geq i\}$. For a partition λ, the Young diagram of λ is the arrangement of $|\lambda|$ squares; the first row λ_1, the second row λ_2, $\cdots$, the last row λ_n parts, and line up to the left. We denote the coordinates of boxes in a Young diagram in matrix style. For example, if a box is in the i-th row and in the j-th column of a Young diagram λ, it is denoted by $(i, j) \in \lambda$. Each box in a Young diagram λ has its *hook length* h_λ defined by

$$h_\lambda(i, j) = \lambda_i - j + \lambda'_j - i + 1.$$

Let $\gamma = [\alpha, \beta]$ be a pair of partitions. For a fixed n such that $n \geq l(\alpha) + l(\beta)$, we can give a correspondence between staircases and pairs of partitions by

$$(\alpha_1, \alpha_2, \ldots, -\beta_2, -\beta_1) \in \mathbf{Z}^n \Longleftrightarrow [\alpha, \beta].$$

In the following, we suppose that n is large enough comparing to $l(\alpha) + l(\beta)$ and we fix this n. So we can identify a staircase with a pair of partitions by the above correspondence. For a staircase $\gamma = [\alpha, \beta]$, if we take a negative integer s so that $s \leq -\beta_1$, then there exists a partition $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_n)$ such that

$$(\lambda_1 + s, \lambda_2 + s, \ldots, \lambda_n + s) = (\gamma_1, \gamma_2, \ldots, \gamma_n).$$

Staircases are partially ordered by defining

$$\gamma = (\gamma_1, \gamma_2, \ldots, \gamma_n) \subset \gamma' = (\gamma'_1, \gamma'_2, \cdots, \gamma'_n)$$

if and only if

$$\gamma_1 \leq \gamma'_1, \gamma_2 \leq \gamma'_2, \cdots, \gamma_n \leq \gamma'_n.$$

With the language of pairs of partitions, we may define $[\alpha, \beta] \subset [\alpha', \beta']$ by $\alpha_1 \leq \alpha'_1, \alpha_2 \leq \alpha'_2, \cdots$ and $\beta'_1 \leq \beta_1, \beta'_2 \leq \beta_2, \cdots$. If we consider a staircase as a pair of Young diagrams, and consider it as two sets of coordinates in matrix style, then $\gamma \subset \gamma'$ means $\alpha \subset \alpha'$ and $\beta' \subset \beta$. Under this preparation, for an object $\epsilon \in Ob(\mathcal{H})$, we shall associate a set of *tableaux* $\Omega(\epsilon)$. A tableau is a sequence of staircases which is defined as follows.

DEFINITION 3.1. Let $\gamma^{(0)}$ be the staircase defined by the pair of the null partitions $[\emptyset, \emptyset]$. A *tableau* ξ *of length* r *and shape* γ is a sequence $(\gamma^{(1)}, \ldots, \gamma^{(r)} = \gamma)$

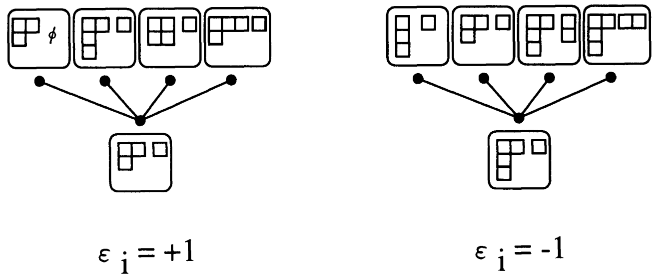


FIGURE 10. The branching rule

of staircases in which either $\gamma^{(i)} \supset \gamma^{(i-1)}, |\gamma^{(i)}| - |\gamma^{(i-1)}| = 1$ or $\gamma^{(i)} \subset \gamma^{(i-1)}$, $|\gamma^{(i)}| - |\gamma^{(i-1)}| = -1$ for $1 \leq i \leq r$. The tableau ξ is said to be of *type* $\epsilon = (\epsilon_1, \dots, \epsilon_r)$, where $\epsilon_i = |\gamma^{(i)}| - |\gamma^{(i-1)}|$.

Figure 10 shows how $\gamma^{(i)}$ is generated from $\gamma^{(i-1)}$ according to the signature ϵ_i in making a tableau. We call this generation rule the *branching rule.*

We denote the number of ones in ϵ by $\mathrm{Pos}(\epsilon)$, and the number of minus ones in ϵ by $\mathrm{Neg}(\epsilon)$.

All the tableaux of type ϵ are conveniently described using the graph Γ_ϵ as follows. Let $\mathrm{Pos}(\epsilon) = k$ and $\mathrm{Neg}(\epsilon) = l$. Vertices of Γ_ϵ are classified to $k + l + 1$ floors. Let

$$\Lambda_{k,l} = \coprod_{m=0}^{\min(k,l)} \{[\alpha, \beta]; \alpha, \beta \text{ partitions}, |\alpha| = k - m, |\beta| = l - m\}$$

be a set of pairs of partitions. The top floor (the $k + l$-th floor) of Γ_ϵ has $|\Lambda_{k,l}|$ vertices which are labeled by the elements of $\Lambda_{k,l}$ one by one. The bottom floor (the 0-th floor) has a unique vertex labeled by the pair of the null partitions $\gamma^{(0)} = [\emptyset, \emptyset] \in \Lambda_{0,0}$. The i_0-th floor $(1 \leq i_0 < k + l)$ of Γ_ϵ has $|\Lambda_{k_0,l_0}|$ vertices which are labeled by staircases in Λ_{k_0,l_0} one by one. Here $k_0 = |\{\epsilon_i > 0; i = 1, 2, \dots, i_0\}|$ and $l_0 = |\{\epsilon_i < 0; i = 1, 2, \dots, i_0\}|$. Two vertices labeled by γ and γ' respectively are joined by an edge if and only if they are different each other only by one box as pairs of partitions.

EXAMPLE 3.2. If $\epsilon = (+1, -1, +1, -1, +1)$, Γ_ϵ is pictured in Figure 11.

We can get any tableau of shape γ and of type ϵ from the graph Γ_ϵ as an ascending path from the bottom vertex $[\emptyset, \emptyset]$ to the top vertex γ. Conversely, any ascending path from the bottom vertex to a top vertex γ expresses some tableau. We identify each of these paths with the corresponding tableau.

As it defined in [**GHJ, KM**], each vertex of Γ_ϵ has its *weight.* These weights are defined by the indices $\{\gamma\}$ which are assigned to the vertices. Let Λ be the set of all the pairs of partitions:

$$\Lambda = \bigcup_{r=0}^{\infty} \Big(\bigcup_{\substack{k \geq 0,\ l \geq 0 \\ k+l=r}} \Lambda_{k,l} \Big).$$

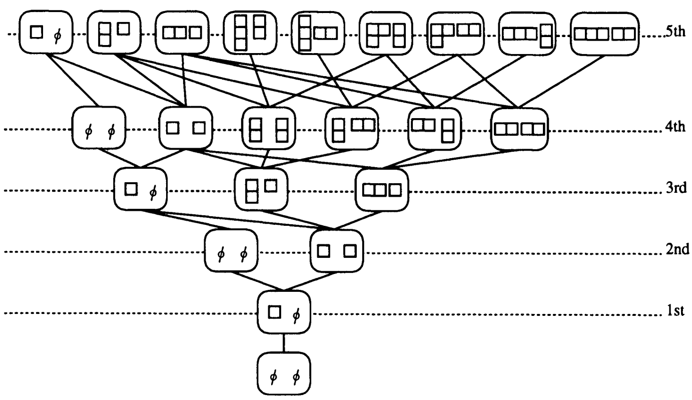


FIGURE 11. $\Gamma_{(+1,-1,+1,-1,+1)}$

By the definition of $\Lambda_{k,l}$ it is easy to see that $\Lambda_{k+1,l+1} \supset \Lambda_{k,l}$. On the other hand, if $k-l \neq k'-l'$, then $\Lambda_{k,l} \cap \Lambda_{k',l'} = \emptyset$. Hence we have

$$\Lambda = \coprod_{p=-\infty}^{\infty} \Big(\bigcup_{\substack{k\geq 0,\ l\geq 0 \\ k-l=p}} \Lambda_{k,l} \Big).$$

Let $\gamma = [\lambda, \mu]$ such that $\lambda = (\lambda_1, \lambda_2, \dots)$ and $\mu = (\mu_1, \mu_2, \dots)$. Then the weight $s[\gamma]$ of γ is defined by

$$(3.3) \qquad s[\gamma] = \frac{\prod_{(i,j)\in\mu}\left([a;j-i-l(\lambda)]\prod_{k=1}^{l(\lambda)}\frac{[a;j-i+\lambda_k-k+1]}{[a;j-i+\lambda_k-k]}\right)\prod_{(i,j)\in\lambda}[a;j-i]}{\prod_{(i,j)\in\lambda}[h_\lambda(i,j)]\prod_{(i,j)\in\mu}[h_\mu(i,j)]},$$

where

$$[a;m] = \frac{a^{-1}q^m - aq^{-m}}{q-q^{-1}} \text{ and } [m] = [1;m] = \frac{q^m - q^{-m}}{q-q^{-1}}.$$

In the following we fix a staircase $\gamma \in \Lambda$. For the fixed staircase γ, $\Omega(\epsilon)^\gamma$ is the set of all the tableaux whose shapes are γ and whose types are ϵ. The objects of $\mathcal{L}^\gamma$ are the $\mathbf{C}$-vector spaces $\{\mathbf{C}\Omega(\epsilon)^\gamma | \epsilon \in Ob(\mathcal{H})\}$. If $\Omega(\epsilon)^\gamma = \emptyset$, then $\mathbf{C}\Omega(\epsilon)^\gamma = \{0\}$. We denote the natural basis of $\mathbf{C}\Omega(\epsilon)^\gamma$ defined by the tableaux $\{\xi | \xi \in \Omega(\epsilon)^\gamma\}$ by $\{v_\xi\}$. The morphisms of $\mathcal{L}^\gamma$ are the linear maps between two objects of $\mathcal{L}^\gamma$ and the composition is the composition of linear maps.

An object $\epsilon = (\epsilon_1, \dots, \epsilon_k)$ of $\mathcal{H}$ is mapped by $\mathbf{P}^\gamma$ to an object $\mathbf{P}^\gamma(\epsilon) = \mathbf{C}\Omega(\epsilon)^\gamma$ of $\mathcal{L}^\gamma$. If either $\mathbf{C}\Omega(\epsilon)^\gamma$ or $\mathbf{C}\Omega(\epsilon')^\gamma$ is the 0 space, then $Mor_{\mathcal{L}^\gamma}(\epsilon, \epsilon') = \{0\}$. Hence if either $\Omega(\epsilon)^\gamma = \emptyset$ or $\Omega(\epsilon')^\gamma = \emptyset$, then $\mathbf{P}^\gamma(\iota(T)) = 0$ for any tangle T such that $\partial_- T = \epsilon$ and $\partial^+ T = \epsilon'$.

In the following we define the linear map $\mathbf{P}^\gamma$ assigning each generator of the Hecke category $\mathcal{H}$ to a morphism of $\mathcal{L}^\gamma$.

Definition of $\mathbf{P}^\gamma(\iota([I_\epsilon X^+ I_{\epsilon'}]))$ and $\mathbf{P}^\gamma(\iota([I_\epsilon X^- I_{\epsilon'}]))$

Let $x = (\epsilon, +1, +1, \epsilon')$ be an object on which $\iota([I_\epsilon X^+ I_{\epsilon'}])$ is defined. Suppose that $\mathrm{Pos}(x) = k$, $\mathrm{Neg}(x) = l$ and $\epsilon = (\epsilon_1, \epsilon_2, \dots, \epsilon_{i-1})$, $\epsilon' = (\epsilon_{i+2}, \epsilon_{i+3}, \dots, \epsilon_{k+l})$.

If $\gamma \notin \Lambda_{k,l}$, then define $\mathbf{P}^\gamma(\iota([I_\epsilon X^+ I_{\epsilon'}])) = 0$.

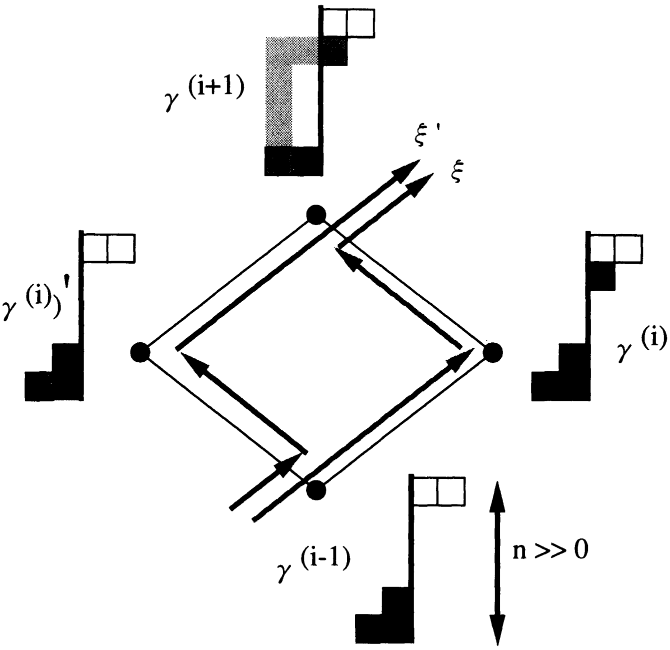


FIGURE 12. Tableaux ξ and ξ'

Otherwise, each of the generators of the form $\{\iota([I_\epsilon X^+ I_{\epsilon'}])\}$ is mapped to a morphism from the object $\mathbf{C}\Omega(x)^\gamma$ to itself. Let

$$\xi = (\gamma^{(1)}, \dots, \gamma^{(i-1)}, \gamma^{(i)}, \gamma^{(i+1)}, \dots, \gamma^{(k+l)} = \gamma)$$

be a tableau of shape γ and of type x. Then according to the branching rule as in Figure 10, the staircase $\gamma^{(i+1)}$ is obtained from $\gamma^{(i-1)}$ one of three ways.

1. By adding two boxes to the same row of $\gamma^{(i-1)}$.
2. By adding two boxes to the same column of $\gamma^{(i-1)}$.
3. By adding boxes in different rows and columns of $\gamma^{(i-1)}$.

(Here we regard the staircases $\gamma^{(i-1)}$ and $\gamma^{(i+1)}$ as Young diagrams defined by partitions and a negative integer.) In case (c), there exists exactly one tableau

$$\xi' = (\gamma^{(1)}, \dots, \gamma^{(i-1)}, (\gamma^{(i)})', \gamma^{(i+1)}, \dots, \gamma^{(k+l)}),$$

which differs from ξ in its i-th coordinate only. Further in this case, the two boxes $\gamma^{(i+1)} \setminus \gamma^{(i)}$ and $\gamma^{(i)} \setminus \gamma^{(i-1)}$ make a hook as pictured in Figure 12. Write h for the hook length (including the added two boxes). The *axis distance* $d(\xi, i)$ is defined as follows:

$$d(\xi, i) = \begin{cases} h - 1, & \text{if the lower left box was added first,} \\ 1 - h, & \text{if the upper right box was added first.} \end{cases}$$

We note that axis distance may be negative. If $\gamma^{(i-1)}$ and $\gamma^{(i)}$ are both partitions and if the first box is added to (r_i, c_i) and the second box is added to (r_{i+1}, c_{i+1}), then we have

$$d(\xi, i) = (c_{i+1} - r_{i+1}) - (c_i - r_i).$$

Using this axis distance d and q-integers $[i]$ which is defined in (3.3), we define $\mathbf{P}^\gamma(\iota([I_\epsilon X^+ I_{\epsilon'}]))$ and $\mathbf{P}^\gamma(\iota([I_\epsilon X^- I_{\epsilon'}]))$as follows:

$$\begin{aligned}
\mathbf{P}^\gamma(\iota([I_\epsilon X^+ I_{\epsilon'}]))v_\xi &= a\cdot a_\xi v_\xi + a\cdot b_\xi v_{\xi'} = \begin{cases} a\cdot q v_\xi & \text{case (a)},\\ -a\cdot q^{-1} v_\xi & \text{case (b)},\\ a\cdot \frac{q^d}{[d]} v_\xi + a\cdot \frac{[d-1]}{[d]} v_{\xi'} & \text{case (c)},\end{cases}\\
\mathbf{P}^\gamma(\iota([I_\epsilon X^- I_{\epsilon'}]))v_\xi &= a^{-1}\cdot a'_\xi v_\xi + a^{-1}\cdot b_\xi v_{\xi'}\\
&= \begin{cases} a^{-1}\cdot q^{-1} v_\xi & \text{case (a)},\\ a^{-1}\cdot(-q) v_\xi & \text{case (b)},\\ a^{-1}\cdot \frac{q^{-d}}{[d]} v_\xi + a^{-1}\cdot \frac{[d-1]}{[d]} v_{\xi'} & \text{case (c)}.\end{cases}
\end{aligned}$$

If the axis distance involves the depth of staircases n, then we replace q^n by a^{-1}. For example if $d = i+n$, then

$$[d] = [i+n] = \frac{q^{i+n} - q^{-i-n}}{q-q^{-1}} = \frac{a^{-1}q^i - aq^{-i}}{q-q^{-1}} = [a;i].$$

Definition of $\mathbf{P}^\gamma(\iota([I_\epsilon U_r I_{\epsilon'}]))$ and $\mathbf{P}^\gamma(\iota([I_\epsilon U_l I_{\epsilon'}]))$

Let $x = (\epsilon,\epsilon')$, $x_r = (\epsilon,+1,-1,\epsilon')$ $x_l = (\epsilon,-1,+1,\epsilon')$ be objects such that $\iota([I_\epsilon U_r I_{\epsilon'}]) : x \to x_r$ and $\iota([I_\epsilon U_l I_{\epsilon'}]) : x \to x_l$ are defined. Suppose that $\mathrm{Pos}(x) = k, \mathrm{Neg}(x) = l$ and $\epsilon = (\epsilon_1,\epsilon_2,\dots,\epsilon_i)$, $\epsilon' = (\epsilon_{i+1},\epsilon_{i+2},\dots,\epsilon_{k+l})$.

If $\gamma \notin \Lambda_{k,l}$, then define $\mathbf{P}^\gamma(\iota([I_\epsilon U_r I_{\epsilon'}])) = 0$ and $\mathbf{P}^\gamma(\iota([I_\epsilon U_l I_{\epsilon'}])) = 0$.

A generator $\iota([I_\epsilon U_r I_{\epsilon'}])$ (resp. $\iota([I_\epsilon U_l I_{\epsilon'}])$) is mapped by $\mathbf{P}^\gamma$ to a morphism from the object $\mathbf{C}\Omega(x)^\gamma$ to the object $\mathbf{C}\Omega(x_r)^\gamma$ (resp. $\mathbf{C}\Omega(x_l)^\gamma$). For each tableau

$$\xi = (\gamma^{(1)},\dots,\gamma^{(i-1)},\mu,\gamma^{(i+1)},\dots,\gamma^{(k+l)} = \gamma)$$

of shape γ and of type x, we define the tableau $\xi(j)$ (resp. $\xi'(j')$) of shape γ and of type x_r (resp. x_l) as follows:

$$\begin{aligned}
\xi(j) &= (\gamma^{(1)},\dots,\gamma^{(i-1)},\mu,\lambda(j),\mu,\gamma^{(i+1)},\dots,\gamma^{(k+l)} = \gamma),\\
\big(\text{resp. } \xi'(j') &= (\gamma^{(1)},\dots,\gamma^{(i-1)},\mu,\nu(j'),\mu,\gamma^{(i+1)},\dots,\gamma^{(k+l)} = \gamma),\big)
\end{aligned}$$

where $\{\lambda(j)\}$ $(j = 1,2,\dots,p(\mu))$ (resp. $\{\nu(j')\}$ $(j' = 1,2,\dots,p'(\mu))$ are all the staircases such that $\lambda(j) \supset \mu$ and $|\lambda(j)| - |\mu| = 1$ (resp. $\nu(j') \subset \mu$ and $|\nu(j')| - |\mu| = -1$). See the branching rule pictured in Figure 10. Under these notation $\mathbf{P}^\gamma(\iota([I_\epsilon U_r I_{\epsilon'}]))$ (resp. $\mathbf{P}^\gamma(\iota([I_\epsilon U_l I_{\epsilon'}]))$) is defined as follows:

$$\begin{aligned}
\mathbf{P}^\gamma(\iota([I_\epsilon U_r I_{\epsilon'}]))v_\xi &= \sum_j^{p(\mu)} v_{\xi(j)}.\\
\Bigg(\text{resp. } \mathbf{P}^\gamma(\iota([I_\epsilon U_l I_{\epsilon'}]))v_\xi &= \sum_{j'}^{p'(\mu)} \frac{s[\nu(j')]}{s[\mu]} v_{\xi'(j')}.\Bigg)
\end{aligned}$$

Definition of $\mathbf{P}^\gamma(\iota([I_\epsilon \bar{U}_r I_{\epsilon'}]))$ and $\mathbf{P}^\gamma(\iota([I_\epsilon \bar{U}_l I_{\epsilon'}]))$

Let $x_r = (\epsilon,-1,+1,\epsilon')$, $x_l = (\epsilon,+1,-1,\epsilon')$, $\hat{x} = (\epsilon,\epsilon')$ be objects such that $\iota([I_\epsilon \bar{U}_r I_{\epsilon'}]) : x_r \to \hat{x}$ and $\iota([I_\epsilon \bar{U}_l I_{\epsilon'}]) : x_l \to \hat{x}$ are defined. Suppose that $\mathrm{Pos}(x_r) = \mathrm{Pos}(x_l) = k, \mathrm{Neg}(x_r) = \mathrm{Neg}(x_l) = l$ and

$$\epsilon = (\epsilon_1,\epsilon_2,\dots,\epsilon_{i-1}),\quad \epsilon' = (\epsilon_{i+2},\epsilon_{i+3},\dots,\epsilon_{k+l}).$$

If $\gamma \notin \Lambda_{k-1,l-1}$, then define $\mathbf{P}^\gamma(\iota([I_\epsilon \bar{U}_r I_{\epsilon'}])) = 0$ and $\mathbf{P}^\gamma(\iota([I_\epsilon \bar{U}_l I_{\epsilon'}])) = 0$.

A generator $\iota([I_\epsilon \bar{U}_r I_{\epsilon'}])$ (resp. $\iota([I_\epsilon \bar{U}_l I_{\epsilon'}])$) is mapped by $\mathbf{P}^\gamma$ to a morphism from the object $\mathbf{C}\Omega(x_r)^\gamma$ (resp. $\mathbf{C}\Omega(x_l)^\gamma$) to the object $\mathbf{C}\Omega(\hat{x})^\gamma$. For each tableau

$$\xi = (\gamma^{(1)}, \dots, \gamma^{(i-1)} = \nu, \gamma^{(i)} = \mu, \gamma^{(i+1)}, \dots, \gamma^{(k+l)} = \gamma)$$

of shape γ and of type x_r (resp. x_l), we define

$$\begin{aligned} \mathbf{P}^\gamma(\iota([I_\epsilon \bar{U}_r I_{\epsilon'}]))v_\xi &= \delta(\gamma^{(i-1)}, \gamma^{(i+1)})v_{\hat{\xi}} \\ &= \begin{cases} 0, & \text{if } \gamma^{(i-1)} \neq \gamma^{(i+1)}, \\ v_{\hat{\xi}}, & \text{if } \gamma^{(i-1)} = \gamma^{(i+1)}, \end{cases} \end{aligned}$$

$$\left(\text{resp. } \mathbf{P}^\gamma(\iota([I_\epsilon \bar{U}_l I_{\epsilon'}]))v_\xi = \begin{cases} 0, & \text{if } \gamma^{(i-1)} \neq \gamma^{(i+1)}, \\ \frac{s[\mu]}{s[\nu]} v_{\hat{\xi}}, & \text{if } \gamma^{(i-1)} = \gamma^{(i+1)}, \end{cases} \right)$$

where $\hat{\xi}$ is a tableau of shape γ and of type $\hat{x}$ which is obtained from the tableau ξ by removing the i-th coordinate $\gamma^{(i)} = \mu$ and the $(i+1)$-st coordinate $\gamma^{(i+1)}$.

4. Irreducible representations of the Jones category

In this section we define linear maps $\{\mathbf{Rep}_l = (\mathbf{Rep}_l, \mathcal{L}_l)\}$ from $\mathcal{J}$ to the categories of linear spaces $\{\mathcal{L}_l\}$. These linear maps define all the irreducible representations of the Jones category $\mathcal{J}$. Let $q \in \mathbf{C}$ be a non zero parameter which is not a root of unity. (See the condition in Theorem 0.3.) Let $\mathcal{J} = \mathcal{J}(\mathbf{C}; q)$ be the Jones category corresponding to the complex field $\mathbf{C}$ and the parameter q.

In this section, a *tableau* is a sequence of partitions which is defined as follows.

DEFINITION 4.1. Let $\alpha^{(0)}$ be the null partition. A *tableau ξ of length n and shape α* is a sequence $(\alpha^{(1)}, \dots, \alpha^{(n)} = \alpha)$ of partitions in which satisfies $l(\alpha^{(i)}) \leq 2$, $\alpha^{(i)} \supset \alpha^{(i-1)}$ and $|\alpha^{(i)}| - |\alpha^{(i-1)}| = 1$. for $i = 1, 2, \dots, n$.

In the above definition, since the lengths of the shapes are at most 2, each shape α has a presentation by two non negative integers (α_1, α_2). It is also characterized by two non negative integers $l = \alpha_1 - \alpha_2$ and $n = \alpha_1 + \alpha_2$.

Let $V_l(n)$ be a set of tableaux whose shapes are $\alpha = (\alpha_1, \alpha_2)$ such that $l = \alpha_1 - \alpha_2$ and $n = \alpha_1 + \alpha_2$. Now we define categories $\{\mathcal{L}_l\}$. The objects of the categories $\{\mathcal{L}_l\}$ are $\mathbf{C}$-vector spaces $\{\mathbf{C}V_l(n) | n \in Ob(\mathcal{J})\}$ and the morphisms of $\mathcal{L}_l$ are the linear maps between two objects of $\mathcal{L}_l$.

All the tableaux are described using the graph Γ_n as follows. Vertices of Γ_n are classified to $n+1$ floors. Put

$$P_2(n) = \{\alpha = (\alpha_1, \alpha_2) | \alpha \text{ partition}, \ l(\alpha) \leq 2, \ \alpha_1 + \alpha_2 = n\}$$

The top floor (the n-th floor) of Γ_n has $|P_2(n)|$ vertices which are labeled by the elements of $P_2(n)$ one by one. The bottom floor (the 0-th floor) has a unique vertex labeled by the null partition $\alpha^{(0)} = \emptyset \in P_2(0)$. The i_0-th floor $(1 \leq i_0 < n)$ of Γ_n has $|P_2(i_0)|$ vertices which are labeled by partitions in $P_2(i_0)$ one by one. Two vertices labeled by α and α' respectively are joined by an edge if and only if they are different each other only by one box.

EXAMPLE 4.2. Γ_5 is pictured in Figure 13.

We can get any tableau of shape α from the graph Γ_n as an ascending path from the bottom vertex $\emptyset$ to the top vertex α. Conversely, any ascending path from the bottom vertex to a top vertex α expresses some tableau. We identify each of these paths with the corresponding tableau.

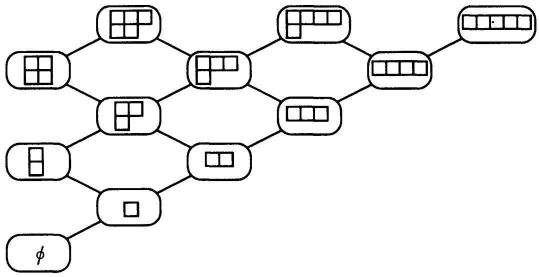


FIGURE 13. Γ_5

As it defined in [**GHJ, KM**], each vertex of Γ_n has its *weight*. These weights are defined by the partitions $\{\lambda\}$ which are assigned to the vertices. Let $\lambda = (\lambda_1, \lambda_2)$ be a partition of the length at most 2. Put $l = \lambda_1 - \lambda_2$ and $n = \lambda_1 + \lambda_2$. Then the weight $s[\lambda]$ of λ is defined by

$$s[\lambda] = \prod_{(i,j)\in\lambda} \frac{[j-i+2]}{[h_\lambda(i,j)]} = [l+1].$$

In the following we fix a partition $\alpha = (\alpha_1, \alpha_2)$ of the length at most 2. Suppose that $\alpha_1 - \alpha_2 = l$ and $\alpha_1 + \alpha_2 = n$. For the fixed partition α, $V_l(n)$ is the set of all the tableaux whose shapes are α. The objects of $\mathcal{L}_l$ are the $\mathbf{C}$-vector spaces $\{\mathbf{C}V_l(n) | n \in Ob(\mathcal{J})\}$. If $V_l(n) = \emptyset$, then $\mathbf{C}V_l(n) = \{0\}$. We denote the natural basis of $\mathbf{C}V_l(n)$ defined by the tableaux $\{\xi | \xi \in V_l(n)\}$ by $\{v_\xi\}$. The morphisms of $\mathcal{L}_l$ are the linear maps between two objects of $\mathcal{L}_l$ and the composition is the composition of linear maps.

An object n of $\mathcal{J}$ is mapped by $\mathbf{Rep}_l$ to an object $\mathbf{Rep}_l(n) = \mathbf{C}V_l(n)$ of $\mathcal{L}_l$. If either $\mathbf{C}V_l(n)$ or $\mathbf{C}V_l(n')$ is the 0 space, then $Mor_{\mathcal{L}_l}(n, n') = \{0\}$. Hence if either $V_l(n) = \emptyset$ or $V_l(n') = \emptyset$, then $\mathbf{Rep}_l(D) = 0$ for any diagram D such that $\partial_- D = n$ and $\partial^+ D = n'$.

In the following we define the linear map $\mathbf{Rep}_l$ assigning each generator of the Jones category $\mathcal{J}$ to a morphism of $\mathcal{L}_l$.

<u>Definition of $\mathbf{Rep}_l([I_n \tau I_{n'}])$</u>

If $l \geq n + n'$ or $n + n' \not\equiv l \bmod 2$, then define $\mathbf{Rep}_l([I_n \tau I_{n'}]) = 0$.

A generator $[I_n \tau I_{n'}]$ is mapped by $\mathbf{Rep}_l$ to a morphism from the object $\mathbf{C}V_l(n + n')$ to the object $\mathbf{C}V_l(n + 2 + n')$. For each tableau

$$\xi = (\alpha^{(1)}, \ldots, \alpha^{(n-1)}, \alpha^{(n)} = \lambda, \alpha^{(n+1)}, \ldots, \alpha^{(n+n')} = \alpha)$$

of shape α, we define the tableau $\xi(j)$ $(j = 1, 2)$ of shape α as follows:

$$\xi(j) \quad = \quad (\alpha^{(1)}, \ldots, \alpha^{(n-1)}, \lambda, \lambda(j), \lambda_+, \alpha_+^{(n+1)}, \ldots, \alpha_+^{(n+n')} = \alpha_+),$$

where $\{\lambda(j)\}$ $(j = 1, 2)$ are partitions such that $l(\lambda(j)) \leq 2$, $\lambda(j) \supset \lambda$ and $|\lambda(j)| - |\lambda| = 1$ and $\alpha_+^{(i)}$ is the partition of length 2 which is made from $\alpha^{(i)}$ by adding one box to each row. Under these notation $\mathbf{Rep}_l([I_n \tau I_{n'}])$ is defined as follows:

$$\mathbf{Rep}_l([I_n \tau I_{n'}]) v_\xi = \begin{cases} v_{\xi(1)} + v_{\xi(2)} & \text{if } n = 2m, \\ \frac{1}{s[\lambda]}(s[\lambda(1)] v_{\xi(1)} + s[\lambda(2)] v_{\xi(2)}) & \text{if } n = 2m+1. \end{cases}$$

<u>Definition of $\mathbf{Rep}_l([I_n \bar{\tau} I_{n'}])$</u>

If $l > n+n'$ or $n+n' \not\equiv l \bmod 2$, then define $\mathbf{Rep}_l([I_n \bar{\tau} I_{n'}]) = 0$.

A generator $[I_n \bar{\tau} I_{n'}]$ is mapped by $\mathbf{Rep}_l$ to a morphism from the object $\mathbf{C}V_l(n+2+n')$ to the object $\mathbf{C}V_l(n+n')$. For each tableau

$$\xi = (\alpha^{(1)}, \ldots, \alpha^{(n-1)} = \nu, \alpha^{(n)} = \mu, \alpha^{(n+1)}, \ldots, \alpha^{(n+n')} = \alpha)$$

of shape α, if $\alpha^{(n+1)}$ is not the partition obtained from ν by adding one box to each row, then we define

$$\mathbf{Rep}_l([I_n \bar{\tau} I_{n'}]) v_\xi = 0.$$

Otherwise, we put

$$\hat{\xi} = (\alpha^{(1)}, \ldots, \alpha^{(n-1)} = \nu, \alpha_-^{(n+1)}, \ldots, \alpha_-^{(n+n')} = \alpha_-),$$

where $\alpha_-^{(i)}$ is the partition obtained from $\alpha^{(i)}$ by removing one box from each row. Under these notation, we define $\mathbf{Rep}_l([I_n \bar{\tau} I_{n'}]) v_\xi$ as follows.

$$\mathbf{Rep}_l([I_n \bar{\tau} I_{n'}]) v_\xi = \begin{cases} \frac{s[\mu]}{s[\nu]} v_{\hat{\xi}}, & \text{if } n = 2m, \\ v_{\hat{\xi}}, & \text{if } n = 2m+1. \end{cases}$$

References

[ADO] Y. Akutsu, T. Deguchi, and T. Ohtsuki, *Invariants of colored links*, J. of Knot theory and Its Ramifications 1, **2** (1992), 161–184.

[BCHLLS] G. Benkart, M. Chakrabarti, T. Halverson, R. Leduc, C. Lee, and J. Stroomer, *Tensor product representations of general linear groups and their connections with Brauer algebras*, J. Algebra, **166** (1994), 529–567.

[GHJ] F. M. Goodman, P. de la Harpe, and V. F. R. Jones, *Coxeter Graphs and Towers of Algebras*, Springer-Verlag New York, 1989.

[K] M. Kosuda, *The irreducible representations of the Hecke category*, preprint.

[KM] M. Kosuda and J. Murakami, *Centralizer algebras of the mixed tensor representations of quantum group $U_q(gl(n, \mathbf{C}))$*, Osaka J. Math., **30** (1993), 475–507.

[N] Y. A. Neretin, *Extension of representations of the classical groups to representations of categories*, St. Peterburg Math. J., **3** (1992), 147–169.

[O] T. Ohtsuki, *Colored ribbon Hopf algebras and universal invariants of framed links*, J. of Knot theory and Its Ramifications 2, *2* (1993), 211–232.

[S] J. R. Stembridge, *Rational tableaux and the tensor algebra of gl_n*, J. Combin. Theory, *A46* (1987), 79–120.

[T] V. G. Turaev, *Operator invariants of tangles and R-matrices*, Math. USSR Izvestiya, **35** (1990), 411–444.

[Y] Y. Yoshioka, *Representation of the Jones category (in japanese)*, Master thesis (Osaka Univ.), February 1993.

Department of Mathematical Sciences, University of the Ryukyus, Nishihara-cho Okinawa 903-0213, Japan

E-mail address: `kosuda@math.u-ryukyu.ac.jp`

This page intentionally left blank

http://dx.doi.org/10.1090/conm/224/03196

Contemporary Mathematics
Volume **224**, 1999

Prounipotent Prolongation of Algebraic Groups

Andy R. Magid

ABSTRACT. G is a linear algebraic group (scheme) over the algebraically closed characteristic zero field k. The kernel UG of the natural map from points of G in one variable formal powers series over k to the k points of G is an inverse limit of unipotent algebraic groups; that is, a *prounipotent* group. This paper considers to what extent G can be recovered from UG. It is shown that the related question for Lie algebras can be answered when the Lie algebra is semi-simple, and from this an answer is derived when G is semi-simple and a linear representation of G over k is specified.

Introduction

In the study of finite p groups, a number of topics become easier to investigate, and some new and intriguing questions arise, through passage to inverse limits to the study of pro-p groups. For example, the existence of free pro-p groups makes possible the study of combinatorial group theory entirely in the (pro) "p" category; free objects like this make cohomology more convenient to study and use; and the new and interesting question about characterizing the (continuously) linear (over $\mathbb{Q}_p$) pro-p groups arises.

Unipotent algebraic groups over an algebraically closed field k of characteristic zero (which will henceforth be assumed to be the complex numbers $\mathbb{C}$) share some formal properties with finite p groups in characteristic p, most notably that k is their unique simple module, and so it should not be surprising that prounipotent groups naturally arise both as a tool and as a source of interesting new questions in the unipotent context also.

A unipotent k group G (remember that $k = \mathbb{C}$) is also a complex analytic group whose Lie algebra $\mathrm{Lie}(G)$ is nilpotent and whose exponential map $\exp : \mathrm{Lie}(G) \to G$ is an analytic bijection whose inverse is denoted log. Because $\mathrm{Lie}(G)$ is nilpotent the Campbell- Baker-Hausdorff formula for $\mathrm{Lie}(G)$ is actually a polynomial map, which means that the algebraic group structure on G, as well as the maps exp and log are canonically algebraic (polynomial). Moreover any analytic homomorphism between unipotent groups is automatically algebraic for the same reason. There are

1991 *Mathematics Subject Classification.* 14L15, 20G20, 22E65.
Key words and phrases. algebraic group, Lie algebra, unipotent, prounipotent.

analytic but not algebraic maps from a unipotent group G to $GL_n(k)$ (for example, $\mathbb{C} \to GL_1(\mathbb{C})$ by $t \mapsto e^t$), but any analytic map from G to a unipotent subgroup of GL_n is necessarily algebraic. A finite dimensional (algebraic) G module V is a finite dimensional k vector space such that the corresponding representation $G \to GL(V)$ is analytic and has range in a unipotent subgroup; in general, a G module is a k vector space which is a direct limit of finite dimensional modules. If V is a G module and if $V \neq 0$ then $V^G \neq 0$.

Prounipotent groups.

A *prounipotent group* G is the limit of an inverse system of unipotent groups with surjective algebraic transition morphisms: $G = \varprojlim(G_i)$ where G_i is unipotent and the maps $G_i \to G_j$ are surjective analytic homomorphisms.

Here are some examples:

EXAMPLE 1. Any unipotent group G is prounuipotent.

EXAMPLE 2. An infinite direct product $\prod_{i\in I} G_i$, where each G_i is unipotent, is a prounipotent group, such as

$$\prod_0^\infty \mathbb{G}_a.$$

EXAMPLE 3. Let $R = k << t_1, \ldots, t_d >>$ be the non-commutative formal power series algebra, let $x_r = 1 + t_r$, $1 \leq r \leq d$, and let M be the maximal ideal of R generated by the t_r. Then $R = \varprojlim(R/M^i)$. Let G_i be the subgroup of the group of units of R/M^i generated by the images of the x_r; G_i is unipotent and the inverse limit $\varprojlim(G_i)$ is a prounipotent subgroup of the group of units of R. We denote the inverse limit $F = F(x_1, \ldots, x_d)$; it is a free prounipotent group on $x_1, \ldots, x_d$. There is a direct construction of F also, which in addition makes sense for infinite sets of generators.

EXAMPLE 4. Proalgebraic groups are inverse limits of algebraic groups, and they have pronuipotent radicals which are prounuipotent groups. For instance, let Γ be a finitely generated group. Take all representations $\rho : \Gamma \to GL(W)$ on a finite dimensional k spaces, and form the product and map

$$P : \Gamma \to \prod_\rho GL(W).$$

The Zariski closure $A(\Gamma)$ of the image of P is a proalgebraic group, and its prounipotent radical $R_uA(\Gamma)$ is a prounipotent group. When Γ is free, $R_uA(\Gamma)$ is a free prounipotent group (on an infinite set).

EXAMPLE 5. $GL_n(k[[t]]) = \{\sum_{i\geq 0} A_i t^t \mid A_0 \in GL_n(k)\}$.
Let $UGL_n = \mathrm{Ker}(GL_n(k[[t]]) \to GL_n(k))$. If $UGL_n, i = \mathrm{Ker}(GL_n(k[[t]]/t^{i+1}) \to GL_n(k))$ then it is clear that $UGL_n = \varprojlim(UGL_n, i)$. We will see in the next section why UGL_n, i is unipotent and hence why UGL_n is unipotent.

The groups in Example 5 are a model for a general class of prounipotent groups associated to affine (eventually semisimple) algebraic groups which will be discussed at length below.

Because of Example 3 (free prounipotent groups), we can construct a combinatorial group theory for prounipotent groups, including presentations by generators and relations. In particular we can talk about the (minimal) number of generators and relations for a prounipotent group, usually denoted d and r, respectively as the minimal number of generators of a free prounipotent group mapping onto the given prounipotent group. Modules for a prounipotent group $G = \varprojlim(G_i)$ are direct limits of G_i modules. Thus k is the only simple G module. The category of G modules has enough injectives (in fact, the coordinate ring $k[G]$ is the injective hull of k) and so one can construct injective resolutions and cohomology, in particular $\mathrm{Ext}^i_G(V, W)$ for any G modules V, W, using an injective resolution of W. We define $H^i(G, W) = \mathrm{Ext}^i(k, W)$ and then talk about the cohomological dimension of G (the smallest integer n for which $H^i(G, W) = 0$ for all W and all $i > n$), and it turns out that the prounipotent groups of cohomological dimension one are precisely the free ones. From this it follows that subgroups of free prounipotent groups are free and that we can calculate the number of generators d of G as the dimension of $H^1(G, k)$ and the number of relations r as the dimension of $H^2(G, k)$. For unipotent groups it even turns out that $r > \frac{d^2}{4}$, except for the special cases when $G = \mathbb{G}_a$ ($d = 1$ and $r = 0$) and when $G = \mathbb{G}_a \times \mathbb{G}_a$ ($d = 2$ and $r = 1$).

For any prounipotent group G, we define the closed lower central series by:

1. $C^1G = G$
2. $C^{i+1}G = \overline{(G, C^iG)}$ (Zariski closure) for $i > 1$

G is finitely generated if and only if the abelian prounipotent group C^1G/C^2G is finite dimensional, and if it is then $C^{i+1}G = (G, C^iG)$ for all i. In other words, the closed lower central series conincides with the lower central series.

We define the Lie algebra of the prounipotent group G to be the left G invariant derivations of the coordinate ring: $\mathrm{Lie}(G) = \mathrm{Der}_G(k[G])$. It follows that if $G = \varprojlim(G_i)$ then $\mathrm{Lie}(G) = \varprojlim(\mathrm{Lie}(G_i))$. In particular, $\mathrm{Lie}(G)$ is *pronilpotent.*

For any pronilpotent Lie algebra L, we define the closed lower central series by:

1. $\mathcal{C}^1L = L$
2. $\mathcal{C}^{i+1}L = \overline{[L, \mathcal{C}^iL]}$ (Zariski closure) for $i > 1$

If G is finitely generated, then so is L (in the pronilpotent category) and for all i $\mathcal{C}^iL = [L, \mathcal{C}^{i-1}L] = \mathrm{Lie}(C^iG)$.

Continue to assume that G is finitely generated. As with any group, the direct sum

$$\oplus_{i\geq 1} C^iG/C^{i+1}G$$

is a Lie algebra, the Lie bracket coming from the commutator in G.

Here, we will want to look at the direct product

$$\hat{gr}(G, C^iG) = \prod_{i\geq 1} C^iG/C^{i+1}G$$

which is a pronilpotent Lie algebra.

Similarly, for any finitely generated ptonilpotent Lie algebra L we have the associated graded pronilpotent Lie algebra

$$\hat{gr}(L, \mathcal{C}^iL) = \prod_{i\geq 1} \mathcal{C}^iL/\mathcal{C}^{i+1}L.$$

Then it turns out that there is an isomorphism $\hat{gr}(L, \mathcal{C}^iL) \cong \hat{gr}(G, C^iG)$.

More generally, if $G = G^1 \geq G^2 \geq \dots$ is a normal series (of closed subgroups of G) with $(G^i, G^j) \leq G^{i+j}$ for all i, j then we can form the Lie algebra

$$\hat{gr}(G, G^i) = \prod_{i \geq 1} G^i/G^{i+1}$$

using the commutator for bracket. If $L^i = \mathrm{Lie}(G^i)$ then we also have an associated graded pronilpotent Lie algebra

$$\hat{gr}(L, L^i) = \prod_{i \geq 1} L^i/L^{i+1}$$

and an isomorphism $\hat{gr}(L, L^i) \cong \hat{gr}(G, G^i)$.

For the material in this section, see the references [**LM1, LM2,LM3,LM4**] and [**M3**].

Linearity.

A pro–p group G is linear if it can be continuously embedded in $GL_n(\mathbb{Z}_p)$. If it has a linear subgroup H of finite index then representation can be induced from H to G to see that G is linear; a "virtually linear" group is linear. A pro–p group is *powerful* if the (closed) subgroup G^p generated by p^{th} powers contains the commutator subgroup; that is $G^p \geq (G, G)$. [**DDMS**] proved that powerful pro–p groups are linear, more precisely, that virtually powerful pro–p groups are linear (everything here is finitely generated in the pro–p category).

One can consider a similar question for prounipotent groups, or equivalently for a pronilpotent Lie algebra L, with $k[[t]]$ taking the place of $\mathbb{Z}_p$. There is no natural analogue of the p power operation, so something like the following is required:

Suppose that L is finitely generated in the pronilpotent category and that there is $\tau \in \mathrm{End}_k(L)$ such that:

1. $\tau[x, y] = [x, \tau y]$ for all $x, y \in L$;
2. $\cap_{i \geq 0} \tau^i L = 0$;
3. $\tau L \supseteq [L, L]$.

Then [**N**] there is an ideal I of finite codimension in L and an embedding

$$I \to \mathfrak{gl}_n(k[[t]]).$$

The embedding takes values in the pronilpotent subalgebra $tM_n(k[[t]])$.

Thus pronilpotent Lie algebras with a suitable "t" operator are virtually (in the sense of finite codimension) linear. On the other hand, it is known that there are pronilpotent Lie algebras L which have finite codimemsion ideals I such that I is linear and L is not [**M1**]. (Note that this is much stronger than saying that there is a representation of I finite dimensional over $k[[t]]$ which does not induce to a representation of L finite dimensional over $k[[t]]$.)

Linearity for prounipotent groups, or equivalently for pronilpotent Lie algebras, is thus more complicated than for pro–p groups. We turn then to the apparently simpler question of starting with known linear prounipotent groups. We have an obvious construction of such groups analogous to Example 5 above, to which we now turn.

Prounipotent prolongations of groups and Lie algebras

In this section, we are going to define some generalizations of Example 5 above.

DEFINITION 1. Let H be an affine algebraic group over k. The *prounipotent prolongation* UH of H is the kernel of $H(k[[t]]) \to H(k)$ induced from $k[[t]] \to k$ by $t \mapsto 0$.

We will check below that UH is indeed prounipotent. H is not, of course, a homomorphic image of UH (for example H could be reductive, and all finite dimensional images of UH are unipotent). The main point of this work is to investigate the question of to what extent UH determines H.

If a faithful representation $H \leq GL_n$ is selected then there is a commutative diagram:

$$(*)\qquad \begin{array}{ccccccccc} 1 & \longrightarrow & UGL_n & \longrightarrow & GL_n(k[[t]]) & \longrightarrow & GL_n(k) & \longrightarrow & 1 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 1 & \longrightarrow & UH & \longrightarrow & H(k[[t]]) & \longrightarrow & H(k) & \longrightarrow & 1 \end{array}$$

There is also a related construction for Lie algebras.

DEFINITION 2. Let L_0 be a finite dimensional Lie algebra over k. Then $\mathcal{U}L_0$ denotes the k Lie algebra $\prod_1^\infty L_0 t^i$ where Lie product is definied by $[xt^i, yt^j] = [x,y]t^{i+j}$ for $x, y \in L_0$.

We will see that $\mathcal{U}L_0$ is pronilpotent and, for H affine, discuss the relation between UH and $\mathcal{U}\mathrm{Lie}(H)$ below.

As with the groups, L is not, of course, a homomorphic image of $\mathcal{U}L_0$ (for example L_0 could be simple, and all finite dimensional images of $\mathcal{U}L_0$ are nilpotent). We will investigate the question of to what extent $\mathcal{U}L_0$ determines L_0.

We intend to address the basic questions:

1. Does UH and the representation $UH \to UGL_n$ determine H?
2. Does UH determine H?
3. Does $\mathcal{U}L_0$ determine L_0?

The first step will be to set up the foundations for the construction of UH.

Higher codual numbers.

Let B be any commutative k algebra. We want to consider the functor from commutative k algebras to sets given by

$$A \mapsto \mathrm{Alg}_k(B, A[t]/t^{m+1}).$$

If this functor is representable, we denote the representing algebra $B[m]$ (so $\mathrm{Alg}_k(B[m], A) = \mathrm{Alg}_k(B, A[t]/t^{m+1})$ for all A). If $m = 1$ then $A[t]/t^2$ is the dual numbers over A, so we call $B[1]$ the codual numbers over B and in general refer to the algebras $B[m]$ as *higher codual numbers.* Of course $B \mapsto B[m]$ is, technically speaking, the adjoint to the functor $A \mapsto A[t]/t^{m+1}$, so that $B[1]$ is adjoint to the dual numbers functor.

A k algebra homomorphism

$$\phi : B \to A[t]/t^{m+1} = A + A\bar{t} + A\bar{t}^2 + \cdots + A\bar{t}^m$$

where

$$\phi(f) = \phi_0(f) + \phi_1(f)\bar{t} + \cdots + \phi_1(f)\bar{t}^m$$

has the properties that

1. $\phi_i : B \to A$ is k linear; and
2. $\phi_i(bc) = \sum_{p+q=i} \phi_p(b)\phi_q(c)$.

Thus to define $B[m]$ we need an object universal for maps meeting the above two conditions. Note that the condition on ϕ_0 is that it be a k algebra morphism.

The symmetric algebra $S_k(B)$ is universal for k linear maps from B and thus $B \otimes S_k(B)^{\otimes m}$ is universal for one algebra and m k linear maps: explicitly, there is a bijection

$$\mathrm{Alg}_k(B \otimes S_k(B)^{\otimes m}, A) \to \mathrm{Alg}_k(B, A) \times \mathrm{Hom}_k(B, A) \cdots \times \mathrm{Hom}_k(B, A)$$

by

$$\Phi \mapsto (\phi_0, \phi_1, \ldots, \phi_m)$$

where

$$\phi_i(b) = \Phi(1 \otimes \cdots \otimes be_i \otimes \cdots \otimes 1).$$

Here we write be_i to denote $b \in S_k^1(B) \subset S_k(B)$ for for $i \geq 1$ and we let $e_0 = 1 \in B$.

Then

$$\phi_i(bc) = \Phi(1 \otimes \cdots \otimes bce_i \otimes \cdots \otimes 1)$$

and

$$\sum_{p+q=i} \phi_p(b)\phi_q(c) = \sum_{p+q=i} \Phi(1 \otimes \cdots \otimes be_p \otimes \cdots \otimes 1)\Phi(1 \otimes \cdots \otimes ce_q \otimes \cdots \otimes 1)$$
$$= \Phi(\sum_{p+q=i} (1 \otimes \cdots \otimes be_p \otimes \cdots \otimes ce_q \otimes \cdots \otimes 1).$$

We let I_m be the ideal of $B \otimes S_k(B)^{\otimes m}$ generated by all

$$1 \otimes \cdots \otimes bce_i \otimes \cdots \otimes 1 - \sum_{p+q=i} (1 \otimes \cdots \otimes be_p \otimes \cdots \otimes ce_q \otimes \cdots \otimes 1)$$

for all $b, c \in B$.

Then we have

PROPOSITION 3. *$B[m] = B \otimes S_k(B)^{\otimes m}/I_m$ represents the functor*

$$A \mapsto Alg_k(B, A[t]/t^{m+1}).$$

where $\Phi : B \to A[t]/t^{m+1}$ by $\Phi(b) = \sum \phi_i(b)\bar{t}^i$ corresponds to $F : B[m] \to A$ defined by $F(b_0e_0 \otimes \cdots \otimes b_me_m) = \prod \phi_i(b_i)$ and $G : B[m] \to A$ corresponds to $\Psi : B \to A[t]/t^{m+1}$ by $\Psi(b) = \sum G(1 \otimes \cdots \otimes be_i \otimes \cdots \otimes 1)\bar{t}^i$

Of course the association $B \mapsto B[m]$ is functorial: if $f : B \to C$ is a k algebra homomorphism then the corresponding map $B[m] \to C[m]$ is induced from $b_0 \times b_1e_1 \otimes \cdots \otimes b_me_m \mapsto f(b_0) \times f(b_1)e_1 \otimes \cdots \otimes f(b_m)e_m$. Note that this implies that if f is surjective then so is $f[m]$.

For any B, we have $B[0] = B$ and for k we have $k[m] = k$ for all m.

We have been using e_i to denote $1 \in B = S_k^1(B)$ in the i^{th} tensor factor in $B \otimes S_k(B)^{\otimes m} = B \otimes_k S(Be_1) \otimes_k \cdots \otimes_k S(Be_m)$. Using the fact that tensor products of symmetric algebras of modules are symmetric algebras of the direct sums of the modules, and that scalar extensions of symmetric algebras of modules are symmetric algebras of the scalar extension of the module, we have

$$B \otimes S_k(B)^{\otimes m} = S_B(B \otimes_k (Be_1 \oplus \dots Be_n))$$

and we write this latter in the notation $B[Be_1, \dots, Be_m]$. Then we write $B[m] = B[Be_1, \dots, Be_m]/I_m = B[x_1(B), \dots, x_m(B)]$, writing $x_i(b)$ for $be_i + I_m$ (including $i = 0$), so that

1. $x_i(ab) = ax_i(b)$ for $a \in k$ and $b \in B$;
2. $x_i(b + c) = x_i(b) + x_i(c)$ for $b, c \in B$; and
3. $x_i(bc) = \sum_{p+q=i} x_p(b)x_q(c)$ for $b, c \in B$.

We are going to retain the notation $x_0(b)$, even though we can identify $x_0(b)$ and b. (More formally, this would be the identification of B and $B[0]$, which can be made consistently for all m via the obvious maps $B[0] \to B[m]$.)

From Proposition 3, the identity map $B[m] \to B[m]$ corresponds to the map $B[m] \to B[m][t]/t^{m+1}$ by $b \mapsto \sum(1 \otimes \cdots \otimes be_i \otimes \cdots \otimes 1)\bar{t}^i$, which we can now translate as $b \mapsto \sum x_i(b)\bar{t}^i$. Similarly, a map $f : B \to A[t]/t^{m+1}$ by $f(b) = \sum f_i(b)\bar{t}^i$ corresponds to the map $F : B[m] \to A$ determined by $F(x_i(b)) = f_i(b)$.

We will use this notation to establish two other basic facts about the higher codual number construction.

PROPOSITION 4. *Suppose $t_1, \dots, t_s$ generate B as a k algebra. Then $\{x_i(t_j) \mid 0 \le i \le m, \quad 1 \le j \le s\}$ generates $B[m]$ as a k algebra.*

PROOF. Clearly $\{x_i(b) \mid b \in B, \quad 0 \le i \le m\}$ generates $B[m]$ as a k algebra. By the k linearity of the x_i, it will be sufficient to prove that for any monomial M in the t_i's, $x_i(M)$ belongs to the subalgebra B' of $B[m]$ generated over k by all $x_i(t_j)$. This is seen by induction on the length $\ell(M)$ of the monomial M: for $\ell(M) = 1$ (that is, $M = t_j$ some j) $x_i(M) \in B'$ by definition. Suppose $x_i(M) \in B'$ for all all monomials of length r, and let M have length $r + 1$. Then $M = M_0t_j$ for some j and some M_0 with $\ell(M_0) = r$, and then $x_i(M) = \sum_{p+q=i} x_p(M_0)x_q(t_j)$ belongs to B' by induction.

As an example of Proposition 4, w can consider the case of a polynomial ring $B[y]$. It follows from the proposition that $B[y][m]$ is generated over $B[m]$ by $x_i(y)$, $0 \le i \le m$. And it is clear that the $x_i(y)$ are algebraically independent over $B[m]$ by considering the B algebra homomorphism $B[y] \mapsto B[y_0, \dots, y_m][t]/t^{m+1}$ by $y \mapsto \sum y_i\bar{t}^i$. Thus we have

COROLLARY. *For polynomial rings, $B[y][m] = B[x_0(y), \dots x_m(y)]$.*

We also record here the situation with localization by a single element: if f is a non-zero divisor in B then mapping $B[f^{-1}]$ to $A[t]/t^{m+1}$ means mapping B in such a way that f goes to a unit. If $\Phi : B[m] \to A$ corresponds to $\phi : B \to A[m]/t^{m+1}$ and $\phi(f) = \sum \phi_i(f)\bar{t}^i$ then $\Phi(x_i(f)) = \phi_i(f)$ and in $A[t]/t^{m+1}$ $\phi(f)$ is a unit if and only if $\phi_0(f)$ is a unit of A. Thus we have the following formula:

$$B[f^{-1}][m] = B[m][x_0(f)^{-1}].$$

PROPOSITION 5. *Let J be an ideal of B and suppose J is generated by $\{b_\alpha \mid \alpha \in \mathcal{A}\}$. Let $J[m]$ be the ideal of $B[m]$ generated by $\{x_i(b_\alpha) \mid 0 \leq i \leq m, \quad \alpha \in \mathcal{A}\}$. Then*

$$(B/J)[m] = B[m]/J[m].$$

PROOF. Let A be a k algebra. $\mathrm{Alg}_k((B/J)[m], A) = \mathrm{Alg}_k(B/J, A[t]/t^{m+1}) = \{f \in \mathrm{Alg}_k(B, A[t]/t^{m+1}) \mid f(J) = 0\}$. Now $f : B \to A[t]/t^{m+1}$ is given by $F : B[m] \to A$ where $f(b) = \sum F(x_i(b))\bar{t}^i$ so that $f(J) = 0$ if and only if $F(x_i(b)) = 0$ for all $b \in J$ and $0 \leq i \leq m$. Thus the kernel of F must contain $\{x_i(b_\alpha) \mid 0 \leq i \leq m, \quad \alpha \in \mathcal{A}\}$. And if it does contain this set, and if $b = \sum a_\alpha b_\alpha$ belongs to J then since

$$x_i(b) = \sum_\alpha x_i(a_\alpha b_\alpha) = \sum_{\alpha, p+q=i} x_p(a_\alpha) x_q(b_\alpha)$$

$F(x_i(b)) = 0$. It follows that $f(J) = 0$ if and only if $F(J[m]) = 0$, and hence that $B[m]/J[m]$ represents the same functor as $(B/J)[m]$, and the proposition follows.

As noted above, the higher codual numbers functors are adjoint functors, from which it follows trivially that they preserve algebra coproducts, and that iterations may be done in any order, facts which we now record:

PROPOSITION 6. *Let B_1 and B_2 be k algebras and m_1 and m_2 positive integers. Then*

1. *$(B_1 \otimes_k B_2)[m]$ is naturally isomorphic to $B_1[m] \otimes_k B_2[m]$; and*
2. *$(B[m_1])[m_2]$ is naturally isomorphic to $(B[m_2])[m_1]$.*

PROOF.

$$\begin{aligned} \mathrm{Alg}_k((B_1 \otimes_k B_2)[m], A) &= \mathrm{Alg}_k(B_1 \otimes_k B_2, A[t]/t^{m+1}) \\ &= \mathrm{Alg}_k(B_1, A[t]/t^{m+1}) \times \mathrm{Alg}_k(B_2, A[t]/t^{m+1}) \\ &= \mathrm{Alg}_k(B_1[m], A) \times \mathrm{Alg}_k(B_2[m], A) \\ &= \mathrm{Alg}_k(B_1[m] \otimes_k B_2[m], A), \end{aligned}$$

which proves the first assertion.

$(A[t]/t^{m_1+1})[s]/s^{m_2+1}$ is naturally isomorphic to $(A[s]/s^{m_2+1})[t]/t^{m_1+1}$ so that

$$\begin{aligned} \mathrm{Alg}_k((B[m_1])[m_2], A) &= \mathrm{Alg}_k((B, (A[t]/t^{m_1+1})[s]/s^{m_2+1}) \\ &= \mathrm{Alg}_k((B, (A[s]/s^{m_2+1})[t]/t^{m_1+1}) \\ &= \mathrm{Alg}_k((B[m_2])[m_1], A). \end{aligned}$$

We can be explict about the isomorphism $(B_1 \otimes_k B_2)[m] \to B_1[m] \otimes_k B_2[m]$: in terms of elements, we have $x_i(b \otimes c) \mapsto \sum_{p+q=i} x_p(b) \otimes x_q(c)$.

Finally, we consider the relation among the higher codual numbers $B[m]$ for different values of m. If $m_1 > m_2$ there is a canonical homomorphism, natural in A, $A[t]/t^{m_1+1} \to A[t]/t^{m_2+1}$ and hence a map, natural in A,

$$\begin{aligned} &\mathrm{Alg}_k(B[m_1], A) = \mathrm{Alg}_k(B, A[t]/t^{m_1+1}) \to \\ &\qquad\qquad \mathrm{Alg}_k(B, A[t]/t^{m_2+1}) = \mathrm{Alg}_k(B[m_2], A) \end{aligned}$$

which must come from a unique k algebra map $B[m_2] \to B[m_1]$. It follows that $\{B[i] \mid i \geq 0\}$ forms a direct system. Using these, we can define the infinitely high codual numbers as $B[\infty] = \varinjlim(B[m])$, and we then have

PROPOSITION 7. $B[\infty]$ *represents the functor*

$$A \mapsto Alg_k(B, A[[t]]).$$

PROOF. Since $A[[t]] = \varprojlim(A[t]/t^{m+1})$,

$$\begin{aligned}\mathrm{Alg}_k(B, A[[t]]) &= \varprojlim \mathrm{Alg}_k(B, A[t]/t^{m+1}) \\ &= \varprojlim \mathrm{Alg}_k(B[m], A) \\ &= \mathrm{Alg}_k(\varinjlim B[m], A) \\ &= \mathrm{Alg}_k(B[\infty], A).\end{aligned}$$

Jet bundle schemes.

DEFINITION. Let $\mathcal{X} = \mathrm{Spec}(B)$ be an affine k scheme. We let $\mathcal{X}[m]$, $0 \leq m \leq \infty$ denote the affine k scheme $\mathrm{Spec}(B[m])$. We call $\mathcal{X}[m]$ the *m jet bundle* of $\mathcal{X}$. If X is an affine k variety we let $X[m]$ denote $\mathrm{Spec}(k[X])[m](k)$, calling it the *m jet bundle* also. If $\phi : \mathcal{X} \to \mathcal{Y}$ is a morphism of schemes, then there is a corresponding morphism $\phi[m] : \mathcal{X}[m] \to \mathcal{Y}[m]$ and if $f : X \to Y$ is a morphism of varieties, then there is a corresponding morphism $\phi[m] : X[m] \to Y[m]$

Note that $\mathcal{X}[0] = \mathcal{X}$, and that $\mathcal{X}[1]$ is the tangent bundle of $\mathcal{X}$. If X is an affine variety (so that $k[X]$ is finitely generated over k) then for finite m, by Proposition 4, $X[m]$ is an affine variety with $k[X[m]] = k[X][m]/\sqrt{0}$.

Now suppose G is an affine algebraic group over k. $A \mapsto \mathrm{Alg}_k(k[G], A[t]/t^{m+1})$ is a group valued functor, and it follows that $k[G][m]$ is a (cocommutative) Hopf algebra over k, and in particular reduced, from which it follows that $G[m]$ is an affine algebraic group over k (proaffine if $m = \infty$) with $k[G[m]] = k[G][m]$. As in the remarks following Proposition 6, we can be explicit about the comultiplication in $k[G[m]]$: if $\gamma : k[G] \to k[G] \otimes k[G]$ is the comultiplication, and $\gamma(b) = \sum b_{(1)} \otimes b_{(2)}$ then $k[G][m] \to k[G][m] \otimes k[G][m]$ is given by

$$x_i(b) \mapsto \sum_{p+q=i} \sum x_p(b_{(1)}) \otimes x_q(b_{(2)}).$$

If $\varepsilon : k[G] \to k$ is the augmentation, then the augmentation $\varepsilon[m] : k[G][m] \to k[m] = k$ is given by $\varepsilon[m](x_i(b)) = x_i(\varepsilon(b))$, and this latter is 0 for $i > 0$. Thus it follows that the augmentation ideal $I(G[m]) = \mathrm{Ker}(\varepsilon[m])$ contains $\{x_i(b) \mid b \in I(G) = \mathrm{Ker}(\varepsilon), 0 \leq i \leq m\}$. So $I(G[m]) \supseteq I(G)[m]$; since by Proposition 5 $k[G][m]/I(G)[m] = (k[G]/I(G))[m]$ and this latter is $k[m] = k$ we have $I(G[m]) = I(G)[m]$.

It is instructive to look more closely at the examples of $G = GL_n$ and $G = SL_n$

EXAMPLE GL. Fix n, and let $k[GL_n] = k[t_{ij}][\det^{-}1]$. As noted in the corollary to and discussion before Proposition 4, it follows that

$$k[GL_n[m]] = k[\{x_p(t_{ij}) \mid 0 \leq p \leq m, 1 \leq i,j \leq n\}][x_0(det)^{-1}].$$

Here $\{x_p(t_{ij}) \mid 0 \leq p \leq m, \quad 1 \leq i,j \leq n\}$ is a set of mn^2 indeterminates over k.

If we interpret k points as morphisms $k[GL_n[m]] \to k$, we can identify k points as follows:

$$GL_n[m](k) \to GL_n(k[t]/t^{m+1}), \quad \alpha \mapsto [\sum_p \alpha(x_p(t_{ij}))].$$

Since comultiplication in $k[GL_n]$ is given by $t_{ij} \mapsto \sum_k t_{ik} \otimes t_{kj}$, we have comultiplication in $k[GL_n][m]$ given by

$$x_p(t_{ij}) \mapsto \sum_k \sum_{r+s=p} x_r(t_{ik}) \otimes x_s(t_{kj})$$

and $x_0(\det)^{-1} \mapsto x_0(\det)^{-1} \otimes x_0(\det)^{-1}$.

Augmentation maps $x_p(t_{ij})$ to $\delta_{0p}\delta_{ij}$ (and therefore $x_0(\det)$ to 1). Antipode formulas may also be determined (which we omit here).

EXAMPLE SL. Fix n, and let $k[SL_n] = k[GL_n]/(\det - 1)$. By Proposition 5, $k[SL_n][m] = k[GL_n][m]/(x_0(\det - 1), \ldots, x_m(\det - 1))$. For $i > 0$, we have $x_i(\det - 1) = x_i(\det)$, and $x_0(\det - 1) = x_0(\det) - 1$. The image of $k[SL_n] = k[SL_n][0]$ in $k[SL_n][m]$ is $k[GL_n][0]/(x_0(\det) - 1)$, so we end up with

$$k[SL_n][m] = k[SL_n][\{x_p(t_{ij}) \mid 1 \leq p \leq m, 1 \leq i,j \leq n\}]/(x_1(\det), \ldots, x_m(\det)).$$

We further recall that to construct the kernel of a morphism $f : G \to H$ of affine algebraic groups, we identify $\mathrm{Ker}(f)$ and $G \times_H \{e\}$, so that $k[\mathrm{Ker}(f)] = k[G]/f^*(I(H))k[G]$, where $I(H)$ is the augmentation ideal of $k[H]$. We can use this to see Lie algebras.

EXAMPLE $\mathrm{LIE}(G[m])$. If H is any affine k group, we have the *group* $\mathrm{Lie}(H)$ as the kernel of $H[1] \to H[0] = H$. Thus

$$k[\mathrm{Lie}(H)] = k[H[1]]/x_0(I(H))k[H[1]].$$

Since $k[H[1]] = k[H][1]$ is generated over k by $\{x_0(b), x_1(b) \mid b \in k[H]\}$, and $x_0(b) - b(e) \in x_0(I(H))k[H[1]]$, it follows that the images $y(b) = x_1(b) + x_0(I(H))k[H[1]]$ generate $k[\mathrm{Lie}(H)]$. Since $x_1(bc) = x_0(b)x_1(c) + x_1(b)x_0(c)$, we also have $y(bc) = b(e)y(c) + y(b)c(e)$. Moreover, these are the only relations, so if $b_1, \ldots, b_s$ give a basis of $I(H)/I(H)^2$, then $k[\mathrm{Lie}(H)]$ is the polynomial algebra on $y(b_1) \ldots y(b_s)$

Applying these formulas to $H = G[m]$ we have that $k[\mathrm{Lie}(G[m])]$ is generated over k by elements $y(x_p(b))$; as above, if we select elements giving a basis of $I(G[m])/I(G[m])^2$ we get polynomial generators over k. In addition, since $I(G[m]) = I(G)[m]$, if $b_1, \ldots, b_r$ generate the ideal $I(G)$ then $\{y(x_p(b_i)) \mid 1 \leq i \leq r, 0 \leq p \leq m\}$ generate $k[\mathrm{Lie}(G[m])]$.

Applied to $G = GL_n$, this gives that

$$k[\mathrm{Lie}(GL_n[m])] = k[\{y(x_p(t_{ij})) \mid 1 \leq i,j \leq n, 0 \leq p \leq m\}]$$

and hence an identification

$$\mathrm{Lie}(GL_n[m])(k) \to M_n(k[t]/t^{m+1}) \quad \beta \mapsto [\sum_p \beta(y(x_p(t_{ij})].$$

Computing $\mathrm{Lie}(SL_n[m])(k)$ is a bit more complicated: it follows from the calculation of $k[SL_n[m]]$ above that

$$k[\mathrm{Lie}(SL_n[m])] = \\ k[\{y(x_p(t_{ij})) \mid 1 \leq i, j \leq n, 0 \leq p \leq m\}]/(y(x_0(\det)), \ldots y(x_m(\det))).$$

To compute $y(x_p(\det))$, we first consider a permutation σ and the monomial

$$m = t_{1\sigma(1)} \ldots t_{n\sigma(n)}.$$

and apply x_p to get

$$x_p(m) = \sum x_{q_1}(t_{1\sigma(1)}) \ldots x_{q_n}(t_{n\sigma(n)})$$

and then apply y and use the fact that $t_{ij}(e) = \delta_{ij}$ to see that $y(x_p(m)) = 0$ unless $\sigma(i) = i \ \forall i$, in which case

$$y(x_p(x_{11} \ldots x_{nn})) = \sum_i y(x_p(t_{ii})).$$

We conclude that

$$k[\mathrm{Lie}(SL_n[m])] \\ = k[\{y(x_p(t_{ij})) \mid 1 \leq i, j \leq n, 0 \leq p \leq m\}]/(\sum_i y(x_0(t_{ii}), \cdots \sum_i y(x_m(t_{ii})).$$

Above, we identified $\mathrm{Lie}(GL_n)(k)$ and $M_n(k[t]/t^{m+1})$. We can write this latter as $\{\sum A_i \bar{t}^i \mid A_i \in M_n(k)\}$. We these identifications, we can then write the above as

$$\mathrm{Lie}(SL_n)(k) = \{\sum A_i \bar{t}^i \in \mathrm{Lie}(GL_n)(k) \mid \mathrm{trace}(A_i) = 0\}.$$

In the above calculations and examples, the case $m = \infty$ follows from the case of finite m by passage to the direct limit.

Finally, we have the relation between infinite jet bundle groups and prounipotent prolongations:

LEMMA 8. *Let G be an affine algebraic group over k. Then there is an isomorphism*

$$Lie(G) = Ker(G[1] \to G) \cong Ker(G[m+1] \to G[m])$$

for all finite m.

PROOF. Let $\alpha \in \mathrm{Ker}(G[m+1] \to G[m]) = G[m+1] \times_{G[m]} \{e\}$. With the identification $G[i] = G[i](k) = \mathrm{Alg}_k(k[G], k[t]/t^{m+1})$, we have the commutative diagram

$$\begin{tikzcd} k[G] \arrow[r, "\alpha"] \arrow[d, "\epsilon"] & k[t]/t^{m+2} \arrow[d] \\ k \arrow[r] & k[t]/t^{m+1} \end{tikzcd}$$

so that α is given by $b \mapsto \alpha_0(b) + \alpha_{m+1}(b)\bar{t}^{m+1}$. Define $\kappa(\alpha) : k[G] \to k[t]/t^2$ by $b \mapsto \alpha_0(b) + \alpha_{m+1}(b)\bar{t}$. Then $\alpha \mapsto \kappa(\alpha)$ is the desired isomorphism.

Of course the vector group $\mathrm{Lie}(G)$ is unipotent. By repeated application of Lemma 8, we then conclude the following:

COROLLARY 9. *Let G be an affine algebraic group over k. Then $Ker(G[i] \to G[j])$ (for $i \geq j$) is unipotent for all finite i, j and prounipotent for $i = \infty$, j finite.*

Combining most of the results of this section, we have the following description of prounipotent prolongations:

THEOREM 10. *Let H be an affine algebraic group over k. Then the prounipotent prolongation $UH = Ker(H[\infty] \to H[0])$ of H is prounipotent and has coordinate ring $k[H][\infty]/I(H)k[H][\infty]$. If a representation $H \to GL_n$ is given, and if $\{f_a \mid a \in \mathcal{A}\}$ generates the kernel of restriction $k[GL_n] \to k[H]$ then*

$$k[UH] = \frac{k[\{x_p(t_ij) \mid 1 \leq i, j \leq n, p = 0, 1, 2, \dots\}][det^{-1}]}{(\{x_0(t_{ij}) - \delta_{ij}, x_p(f_a) \mid 1 \leq i, j \leq n, a \in \mathcal{A}, p = 0, 1, 2, \dots\})}$$

Shift Structures

We are concerned in this section with Lie algebras $L = \prod_{i=1}^{\infty} L_i$ where each L_i is finite dimensional and all "isomorphic"; a typical example being $\mathcal{U}(L_0) = \prod_{i=1}^{\infty} L_0 t^i$ (Definition 2). For $a \in L_i$ we will let $a \in L$ denote the infinite tuple whose i^{th} entry is a and all other entries 0. We assume that L is prograded, in the sense that if $a \in L_i$ and $b \in L_j$ then $[a, b] \in L_{i+j}$: in terms of infinite tuples, the Lie product is thus

$$[(a_i)_1^{\infty}, (b_j)_1^{\infty}] = (c_p)_1^{\infty} \quad \text{where} \quad c_p = \sum_{i+j=p} [a_i, b_j].$$

We begin by making clear what is meant by saying that the L_i are "isomorphic":

DEFINITION 11. Let $L = \prod_{i=1}^{\infty} L_i$ where each L_i is a finite dimensional vector space. A *shift structure* on L is a set of linear ismorphims $\phi_i : L_1 \to L_i$, $\forall i$ such that

1. ϕ_1 is the identity.
2. For all $a, b \in L_1$ and all $i, j \geq 1$

$$[\phi_i(a), \phi_j(b)] = \phi_{i+j}(\phi_2^{-1}[a, b]).$$

On $\mathcal{U}(L_0)$, we have a shift structure defined where $\phi_i : L_0 t \to L_0 t^i$ is given by multiplication by t^{i-1}.

We can use a shift structure to construct a Lie structure on L_1.

LEMMA 12. *Let $\phi = \{\phi_i\}$ be a shift structure on $L = \prod_{i=1}^{\infty} L_i$, Define a product on L_1 by $a \cdot_{\phi} b = \phi_2^{-1}[a, b]$. Then L_1 is a Lie algebra under this product.*

PROOF. The product is clearly k bilinear and skew symmetric. For the Jacobi identity, we need to verify that for $a, b, c \in L_1$,

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c + b \cdot (a \cdot c).$$

First, we have, by the Jacobi identity for L, that

$$[\phi_1(a), [\phi_1(b), \phi_1(c)]] = [[\phi_1(a), \phi_1(b)], \phi_1(c)] + [\phi_1(b), [\phi_1(a), \phi_1(c)]]$$

From the definition of the product,

$$[\phi_1(a), [\phi_1(b), \phi_1(c)]] = [[\phi_1(a), \phi_2(b \cdot c)]$$

and then by the definition of shift structure this latter is

$$\phi_3(\phi_2^{-1}[a, b \cdot c]) = \phi_3(a \cdot (b \cdot c)).$$

Similarly,

$$[[\phi_1(a), \phi_1(b)], \phi_1(c)] = \phi_3((a \cdot b) \cdot c)$$

and

$$[\phi_1(b), [\phi_1(a), \phi_1(c)]] = \phi_3(b \cdot (a \cdot c).$$

Since ϕ_3 is a linear isomorphism, the result now follows.

Since $(L_1, \cdot)$ is a finite dimensional Lie algebra, we can form its pronilpotent prolongation; as we now note, the shift structure makes this isomorphic to L.

PROPOSITION 13. *Let $L = \prod L_i$ have a shift structure $\phi = \{\phi_i \mid i = 1, 2, \dots\}$ and let $L_0 = L_1$ with the product $\cdot_\phi$. Then*

$$\mathcal{U}(L_0) \to L \quad by \quad \sum_{i=1}^{\infty} a_i t^i \mapsto (\phi_i(a_i))_{i=1}^{\infty}$$

is a Lie algebra isomorphism

PROOF. The map is a linear bijection. To check that it is a Lie homomorphism, we note that $[a_i t^i, a_j t^j] = (a_i \cdot a_j) t^{i+j} \mapsto \phi_{i+j}(a_i \cdot a_j)$ and by the definition of the Lie product in L_0 this latter is $\phi_{i+j}(\phi_2^{-1}[a_i, b_j])$ which, by the definition of shift structure is $[\phi_i(a_i), \phi_j(a_j)]$.

Because of Proposition 13, in the presence of a shift struture we can assume that $L = \mathcal{U}(L_0)$. As we now see, in case L_0 is its own commutator, the graded structure on $\mathcal{U}(L_0)$ is determined by the Lie structure.

PROPOSITION 14. *Let L_0 be a finite dimensional k Lie algebra and assume that $L_0 = [L_0, L_0]$. Then*

$$\mathcal{C}^n(\mathcal{U}(L_0)) = \sum_{i \geq n} L_0 t^i.$$

Conversely, if $\mathcal{C}^2(\mathcal{U}(L_0)) = \sum_{i \geq 2} L_0 t^i$ then $L_0 = [L_0, L_0]$.

PROOF. Let $L = \mathcal{U}(L_0)$ and let $L^n = \prod_{i \geq n} L_0 t^i$. We want to prove that $\mathcal{C}^n L = L^n$. We begin by showing $\mathcal{C}^n L \subseteq L^n$ by induction on n. The case $n = 1$ follows since both sides are L. Suppose it holds for some m. Then $\mathcal{C}^{m+1} L = [L, \mathcal{C}^m L] \subseteq [L, L^m]$. If $a = \sum_{i \geq 1} a_i t^i \in L$ and $b = \sum_{i \geq m} b_i t^i \in L^m$ then $[a, b] = \sum_p c_p t^p$ where $c_p = \sum_{i+j=p} [a_i, b_j]$. Clearly $\min(i + j) = 1 + m = m + 1$ so $p \geq m + 1$ and $[a, b] \in L^{m+1}$. (Notice that this part of the proof does not require the hypothesis on L_0.)

Next we show that $\mathcal{C}^n L \supseteq L^n$, also by induction on n. Fix a basis $\{x_1, \ldots, x_r\}$ for L_0. The case $n = 1$ again follows since both sides equal L. Suppose the inclusion holds for m. Let $c = \sum_{p \geq m+1} c_p t^p \in L^{m+1}$. Let $A_i = x_i t$ and for each $p \geq m + 1$ select elements $B_{jp} \in k x_j$ such that $\sum_{i,j} [x_j, B_{jp}] = c_p$ (this is possible because $L_0 = [L_0, L_0] = \sum_i [x_i, L_0]$. Let $B_j = \sum_{p \geq m+1} B_{jp} t^{p-1} \in L^m$. Then $\sum_{i,j} [A_i, B_j] = \sum_{i,j} \sum_p [x_i, B_{jp}] t^p = \sum_p \sum_{i,j} [x_i, B_{jp}] t^p = \sum_p c_p t^p = c$. Since $A_i \in L$ and $B_j \in L^m$, we have $c \in [L, L^m] \subseteq [L, \mathcal{C}^m L] = \mathcal{C}^{m+1} L$, completing the proof.

Finally, suppose that $\mathcal{C}^2(\mathcal{U}(L_0)) = \sum_{i \geq 2} L_0 t^i$, and let $a \in L_0$. Since $x = at^2 \in \sum_{i \geq 2} L_0 t^i = [\mathcal{U}(L_0), \mathcal{U}(L_0)]$, we have $y_i = \sum b_{ij} t^j$ and $z_i = \sum c_{ij} t^j$, $1 \leq i \leq N$ such that $x = \sum [x_i, y_i]$ which implies that $a = \sum [b_{i1}, c_{i1}] \in [L_0, L_0]$.

We retain the notation of the proof of Proposition 14 ($L^n = \prod_{i \geq n} L_0 t^i$) for later use.

Since it is clear that the Lie algebras $L^i \subset \mathcal{U}(L_0)$ are finitely generated, in the pronilpotent sense, Proposition 14 implies the same for the lower central series:

COROLLARY. *Let L_0 be a finite dimensional Lie algebra that coincides with its commutator subalgebra, and let $L = \mathcal{U}(L_0)$. Then, for all i $\mathcal{C}^i L$ is finitely generated as a pronilpotent Lie algebra.*

Note that Propositions 13 and 14 actually characterize pronilpotent prolongations, at least in the case of trivial abelianization:

COROLLARY. *Let L_0 be a finite dimensional Lie algebra that coincides with its commutator subalgebra, and let $L = \mathcal{U}(L_0)$. Then:*

1. *$L = \hat{gr}(L, \mathcal{C}^i L)$; and*
2. *$\mathcal{C}^n(\mathcal{U}(L_0)) = L^n$ for all n; and*
3. *L has a shift structure.*

Conversely, any Lie algebra L satisfying (1), (2), (3) is of the form $\mathcal{U}(L_0)$ for some L_0 satisfying $L_0 = [L_0, L_0]$.

The preceding corollary does *not* assert that the Lie algebra L_0 is uniquely determined by $L = \mathcal{U}(L_0)$. It is to that question that we now turn. In the corollary above, the first two conditions are independent of L_0, so we will continue to assume that $L = \prod L_i$ with $\mathcal{C}^i L = L^i$. If $L = \mathcal{U}(L_0) = \mathcal{U}(L_0')$, then it will have shift structures ϕ and ψ coming from L_0 and L_0', respectively. Here's how ϕ and ψ are related:

LEMMA 15. *Let $\phi = \{\phi_i\}$ and $\psi = \{\psi_i\}$ be shift structures on $L = \prod L_i$. Define $A_i : L_1 \to L_1$ by $\psi_i(x) = \phi_i(A_i(x))$. Then*

$$A_i(a) \cdot_\phi A_j(b) = A_{i+j}(a \cdot_\psi b).$$

In particular,

$$a \cdot_\psi b = A_2^{-1}(a \cdot_\phi b)$$

and in the ϕ product on L_1,

$$a \cdot A_r(b) = A_r(a) \cdot b$$

PROOF. $\phi_{i+j}(A_{i+j}(a \cdot_\psi b)) = \psi_{i+j}(a \cdot_\psi b) = \psi_{i+j}\psi_2^{-1}([a,b]) = [\psi_i(a), \psi_j(b)] = [\phi_i(A_i(a)), \phi_j(A_j(b))] = \phi_{i+j}\phi_2^{-1}([A_i(a), A_j(b)]) = \phi_{i+j}(A_i(a) \cdot_\phi A_j(b))$ so $A_{i+j}(a \cdot_\psi b) = A_i(a) \cdot_\phi A_j(b)$. Since $A_1 = I$, applying this last equation to the case $i = j = 1$ gives $A_2(a \cdot_\psi b) = a \cdot_\phi b$ and the cases $(i,j) = (1,r)$ and $(i,j) = (r,1)$ show that both $a \cdot_\phi A_r(b)$ and $A_r(a) \cdot_\phi b$ coincide with $A_{1+r}(a \cdot_\psi b)$.

NOTATION. To use the results of Lemma 15, we will fix the following notation: L_0 denotes the vector space L_1 regarded as a Lie algebra with bracket the ϕ multiplication. We let $P, Q, R \in GL(L_0)$ be the invertible linear transformations $P = A_2$, $Q = A_3A_2^{-1}$ amd $R = P^{-1}$. We denote the ψ Lie multiplication by a center dot. Thus on L_0 we have the formulas

1. $[a, Pb] = Q[a,b] = [Pa, b]$ and
2. $a \cdot b = R[a,b]$.

We are also going to assume that L_0 is semisimple.

We are going to investigate the implications for L_0 of the existence of P and Q, and we will use these to analyze the relations of the two Lie products.

First, we fix a Cartan subalgebra $\mathcal{H}$ in L_0 and we let $x \in \mathcal{H}$ be a regular element so that $\mathcal{H} = \{a \in L_0 \mid [a,x] = 0\}$. If $a \in \mathcal{H}$ then $0 = [a,x]$ so $0 = Q[a,x] = [Pa,x]$ so $P(a) \in \mathcal{H}$. It follows that $P(\mathcal{H}) = \mathcal{H}$. Let $\mathcal{B} \subset \mathcal{H}^*$ be the set of (non-zero) roots and for $\alpha \in \mathcal{B}$ let $x_\alpha \in L_0$ be a corresponding root vector. Any $x \in L_0$ can be uniquely written as $x = h(x) + \sum_{\beta \in \mathcal{B}} \lambda_\beta(x) x_\beta$ where $h(x) \in \mathcal{H}$ and $\lambda_\beta(x) \in k$. For $a \in \mathcal{H}$, $[a, x_\alpha] = \alpha(a)x_\alpha$, so that

$$[P(a), x_\alpha] = \alpha(Pa)x_\alpha.$$

Let $x = P(x_\alpha)$. Then $[a,x] = [a, h(x)] + \sum \lambda_\beta(x)\beta(a)x_\beta$ so that

$$[a, P(x_\alpha)] = \sum \lambda_\beta(P(x_\alpha)\beta(a)x_\beta.$$

Now $[P(a), x_\alpha] = [a, P(x_\alpha)]$, so choosing an $a \in \mathcal{H}$ such that $\beta(a) \neq 0$ all β and comparing the above equations shows that $P(x_\alpha) = k_\alpha + \gamma_\alpha x_\alpha$ for $k_\alpha \in \mathcal{H}$ and scalar γ_α. Now we compute $[x_\alpha, P(x_\beta)] = [P(x_\alpha), x_\beta]$ for $\alpha \neq \beta$

$$[x_\alpha, P(x_\beta)] = [x_\alpha, k_\beta + \gamma_\beta x_\beta] = -\alpha(k_\beta)x_\alpha + \gamma_\beta[x_\alpha, x_\beta];$$

$$[P(x_\alpha), x_\beta] = [k_\alpha + \gamma_\alpha x_\alpha, x_beta] = \beta(k_\alpha)x_beta + \gamma_\alpha[x_\alpha, x_\beta].$$

If $\alpha + \beta \in \mathcal{B}$ (which entails that $\alpha + \beta \neq \alpha, \beta$) $[x_\alpha, x_\beta]$ is a scalar multiple of $x_{\alpha+\beta}$. Otherwise, $[x_\alpha, x_\beta] \in \mathcal{H}$. Thus comparing the above two expressions for $[x_\alpha, P(x_\beta)] = [P(x_\alpha), x_\beta]$ shows that $\beta(k_\alpha) = 0$ for all $\beta \neq \alpha$. Since $[P(x_\alpha), x_\alpha] = Q[x_\alpha, x_\alpha] = 0$, $0 = [k_\alpha + \gamma_\alpha x_\alpha, x_\alpha] = \alpha(k_\alpha)x_\alpha + \gamma_\alpha[x_\alpha, x_\alpha]$ so $\alpha(k_\alpha) = 0$ also. Since $\mathcal{B}$ spans $\mathcal{H}^*$, we have that $k_\alpha = 0$. Thus we have shown that

$$P(x_\alpha) = \gamma_\alpha x_\alpha \quad \gamma_\alpha \neq 0 \quad \forall \alpha \in \mathcal{B}.$$

($\gamma_\alpha \neq 0$ since P is invertible.)

If $L(\alpha) \subset L_0$ denotes the root space corresponding to α, (which is spanned by x_α), then the above formula shows that $L(\alpha)$ is P stable, with γ_α the eigenvalue of P on $L(\alpha)$.

Now we consider the Lie structure from ψ. Recall that $z \cdot w = R[z, w]$ where $R = P^{-1}$. It follows that for $z, x \in L_0$, $z \cdot x = 0$ if and only if $[z, x] = 0$. Thus an abelian subalgebra in one product is an abelian subalgebra in the other and the centralizer of x in either product is the same. Taking x to be a regular element of $\mathcal{H}$ shows that $\mathcal{H}$ is a Cartan subalgebra in either product. Since $R(x_\alpha) = \gamma_\alpha^{-1} x_\alpha$ for $\alpha \in \mathcal{B}$ and for $a \in \mathcal{H}$ we have

$$a \cdot x_\alpha = R[a, x_\alpha] = \alpha(a)\gamma_\alpha^{-1} x_\alpha$$

which shows that x_α is a root vector for $\mathcal{H}$ in the ψ product with root $\alpha' = \gamma_\alpha^{-1}\alpha$. Suppose $\alpha \neq \beta$ but $\alpha' = \beta'$. Then $\gamma_\alpha \gamma_\beta^{-1} \alpha = \beta$ which implies that $\gamma_\alpha \gamma_\beta^{-1} = -1$, so that $\beta = -\alpha$ and $\gamma_{-\alpha} = -\gamma_\alpha$. Now $[x_\alpha, x_{-\alpha}] \neq 0$, but $\gamma_\alpha [x_\alpha, x_{-\alpha}] = [\gamma_\alpha x_\alpha, x_{-\alpha}] = [P(x_\alpha), x_{-\alpha}] = [x_\alpha, P(x_{-\alpha})] = [x_\alpha, -\gamma_\alpha x_{-\alpha}] = -\gamma_\alpha [x_\alpha, x_{-\alpha}]$, which is a contradiction. Thus $\alpha' \neq \beta'$.

Let $\mathcal{B}' = \{\alpha' \mid \alpha \in \mathcal{B}\}$, and let $L(\alpha')$ be the corresponding root space. We have $L(\alpha) \subseteq L(\alpha')$, and since $\mathcal{B} \to \mathcal{B}'$ is bijective we have equality, so the $\mathcal{B}'$ root spaces are all one dimensional. Moreover,

$$L_0 = \mathcal{H} \oplus_{\mathcal{B}'} L(\alpha')$$

is a root space decomposition in the ψ product.

Furthermore, if $\alpha, \beta, \alpha + \beta \in \mathcal{B}$, so that $L(\alpha), L(\beta)$, and $L(\alpha+\beta) = [L(\alpha), L(\beta)]$ are all one dimensional, then $L(\alpha') \cdot L(\beta') = R([L(\alpha), L(\beta)]) = L(\alpha + \beta)$ is one dimensional, proving that $\alpha' + \beta' = (\alpha + \beta)' \in \mathcal{B}$. Thus the bijection $\mathcal{B} \to \mathcal{B}'$ carries sums to sums. Of course it readily follows from this that the two root systems $\mathcal{B}$ and $\mathcal{B}'$ for the Lie algebras $(L_0, [a, b])$ and $(L_0, a \cdot b)$ are equivalent.

We summarize this discussion with the following theorem:

THEOREM 16. *Let L be a Lie algebra over k. For $n \geq 1$ let $L_n = \mathcal{C}^n L / \mathcal{C}^{n+1} L$ and let $L^n = \prod i \geq n L^i$. Assume that*

1. *L_1 is finite dimensional.*
2. *$L = \hat{gr}(L, \mathcal{C}^i L)$.*
3. *$\mathcal{C}^n L = L^n$ for all n.*
4. *L has a shift structure.*
5. *L_1 is semisimple in the Lie bracket determined by the shift structure.*

Then the isomorphism class of the semisimple Lie algebra L_1 is independent of the choice of shift structure.

Of course the Theorem applies notably to the case of pronilpotent prolongations:

COROLLARY. *Let L_0 be a finite dimensional semisimple Lie algebra. Then L_0 is determined up to isomorphism by the pronilpotent prolongation $\mathcal{U}L_0$.*

Prolongation of groups

Now we turn to the study of the prounipotent prolongation $UH = \mathrm{Ker}(H[\infty] \to H[0])$ of an algebraic group H. Our goal is to find to what extent the group H can be recovered from UH. Since if $H' \to H$ is an isogeny then $UH' \to UH$ is an isomorphism, we will concentrate on simply connected H, so the goal then becomes to recover Lie(H) from UH. Our plan is to relate the Lie algebras Lie(UH) and $\mathcal{U}$Lie(U), since (at least for semi-simple H) the latter determines Lie(U).

The corollary to Theorem 16 implies that for (semi-simple) algebraic groups H if $\mathrm{Lie}(UH) = \mathcal{U}\mathrm{Lie}(U)$ then UH determines Lie(H). We recall the calculations preceding Lemma 8 above, which show that we have this equality for $H = SL_n$: those calucations showed that

$$\mathrm{Lie}(GL_n[\infty]) = \prod_{i=0}^{\infty} \mathfrak{gl}_n t^i$$

and

$$\mathrm{Lie}(SL_n[\infty]) = \prod_{i=0}^{\infty} \mathfrak{sl}_n t^i;$$

since $\mathrm{Lie}(UGL_n) = \mathrm{Ker}(\mathrm{Lie}(GL_n[\infty] \to \mathrm{Lie}(GL_n))$ and the map on Lie algebras amounts to projection on the first factor, we see that $\mathrm{Lie}(UGL_n) = \mathcal{U}\mathrm{Lie}(GL_n)$ and $\mathrm{Lie}(USL_n) = \mathcal{U}\mathrm{Lie}(SL_n)$. (For later use, we note that this implies that $C^i(UGL_n) = C^i(\mathcal{U}\mathrm{Lie}(GL_n) = \prod_{i\geq j} \mathrm{Lie}(GL_n)t^j$.)

Thus we can recover SL_n from its prounipotent prolongation:

COROLLARY. *Let U be a prounipotent group and let $L = Lie(U)$. For $n \geq 1$ let $L_n = C^nL/C^{n+1}L$ and let $L^n = \prod i \geq nL^i$.*

Then U is isomorphic to USL_n if and only if

1. *L_1 is finite dimensional.*
2. *$L = \hat{gr}(L, C^iL)$.*
3. *$C^nL = L^n$ for all n.*
4. *L has a shift structure.*
5. *L_1 is isomorphic to $\mathfrak{sl}_n$ in the Lie bracket determined by the shift structure.*

Note that the corollary implies that $C^m\mathrm{Lie}(USL_n) = \prod_{i\geq m} \mathfrak{sl}_n t^i$, a property that we do not expect for general H.

One of the key points in the characterization of Theorem 16 is that L is the (complete) associated graded Lie algebra of its natural filtration by its lower central series, and that this filtration coincides with the t filtration. The two filtrations are always present on Lie(UH), but as noted there is no reason to expect them to coincide in general. It turns out to be convenient, conceptually and notationally, to consider the filtrations already on the prounipotent group UH.

DEFINITION. On UH we can define t *filtration* as follows: for $i \geq 1$, let $UH^i = \mathrm{Ker}(H[\infty] \to H[i-1])$.

Note that the t filtration on UH, unlike the lower central series, is not intrinsic.

For the t filtration, we have that $UH^1 = UH$, $UH^i > UH^{i+1}$, and UH^i/UH^{i+1} is the kernel of $H[i+1] \to H[i]$ which, by Lemma 8, is Lie(H), hence abelian, so $(UH^i, UH^j) \leq UH^{i+j}$. Moreover, because the succesive quotients are the Lie algebra of H, we also have shown the following:

LEMMA 17. *Let H be an algebraic group. Then the associated graded Lie algebra $\hat{gr}(UH, UH^i)$ is isomorphic to $\mathcal{U}Lie(H)$.*

It follows from Lemma 17 that, for semisimple H, UH, with its t filtration, determines Lie(H).

Although the t filtration is not intrinsic in general, it is for GL_n since, as we noted above, we have shown that it coincides with the lower central series for GL_n (so that $UGL_n^i = C^iUGL_n$). If H is a subgroup of GL_n, the t filtration of UH is the restriction to UH of that of GL_n, so that $UH^i = UH \cap UGL_n^i = UH \cap C^iUGL_n$. In other words, the t filtration on UH as a subgroup of UGL_n is intrinsic. Using this, we can recover Lie(H) from $UH < UGL_n$ in the following sense:

THEOREM 18. *Let H_1 and H_2 be semisimple subgroups of GL_n. Suppose there is an automorphism of UGL_n carrying UH_1 to UH_2. Then Lie(H_1) and Lie(H_2) are isomorphic.*

PROOF. The autoomorphism induces an isomorphism between the filtrations $UH_j^i = UH_j \cap C^iGL_n$ and hence between their complete associated graded Lie algebras. By Lemma 17, these are $\mathcal{U}$(Lie(H_j). Now the corollary to Theorem 16 provides the result.

Lemma 17 also provides additional information about the group UH: the Lie algebra $\mathcal{U}$(Lie(H)) is finitely generated by degree one as a pronilpotent Lie algebra, hence $\hat{gr}(UH, UH^i)$ is finitely generated in the same sense. We have a natural map

$$\hat{gr}(UH, C^iUH) \to \hat{gr}(UH, UH^i)$$

surjective in degree one. If $U \to UH$ is a surjection of prounipotent groups we have a corresponding surjective map

$$\hat{gr}(U, C^iU) \to \hat{gr}(UH, C^iUH);$$

and we can select U to be finitely generated free prounipotent so that the composite

$$\hat{gr}(U, C^iU) \to \hat{gr}(UH, UH^i)$$

is surjective in degree 1, and hence surjective. This means that the corresponding group map $U \to UH$ is also surjective, and hence that UH is finitely generated as a prounipotent group, a fact we now record:

PROPOSITION 19. *Let H be an affine algebraic group such that $H = (H, H)$. Then UH is finitely generated as a prounipotent group.*

In [**M2**], it was shown how to construct differential field extensions of the rational function field $\mathbb{C}(x)$ with given prounipotent group as differential Galois group. That means that it is possible to produce such an extension with group UH, where H is a given linear group. It is also known [**TT**] that every linear group is a differential Galois group over $\mathbb{C}(x)$. It is conceivable that the methods leading to the recovery of H from UH, at least in the semisimple case, will yield a construction of extensions with group H from those with group UH; that was part of the motivation for the investigation reported on here, although that project remains uncompleted. (A construction of differential Galois extensions of $\mathbb{C}(x)$ with given linear algebraic group as differential Galois group is given in [**MS**].)

References

[DDMS] Dixon, J., du Sautoy, M., Mann, A., and Segal, D., *Analytic pro-p Groups*, London Mathematical Society Lecture Note Series Volume 157, Cambridge University Press, Cambridge, 1991.

[LM1] Lubotzky, A. and Magid, A., *Cohomolgy of unipotent and prounipotent groups*, J. of Algebra **74** (1982), 76–95.

[LM2] ———, *Free prounipotent groups*, J. of Algebra **80** (1983), 323–349.

[LM3] ———, *Cohomology, Poincaré series, and group algebras of unipotent groups*, Amer. J. Math. **107** (1985), 531–553.

[LM4] ———, *Varieties of representations of finitely generated groups*, Mem. Amer. Math. Soc. 336, American Mathematical Society, Providence, 1985.

[M1] Magid, A., *Identities for prounipotent groups*, Algebraic Groups and Their Genralizations (W. Haboush and B. Parshall, eds.), Proceedings of Symposia in Pure Mathematics 56, Part I, American Mathematical Society, Providence, 1994, pp. 281–290.

[M2] ———, *Lectures on Differential Galois Theory*, University Lecture Series Volume 7 (Second Printing with Corrections), American Mathematical Society, Providence, 1997.

[M3] ———, *Coordinate rings of prounipotent groups*, J. of Algebra **95** (1985), 46–58.

[MS] Mitschi, C. and Singer, M., *Connected linear groups as differential Galois groups*, J. of Algebra **184** (1996), 333–361.

[N] Nelson, G. G., *Faithful Representations of Lie Algebras over Power Series*, Rings, Extensions, and Cohomology (A. Magid, ed.), Pure and Applied Mathematics 159, Marcel Dekker, Inc, New York, 1994, pp. 181–193.

[TT] Tretkoff, C. and Tretkoff, M., *Solution of the inverse problem of differential Galois theory in the classical case*, Amer. J. Math. **101** (1979), 1327–1332.

NORMAN OK 73019
E-mail address: amagid@ou.edu

This page intentionally left blank

http://dx.doi.org/10.1090/conm/224/03188

Contemporary Mathematics
Volume **224**, 1999

Graded Simple Jordan Algebras and Superalgebras

Consuelo Martínez

Dedicated to Professor Hyo Chul Myung on the occasion of his sixtieth birthday.

ABSTRACT. Superconformal algebras, superalgebras that are extensions of the Virasoro algebra, play an important role in Physics. Here we give an approach to their classification through Jordan theory

1. Introduction

A superconformal algebra is a $\mathbb{Z}$-graded simple Lie superalgebra that contains the Virasoro algebra in the even part and such that the dimensions of all the homogeneous components, $\dim L_i$, are uniformely bounded.

Let $\mathcal{V}$ be a homogeneous variety of algebras, that is, a class of F-algebras satisfying a certain set of homogeneous identities (see [**ZSSS**]). Let $A \in \mathcal{V}$.

Let's introduce the definition of a superalgebra corresponding to a variety $\mathcal{V}$. In general, by a superalgebra we mean just a $\mathbb{Z}/2\mathbb{Z}$-graded algebra, $A = A_{\bar{0}} + A_{\bar{1}}$.

Example Let V be a vector space. The Grassmann (or exterior) algebra $G(V)$ is the quotient of the tensor algebra $T(V)$ modulo the ideal generated by symmetric tensors $v \otimes w + w \otimes v$; $v, w \in V$. Clearly $G(V) = G_{\bar{0}} + G_{\bar{1}}$, where $G_{\bar{0}}$ (resp. $G_{\bar{1}}$) is spanned by products of elements of V of even (resp. odd) length.

Suppose that V is infinite dimensional. By the Grassmann envelope of a superalgebra $A = A_{\bar{0}} + A_{\bar{1}}$ we mean the subalgebra $G(A) = A_{\bar{0}} \otimes G_{\bar{0}} + A_{\bar{1}} \otimes G_{\bar{1}}$ of the tensor product $A \otimes G$.

DEFINITION 1. *A superalgebra $A = A_{\bar{0}} + A_{\bar{1}}$ is called a $\mathcal{V}$-superalgebra if the Grassmann envelope $G(A)$ lies in $\mathcal{V}$.*

In particular, if $A = A_{\bar{0}} + A_{\bar{1}}$ is a $\mathcal{V}$- superalgebra, then $A_{\bar{0}} \in \mathcal{V}$ and $A_{\bar{1}}$ is a module over $A_{\bar{0}}$.

In this way one can define Lie superalgebras, Jordan superalgebras, etc. Clearly, associative superalgebras are just $\mathbb{Z}/2\mathbb{Z}$-graded associative algebras and a commutative superalgebra is more often called a supercommutative (super) algebra.

1991 *Mathematics Subject Classification.* Primary 17A70; Secondary 17C65.

Supported by the Spanish DGICYT (PB 94-1311-C03-01)

In [**KvL**] V. Kac and J. W. van de Leur conjectured that superconformal algebras over an algebraically closed field of zero characteristic admit a classification that is similar to the one obtained by Mathieu in [**M2**] for graded simple algebras. To be more precise, let $F[t^{-1}, t, \xi_1, \dots, \xi_n]$ be the associative supercommutative algebra of polynomials in one Laurent variable t and n odd variables $\xi_1, \dots, \xi_n$. The Lie superalgebra $W(1,n)$ of superderivations of $F[t^{-1}, t, \xi_1, \dots, \xi_n]$, graded by degrees of t, is a graded simple Lie superalgebra containing the Virasoro algebra Vir in the even part and having dimensions of all homogeneous components uniformely bounded. V. Kac and Van de Leur conjectured that an arbitrary graded simple Lie superalgebra containing Vir in the even part and having dimensions of all homogeneous components uniformely bounded is isomorphic to $W(1,n)$ (for some n) or to one of known subsuperalgebras of $W(1,n)$.

Without the assumption of the existence of a Virasoro subalgebra also loop algebras and superalgebras of Cartan type appear.

The above conjecture about superalgebras, as it has been mentioned before, is inspired by the results known for graded simple algebras.

The study of graded simple Lie algebras with restrictions on dimensions of graded components was initiated by V. Kac in [**K1**]. In this work he formulated the following

Conjecture: Let L be a graded simple Lie algebra such that the function $n \to dim(L_n)$ is bounded by some polynomial in n. Then L is either a simple finite dimensional Lie algebra or a loop algebra or an algebra of Cartan type or the Virasoro algebra.

Let us look through the list of algebras that appear in Kac's conjecture.

Loop algebras. Let n be a natural number, $\mathcal{G}$ be a $\mathbb{Z}/n\mathbb{Z}$-graded finite dimensional algebra, $\mathcal{G} = \mathcal{G}_0 + \mathcal{G}_1 + \cdots + \mathcal{G}_{n-1}$. For an arbitrary integer i, let $\bar{i}$, $0 \leq \bar{i} \leq n-1$, denote the residue of i modulo n. By a loop algebra corresponding to $\mathcal{G}$ we mean the subalgebra $\mathcal{L}(G) = \sum_{i \in \mathbb{Z}} \mathcal{G}_{\bar{i}} \otimes t^i$ of the tensor product $\mathcal{G} \otimes F[t^{-1}, t]$. If $\mathcal{G}$ is a simple finite dimensional Lie (Jordan) algebra then $\mathcal{L}(G)$ is a graded simple Lie (Jordan) algebra and the dimensions of all homogeneous components are uniformely bounded.

Equivalently, we can define loop algebras in the following way:

A $\mathbb{Z}/n\mathbb{Z}$-graded algebra is an algebra with an automorphism ω of order n. Then ω can be extended to an automorphism $\bar{\omega} : \mathcal{G} \otimes F[t^{-1}, t] \longrightarrow \mathcal{G} \otimes F[t^{-1}, t]$, $a \otimes t^i \to \eta^i \omega(a) \otimes t^i$, where η is a primitive nth-root of the unit in F.

So $\mathcal{L}(G)$ is the set of fixed points of $\bar{\omega}$.

Virasoro algebra, Vir, is the Lie algebra of derivations of the Laurent polynomial ring $F[t^{-1}, t]$. It is well known that elements $e_n = t^{n+1} \frac{d}{dt}$ form a basis that satisfies $[e_i, e_j] = (j - i) e_{i+j}$.

The subalgebra Vir_1, derivation algebra of $F[t]$, has the basis $\{e_j\}_{j \geq -1}$.

Cartan algebras. Let W_n be the algebra of derivations of $F[t_1, \dots, t_n]$. Cartan algebras are W_n and the subalgebras $S_n < W_n$, $H_{2m} < W_{2m}$, $K_{2m+1} < W_{2m+1}$ (see [**K1**] or [**M2**]).

In [**M1,M2**] O. Mathiew proved the conjecture of V. Kac, proving the following:

THEOREM 2. *(O. Mathieu) Let L be a graded simple Lie algebra over an algebraically closed field of zero characterisitic with the dimensions of the graded components L_i uniformely bounded (***growth one***). Then L is isomorphic to one of the following algebras:*
(1) a simple finite dimensional Lie algebra, or
(2) a loop algebra, or
(3) Vir, or
(4) Vir_1.

If we only assume that the function $n \to dim(L_n)$ is bounded by some polynomial in n (**finite growth***) then other Cartan algebras can appear in (4) (not only Vir_1).*

2. Lie-Jordan relations

DEFINITION 3. *A (linear) Jordan algebra is a vector space J with a binary operation $(x, y) \to xy$ satisfying the following identities:*
(J1) $xy = yx$
(J2) $(x^2y)x = x^2(yx)$.

EXAMPLES (see [**J**])

1) If A is an associative algebra over F, $(\frac{1}{2} \in F)$ we then can define a new product $\cdot$ in A by : $a \cdot b = \frac{1}{2}(ab + ba)$. Denote as $A^{(+)}$ the new algebra obtained in this way. It is easy to check that $(A^{(+)}, \cdot)$ is a Jordan algebra.

A Jordan algebra J is called special if it is a subalgebra of the Jordan algebra $(A^{(+)}, \cdot)$ for some associative algebra A. In the other case A is called exceptional.

2) If $(A, *)$ is an associative algebra with involution, $H(A, *) = \{a \in A | a^* = a\}$ is a Jordan subalgebra of $(A^{(+)}, \cdot)$.

3) Let $\mathcal{O}$ be the octonions, $H_3(\mathcal{O}, *)$ denotes the algebra of 3x3 hermitians matrices over the octonions. It is an exceptional Jordan algebra.

4) Let V be a vector space over F with a symmetric bilinear form $<,>$. Then $J = F1 + V$ with the product $(\alpha 1 + v)(\beta 1 + w) = (\alpha\beta + < v, w >)1 + \beta v + \alpha w$ is a (special) Jordan algebra, called the Jordan algebra of a bilinear form.

Every simple finite-dimensional Jordan algebra over an algebraically closed field F is either special or isomorphic to $H_3(\mathcal{O}, *)$ (see [**J**]).

Let L be a Lie algebra containing a subalgebra $Fe + Fh + Ff$ which is isomorphic to $sl_2(F)$, that is, $[e, f] = h$, $[f, h] = 2f$, $[e, h] = -2e$.

Suppose that the operator $ad(h) : L \to L$ is diagonalizable and that the only eigenvalues of $ad(h)$ are -2,0,2. Let $L = L_{(-2)} + L_{(0)} + L_{(2)}$ be the decomposition of L into a sum of eigenspaces. Following J. Tits [**T**] we will define a structure of a Jordan algebra on $J = L_{(-2)}$ via $x_{(-2)} \star y_{(-2)} = [[x_{(-2)}, f], y_{(-2)}]$ for arbitrary elements $x_{(-2)}, y_{(-2)} \in L_{(-2)}$. The algebra L can be recovered (up to central extensions) from J.

On the other hand, for an arbitrary Jordan algebra J with 1 there exists the unique (up to isomorphism) pair $L \supseteq sl_2(F)$ with these properties such that $L_{(-2)} \simeq J$ and L has zero center. We will call such a Lie algebra the Tits-Kantor-Koecher construction of J and denote it $K(J) = J^- + [J^-, J^+] + J^+$ (see [**J**]).

Let $L = L_{\bar{0}} + L_{\bar{1}}$ be a graded Lie superalgebra such that dimensions $\dim L_i$, $L_i = L_{i\bar{0}} + L_{i\bar{1}}$, are uniformely bounded. Then the zero component L_0 is a finite dimensional Lie superalgebra, $L_0 = L_{0\bar{0}} + L_{0\bar{1}}$. It is known (see [**K1**]) that a finite dimensional Lie superalgebra is solvable if and only if its even part is solvable. Suppose that the Lie algebra $L_{0\bar{0}}$ is not solvable. Then (see [**K1**]) $L_{0\bar{0}}$ contains a subalgebra $sl_2(F) = Fe + Fh + Ff$ with $[e, f] = h$, $[f, h] = 2f$, $[e, h] = -2e$. An arbitrary homogeneous component L_i is a module over $sl_2(F)$. Since there is only one irreducible $sl_2(F)$-module in each dimension and dimensions of L_i are uniformely bounded it follows that only finitely many irreducible $sl_2(F)$-modules can occur in decompositions of L_i, $i \in \mathbb{Z}$. This implies that $ad(h) : L \to L$, $x \to [x, h]$ is diagonalizable and has finitely many eigenvalues. In [**Z1**] it was shown that such Lie algebras can be studied by means of Jordan theory.

The classification of $\mathbb{Z}$-graded simple Jordan superalgebras with the dimensions of homogeneous components uniformely bounded appears now as a natural task.

<u>EXAMPLES</u>

1) Let $\mathcal{G}$ denote now a $\mathbb{Z}/n\mathbb{Z}$-graded finite dimensional superalgebra, $\mathcal{G} = \mathcal{G}_0 + \mathcal{G}_1 + \cdots + \mathcal{G}_{n-1}$. The loop superalgebra corresponding to $\mathcal{G}$ is $\mathcal{L}(G) = \sum_{i \in \mathbb{Z}} \mathcal{G}_{\bar{i}} \otimes t^i$.
If $\mathcal{G}$ is a simple Jordan (Lie) superalgebra then $\mathcal{L}(G)$ is a graded simple Jordan (Lie) superalgebra and dimensions of the graded components, $dim \mathcal{L}(G)_i$, $i \in \mathbb{Z}$, are uniformely bounded.

2) A graded simple Jordan superalgebra J is of Cartan type if J contains a graded subsuperalgebra B of finite codimension such that the corresponding subspace $B^- + [B^-, J^+] + [J^-, B^+] + B^+$ of the Tits-Kantor-Koecher Lie superalgebra $K(J)$ is a subsuperalgebra of $K(J)$ of finite codimension. Thus $K(J)$ is a Lie superalgebra of Cartan type.

3) Let V be a direct sum of two vector spaces, both $V_{\bar{0}} = \oplus_{i \in \mathbb{Z}} V_{\bar{0}i}$ and $V_{\bar{1}} = \oplus_{i \in \mathbb{Z}} V_{\bar{1}i}$ are represented as direct sums of finite dimensional vectors spaces such that dimensions of subspaces $V_i = V_{\bar{0}i} + V_{\bar{1}i}$, $i \in \mathbb{Z}$ are uniformely bounded. Suppose further that the space V is equipped with a nondegenerate supersymmetric form $<,>: V \times V \to F$. That is, $<,>$ is symmetric on $V_{\bar{0}}$, skew-symmetric on $V_{\bar{1}}$ and $< V_{\bar{0}}, V_{\bar{1}} > = < V_{\bar{1}}, V_{\bar{0}} > = < V_i, V_j > = (0)$ if $i + j \neq 0$. Then the direct sum of vector spaces $J = F1 + V = J_{\bar{0}} + J_{\bar{1}}$, $J_{\bar{0}} = F1 + V_{\bar{0}}$, $J_{\bar{1}} = V_{\bar{1}}$ becomes a Jordan superalgebra under multiplication $vw = < v, w > 1$ for $v, w \in V$. The superalgebra J is graded simple, $J_i = V_i$ for $i \neq 0$, $J_0 = F1 + V_0$.

4) Let $A = A_{\bar{0}} + A_{\bar{1}}$ be an associative supercommutative algebra. If $a \in A_{\bar{i}}$ then we denote $|a| = i$. A bracket $[,] : A \times A \to A$ is called a <u>contact bracket</u> ("generalized Poisson bracket" in [**KvL,Ki**]). Compare also to "Jordan bracket" in [**Ki**]) if:
(i) $(A, [,])$ is a Lie superalgebra,
(ii) $D : a \to [a, 1]$ is a derivation of A,
(iii) $D(a)[b, c] + (-1)^{|a|(|b|+|c|)} D(b)[c, a] + (-1)^{|c|(|a|+|b|)} D(c)[a, b] = 0$,
(iv) $[a, bc] = [a, b]c + (-1)^{|a||b|} b[a, c] - D(a)bc$,
(v) for $a \in A_{\bar{1}}$ we have $D(a)[a, a] = 0$.

Starting with an associative supercommutative superalgebra A with a contact bracket $[,] : A \times A \to A$ consider a direct sum of vector spaces $J = J(A, [,]) = A + Ax$. We shall define a multiplication on J. For arbitrary elements $a, b \in A$ their product in J is the product ab in A, $a(bx) = (ab)x$, $(bx)a = (-1)^{|a|}(ba)x$, $(ax)(bx) = (-1)^{|b|}[a, b]$.

The $\mathbb{Z}/2\mathbb{Z}$-gradation on A can be extended to a $\mathbb{Z}/2\mathbb{Z}$-gradation on J via $J_{\bar{0}} = A_{\bar{0}} + A_{\bar{1}}x$, $J_{\bar{1}} = A_{\bar{1}} + A_{\bar{0}}x$. The superalgebra J is a Jordan superalgebra (see [**Kn**] and [**KM**]). We call it the Kantor Double of $(A, [,])$.

Let $n \geq 1$, $V = V_0 + \ldots + V_{n-1}$ a finite dimensional $\mathbb{Z}/n\mathbb{Z}$-graded vector space over F. The gradation on V can be uniquely extended to a $Z/n\mathbb{Z}$-gradation on the Grassmann algebra, $G(V) = \sum_{i=0}^{n-1} G(V)_i$.

Let $A = \sum_{i\in\mathbb{Z}} G(V)_{\bar{i}} \otimes t^i = \mathcal{L}(G(V))$. If $[,] : A \times A \to A$ is a contact bracket, the element x in the Kantor Double construction is given degree i such that $2i \in n\mathbb{Z}$ and $[A_j, A_k] \subseteq A_{j+k+2i}$ for arbitrary $j, k \in \mathbb{Z}$, then the Kantor Double $J = A + Ax$ is a $\mathbb{Z}$-graded Jordan superalgebra having all dimensions $dim(J_i)$, $i \in \mathbb{Z}$, uniformely bounded.

It has been proved in [**KMZ**] that the examples given before "nearly" cover the collection of graded simple Jordan superalgebras having dimensions of graded component uniformely bounded.

3. Previous Results

Before formulating the main result of [**KMZ**], we will discuss some results that are used in the proof.

A) GK-dimension in Jordan algebras

DEFINITION 4. *Let A be a finitely generated (no necessarily associative) algebra. Let V be a finite dimensional F-vector space generating A and let V^n denote the linear span of all product of lenght $\leq n$ in elements of V. The Gelfand-Kirillov dimension of A (denoted GK dim(A) for short) is defined by:*

$$GKdim(A) = \limsup_{n\to\infty} \frac{\ln[dimV^n]}{\ln n}$$

If the algebra A is not necessarily finitely generated then GK dim(A) = sup GK dim(C), where C runs over all finitely generated subalgebras of A.

It is known that the above definition does not depend on the particular finite dimensional vector space generating A (see [**BK**], [**GK**] and [**KL**]).

If A is associative, Lie, Jordan or alternative, then GK dim$A = 0$ if and only if $dim_F A < \infty$ and there are no algebras with $0 < GKdim\mathrm{A} < 1$ (see [**KL**]). In the associative case G. Bergman proved (see [**KL**]) that there are no associative algebras with $1 < GKdim\mathrm{A} < 2$. But there are algebras having dimension s for every real number $2 \leq s$.

The structure of associative algebras having GK dim $= 1$ was determined in a series of papers by Small, Stafford and Warfield Jr. They proved that a finitely generated associative algebra having GK dimension 1 is PI. If it is prime, then it is a finite module over its center. The prime radical is nilpotent.

Some general properties of Gelfand Kirillov dimension in Jordan algebras were studied in [**M**]. Then in [**MZ1**] the result of Small, Stafford and Warfield Jr. has been extended to Jordan algebras.

THEOREM 5. *Let A be a finitely generated linear Jordan algebra of GK dimension 1. Then:*

(a) if A is semiprime, then A is a finite module over a finitely generated central subalgebra of the associative center of A,

(b) the radical of A is nilpotent.

In the same paper we proved that there are no Jordan algebras having GK dimension strictly between 1 and 2.

Notice that the even part A of a Jordan superalgebra of the type that we are interested in is a $\mathbb{Z}$-graded Jordan algebra in which dimensions of all homogeneous components are uniformely bounded. So either A is finite dimensional or it has GK $\dim = 1$.

B) Simple graded and prime graded Jordan algebras

For graded algebras we can get more precise information. The following result is an analog from the theorem of O. Mathieu in [**M2**].

THEOREM 6. *Let $A = \sum_{i \in \mathbb{Z}} A_i$ be a graded simple Jordan algebra of finite growth, that is, $dim J_i < |i|^c + d$, where c, d are constants. If we assume that A is infinite dimensional, then A is isomorphic to one of the following Jordan algebras:*

(a) The simple Jordan algebra associated to a symmetric nondegenerate bilinear form over an infinite dimensional vector space V, or

(b) A loop algebra.

Recall that a (nonassociative) algebra A is said to be prime if for any two nonzero ideals I and L of A their product IL is nonzero. A Jordan algebra A is said to be nondegenerate if, for an arbitrary element a from A, $a^2 = 0$ and $(Aa)a = (0)$ imply $a = 0$.

In the proof of Theorem 6 the following facts are used:

- The algebra A is non-degenerate if and only if is graded non-degenerate.
- The algebra A is prime non-degenerate if and only if it is graded prime non-degenerate.

Consequently, the structure of prime nondegenerate algebras, studied in [**Z1**] plays a very important role. Also Mathieu's result is used. In a concrete way, it is used that fact that a graded simple Lie algebra of finite growth is PI.

Once the structure of simple graded Jordan algebras of finite growth (that is, finite GK dimension) is known, we can study the structure of graded prime algebras. The change of simple by prime forces the change of finite growth by growth one (GK-dimension 1). Now the structure of this algebras is given by the following:

THEOREM 7. *Let $A = \sum_{i \in \mathbb{Z}} A_i$ be a prime nondegenerate graded Jordan algebra. Suppose that there exists $d > 0$ such that $dim A_i < d$, for all i. Then A is:*

(a) either a graded simple algebra (so known by the previous theorem) or

(b) only finitely many negative (resp. finitely many positive) components of A are nonzero, that is, there exists $s \geq 1$ such that $A_i = 0$ for all $i < -s$ (or $A_i = 0$ for all $i > s$). Moreover, there exists a simple finite dimensional $\mathbb{Z}/n\mathbb{Z}$-graded algebra $\mathcal{G}$ and a monomorphism of graded algebras $\phi : A \to \mathcal{L}(G)$ such that $\phi(A_k) = \mathcal{L}(G)_k$ for all k greater than a certain number $m \geq 1$ (resp. less than $-m$).

Remark. We will refer to algebras of type (b) as "one-sided graded algebras".

4. The main result. General ideas of its proof

The aim of [**KMZ**] is to prove the following result

THEOREM 8. *Let $J = \sum_{i\in\mathbb{Z}} J_i$ be an infinite dimensional graded simple Jordan superalgebra over an arbitrarily closed field F of zero characteristic such that dimensions $dim(J_i)$ are uniformely bounded. Then J is isomorphic to one of the following superalgebras:*

1) a loop superalgebra $\mathcal{L}(G)$, where $\mathcal{G} = \mathcal{G}_0 + \mathcal{G}_1 + \cdots + \mathcal{G}_{n-1}$ is a finite dimensional simple $\mathbb{Z}/n\mathbb{Z}$- graded superalgebra,

2) a Jordan superalgebra $F1 + V$ of a nondegenerate supersymmetric form in a $\mathbb{Z}$-graded vector space $V = V_{\bar{0}} + V_{\bar{1}}$,

3) a Kantor Double $J = A + Ax$ of an associative supercommutative algebra $A = \sum_{i\in\mathbb{Z}} G(V)_{\bar{i}} \otimes t^i$ with a contact bracket, where $V = V_0 + \cdots + V_{n-1}$ is a $\mathbb{Z}/n\mathbb{Z}$- graded finite dimensional vector space. If n is odd then there is one (up to isomorphism) Jordan superalgebra of this type with x being of degree 0. If n is even then there are two contact brackets on A leading to two nonisomorphic Jordan superalgebras, one with x having degree 0 and one with x having degree $\frac{-n}{2}$,

4) a Jordan superalgebra of Cartan type,

*5) an exceptional Jordan superalgebra J_8 whose Tits-Kantor Koecher construction is isomorphic to the exceptional Cheng-Kac superalgebra $CK(6)$ (see [**CK**]).*

Let us denote A and M the even and odd part respectively of J. For every element $x \in M$ the operator $R(x)^2 : J \to J,\ y \to (yx)x$ is a derivation.

Let $\mathcal{D}$ be the linear span of $\{R(x)^2 | x \in M\}$ and let I be maximal graded $\mathcal{D}$-invariant ideal of A such that I_0 is nilpotent.

It can be proved that A/I is a direct sum of prime nondegenerate $\mathcal{D}$-invariant graded ideals: $\bar{A} = A/I = \bar{A^{(1)}} \oplus \cdots \oplus \bar{A^{(r)}}$.

According to the previous section the structure of each of these $\bar{A^{(i)}}$ is known to be of one of the following types:

(a) finite dimensional, or
(b) a loop algebra, or
(c) an infinite dimensional Jordan algebra associated to a bilinear form, or
(d) a one sided graded algebra.

More precise information on the structure of A is given by the following proposition:

PROPOSITION 9. *If a superalgebra J satisfies the assumptions of the Theorem and A denotes its even part, then one of the following assertions holds:*

1) $A/I \simeq \mathcal{L}(G)$ a loop algebra of a simple finite dimensional Jordan algebra of a bilinear form, the ideal I is nilpotent and $I \neq (0)$,

2) A/I is a one-sided graded algebra commensurable with a loop algebra $\mathcal{L}(G)$ of a simple finite dimensional Jordan algebra of a bilinear form,

3) A/I is a finite dimensional simple Jordan algebra of a bilinear form, $I \neq (0)$,

4) $A = A^{(1)} \oplus A^{(2)}$, where $A^{(i)}$ are algebras of the types (a), (b), (c) or (d) that we have mentioned above,

5) $A \simeq \mathcal{L}(G)$, where $\mathcal{G}$ is a simple finite dimensional Jordan algebra of a bilinear form,

6) A is a finite dimensional simple algebra,
7) A/I is a simple infinite dimensional Jordan algebra, $I \neq (0)$,
8) A is a simple infinite dimensional Jordan algebra of a bilinear form.

The Jordan superalgebra J is of Cartan type in the following cases:
i) If $I = (0)$, $A = A^{(1)} \oplus A^{(2)}$, $A^{(1)}$ is one sided graded and $A^{(2)}$ is either finite dimensional or one sided graded of the same type as $A^{(1)}$ (that is, both positively or both negatively graded).
ii) If A/I is one sided graded (I can be (0) or not).

If $I \neq (0)$ and A/I is finite dimensional, then J is finite dimensional.
If $I = (0)$ and A is either finite dimensional or infinite dimensional of a bilinear form, then J is either finite dimensional or the Jordan algebra of a superform.

The following cases are shown to be impossible:
a) $A = A^{(1)} \oplus A^{(2)}$ with $A^{(1)}$ finite dimensional and $A^{(2)}$ a loop algebra.
b) $A = A^{(1)} \oplus A^{(2)}$, with $A^{(1)}$ and $A^{(2)}$ one-sided graded, one of them positively graded and the other one negatively graded.
c) $A = A^{(1)} \oplus A^{(2)}$ with $A^{(1)}$ an infinite dimensional Jordan algebra of a bilinear form.
d) $A^{(1)} \oplus A^{(2)}$ with $A^{(1)}$ a loop algebra and $A^{(2)}$ one sided graded.
e) $(0) \neq I$ and A/I infinite dimensional of a bilinear form.

If A is a sum of two loop algebras then J is either a loop superalgebra or an algebra obtained by the Kantor double process.

If $I = (0)$ and A is a loop algebra associated to a simple finite dimensional Jordan algebra $\mathcal{G}$, then J is either a loop superalgebra or, in case when A is associated to the algebra of 2×2 matrices, the exceptional algebra J_8. The Tits-Kantor-Koecher construction of J_8 is the exceptional Lie superalgebra $CK(6)$ discovered by Cheng and Kac (see [**CK**]).

Finally, the main case corresponds to $A/I \simeq \mathcal{L}(G)$ the loop algebra associated to a Jordan algebra of a bilinear form $\mathcal{G}$. In this case, $(0) \neq I = \mathcal{M}_c(A)$ is nilpotent.
First it is proved that the algebra A splits over its McCrimmon radical I, that is, there is a subalgebra B of A with $B \simeq \mathcal{L}(G)$ and $A = I + B$. in this case J is a Kantor double superalgebra.

References

[BK] W. Borho and H. Kraft, *Uber die Gelfand-Kirillov dimension*, Math. Ann. **220** (1976), 1–24.

[CK] S. Cheng and V. Kac, *A New $N = 6$ Superconformal Algebra*, Preprint.

[GK] I. M. Gelfand and A. A. Kirillov, *Fields associated with enveloping algebras of Lie algebras*, Doklady **167** (1966), 407–409.

[J] N. Jacobson, *Structure and representation of Jordan algebras*, A. M. S. Colloq. Publ., Providence, 1969.

[K1] V. Kac, *Simple graded Lie algebras of finite growth*, Math. USSR. Izv **2** (1968), 1271–1311.

[K2] V. Kac, *Lie superalgebras*, Adv. Math. **28** (1977), 8–96.

[K3] V. Kac, *Some Problems on infinite dimensional Lie algebras*, Lecture Notes in Math. **933** (1982), 117–126.

[KMZ] V. Kac, C. Martínez and E. Zelmanov, *Graded Simple Jordan superalgebras of growth one* (to appear).

[KvL] V. Kac and J. W. van de Leur, *On classification of superconformal algebras*, Strings 88, World Scientific (1988), 77–106.

[Kn] I. L. Kantor, *Jordan and Lie superalgebras determined by a Poisson algebra*, Amer. Math. Soc. Transl. (2) **151** (1992), 55–79.

[KM] D.King and K. McCrimmon, *The Kantor Construction of Jordan Superalgebras*, Commun. Algebra **20 (1)** (1992), 109–126.

[Ki] A. A. Kirillov, *Local Lie Algebras*, Russian Math. Surveys **31** (1976), 55–76.

[KL] G. Krause and T. H. Lenagan, *Growth of Algebras and Gelfand-Kirillov dimension*, Research Notes in Math. **116** (1985).

[M] C. Martínez, *Gelfand-Kirillov dimension in Jordan Algebras*, Trans. of the A.M.S. **348** (1996), 119–126..

[MZ1] C. Martínez and E. Zelmanov, *Jordan algebras of Gelfand-Kirillov Dimension one*, J. Algebra **180** (1996), 211–238..

[MZ2] C. Martínez and E. Zelmanov, *Simple and Prime Graded Jordan Algebras*, J. Algebra **196** (1997), 596–613..

[M1] O. Mathieu, *Classification des algebres de Lie graduees simples de croissance* ≤ 1, Invent. Math. **86** (1986), 371–426..

[M2] O. Mathieu, *Classification of Simple Graded Lie Algebras of Finite Growth*, Invent. Math. **108**, 455–519..

[RZ] M. Racine and E. Zelmanov, *Finite dimensional simple Jordan superalgebras with semisimple even part* (to appear).

[SSW] L. W. Small, J. T. Stafford and R. B.Warfield Jr, *Affine algebras of Gelfand-Kirillov dimension one are PI*, Math.Proc. Camb. Phil.Soc. **97** (1985), 407–414..

[T] J. Tits, *Une class d'algèbres de Lie en relation avec les algèbres de Jordan*, Indag. Math. **24** (1962), 530–535..

[Z1] E. Zelmanov, *On prime Jordan Algebras II*, Siberian Math. J. **24** (1983), 73–85..

[Z2] E. Zelmanov, *Lie algebras with a finite grading*, Math. USSR Sbornik **52 (2)** (1985), 347–385.

[ZSSS] K.A. Zhevlakov, A.M. Slin'ko, I.P. Shestakov and A.I. Shirshov, *Rings that are Nearly Associative*, Academic Press, New York, 1982.

Departamento de Matemáticas, Universidad de Oviedo. 33007 Oviedo, Spain
E-mail address: chelo@pinon.ccu.uniovi.es

This page intentionally left blank

http://dx.doi.org/10.1090/conm/224/03191

Contemporary Mathematics
Volume **224**, 1999

The Centralizer Algebra of the Lie Superalgebra $\mathfrak{p}(n)$ and the Decomposition of $V^{\otimes k}$ as a $\mathfrak{p}(n)$-module

Dongho Moon

ABSTRACT. We construct an associative algebra A_k and show that there is a representation of A_k on $V^{\otimes k}$ where V is the natural $2n$-dimensional representation of the Lie superalgebra $\mathfrak{p}(n)$. We show that A_k is the full centralizer of $\mathfrak{p}(n)$ on $V^{\otimes k}$. Using A_k, we decompose the tensor space $V^{\otimes k}$, for $k = 2$ or 3, and show that $V^{\otimes k}$ is not completely reducible for any $k \geq 2$.

0. Introduction

In his papers [**16**] [**17**], I. Schur showed that the action of the symmetric group S_k on the tensor product space $V^{\otimes k}$ by place permutations and the natural action of the general linear group $GL(V)$ on $V^{\otimes k}$ commute with each other. Moreover he proved that those two actions determine the full centralizers of each other. This result, which is often quoted as *Schur-Weyl duality*, connects the combinatorial theory and the representation theory of $GL(V)$ and S_k. For example, the decomposition of the $GL(V)$-module $V^{\otimes k}$ into irreducible summands can be obtained from the decomposition of the group algebra $\mathbb{C}S_k$ into minimal left ideals which are labeled by standard Young tableaux.

After Schur's initial results, there have been various attempts to obtain analogues of Schur-Weyl duality (or to determine the full centralizer algebras) in other settings. In [**5**], R. Brauer described the centralizer of the orthogonal Lie group $O(n)$, and the symplectic Lie group $Sp(n)$ (for n even) using what are now called Brauer algebras. An analogue of Schur-Weyl duality for the general linear Lie superalgebra $gl(m,n)$ was obtained by A. Berele and A. Regev [**3**]. A.N. Sergeev [**18**] obtained the same result for $gl(m,n)$ independently. In the same paper [**18**], Sergeev also determined the full centralizer of the almost simple Lie superalgebra $\mathfrak{sq}(n)$. The orthosymplectic Lie superalgebras $spo(m,n)$ were studied by G. Benkart, C. Lee Shader and A. Ram in [**2**] (see also [**9**] and [**10**]). The centralizer algebras for Lie color algebras, which are Lie algebras graded by a finite abelian group, and their relation with the Lie superalgebra case were studied by the author in [**11**] [**13**]. The general linear Lie color algebra case was also investigated by S. Montgomery and D. Fischman using Hopf algebra methods in [**6**].

1991 *Mathematics Subject Classification.* Primary 17B10; Secondary 05E10.

In this paper we will discuss the Lie superalgebras $\mathfrak{p}(n)$. The algebras $\mathfrak{sp}(n) = \mathfrak{p}(n) \cap sl(n,n)$ are the only ones in Kac's list [**7**] of classical simple Lie superalgebras whose centralizer algebras are not known (excluding the exceptional algebras $F(4)$, $G(3)$ and $D(2,1;\alpha)$). We obtain the full centralizer algebra of $\mathfrak{p}(n)$ in End $(V^{\otimes k})$. We also construct maximal vectors of $\mathfrak{p}(n)$. Then we use the centralizer algebra of $\mathfrak{p}(n)$ to decompose the tensor space $V^{\otimes 2}$ and $V^{\otimes 3}$. This decomposition enables us to find dimension formulas for some highest weight $\mathfrak{p}(n)$-modules. It will follow that $V^{\otimes k}$ is not completely reducible for every $k \geq 2$. The author hopes that the technique developed to decompose $V^{\otimes 2}$ and $V^{\otimes 3}$ could be used for higher values of k.

This paper is based on the presentation given at the conference on *Recent Progress in Algebra* held at KAIST, Taejon, Korea. But there are few new results after the conference. For example Theorem 2.7 (b) was not announced at the conference. More details with complete proofs of the results in this paper will appear elsewhere (see for example, [**12**] or [**13**]).

The author wishes to express his sincere gratitude to Professor G. Benkart, under whose guidance the work presented here was done.

1. The Lie superalgebra $\mathfrak{p}(n)$

Let $V = \mathbb{C}^{m+n}$ be a $\mathbb{Z}_2$-graded $(m+n)$-dimensional vector space over $\mathbb{C}$, with $V = V_{\bar{0}} \oplus V_{\bar{1}}$, where $V_{\bar{0}} = \mathbb{C}^m$ and $V_{\bar{1}} = \mathbb{C}^n$. The *general linear Lie superalgebra* $gl(m,n) = gl(m,n)_{\bar{0}} \oplus gl(m,n)_{\bar{1}}$ is the set of all $(m+n) \times (m+n)$ matrices over $\mathbb{C}$, which is $\mathbb{Z}_2$-graded by

$$gl(m,n)_{\bar{0}} = \left\{ \begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix} \middle| A \in \mathrm{M}_{m\times m}(\mathbb{C}), \quad B \in \mathrm{M}_{n\times n}(\mathbb{C}) \right\},$$
$$gl(m,n)_{\bar{1}} = \left\{ \begin{pmatrix} 0 & B \\ C & 0 \end{pmatrix} \middle| B \in \mathrm{M}_{m\times n}(\mathbb{C}), \quad C \in \mathrm{M}_{n\times m}(\mathbb{C}) \right\},$$

together with the super bracket

$$[x,y] = xy - (-1)^{ab} yx$$

for $x \in gl(n,n)_{\bar{a}}, \quad y \in gl(n,n)_{\bar{b}} \qquad a,b = 0, 1.$

Let $\gamma : V \longrightarrow V$ be the linear mapping which satisfies

$$\gamma(v) = (-1)^i v \text{ for } v \in V_{\bar{i}}.$$

We define the supertrace str on $gl(m,n)$ by,

$$str(x) = Tr(\gamma x) = TrA - TrD,$$

for $x = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in gl(m,n)$, where Tr is the usual matrix trace. The special linear Lie superalgebra $sl(m,n)$ is the subalgebra,

$$sl(m,n) = \{x \in gl(m,n) | str(x) = 0\},$$

of $gl(m,n)$ of matrices of supertrace zero.

There is a natural action of $gl(m,n)$ on V by matrix multiplication, which extends to an action on the k-fold tensor product $V^{\otimes k}$ of V. More precisely,

$$\begin{aligned} x\cdot(v_1\otimes v_2\otimes\cdots\otimes v_k) \\ =\sum_{i=1}^{k}(-1)^{ab_1+\cdots+ab_{i-1}}\, v_1\otimes\cdots\otimes v_{i-1}\otimes xv_i\otimes v_{i+1}\otimes\cdots\otimes v_k, \end{aligned}$$

where $x\in gl(n,n)_{\bar a}$, and $v_i\in V_{\bar b_i}$, $a,b_i=0$ or 1.

The symmetric group S_k on k-letters acts on $V^{\otimes k}$ by graded place permutation. So for $(i\;i+1)\in S_k$,

$$(i\;i+1)v_1\otimes\cdots\otimes v_k=(-1)^{a_ia_{i+1}}v_1\otimes\cdots\otimes v_{i-1}\otimes v_{i+1}\otimes v_i\otimes\cdots\otimes v_k,$$

where $v_j\in V_{a_j}$. The actions of S_k and $gl(m,n)$ on $V^{\otimes k}$ commute with each other (see for example, [**3**] or [**18**]).

For the rest of this paper we restrict our considerations to the case $\dim V_{\bar 0}=\dim V_{\bar 1}=n$. Let $\langle\ ,\rangle$ be a nondegenerate bilinear form on $V\times V$ such that

(i) $\langle v,w\rangle=(-1)^{ab}\langle w,v\rangle$ for $v\in V_{\bar a}$, and $w\in V_{\bar b}$.
(ii) $\langle v,w\rangle=0$ if $v,w\in V_{\bar 0}$ or $v,w\in V_{\bar 1}$.

Then we define the homogeneous spaces of the Lie superalgebra $\mathfrak{p}(n)$ as follows. For $a=0$ or 1,

$$\mathfrak{p}(n)_{\bar a}=\Big\{x\in gl(n,n)_{\bar a}\;\Big|\;\langle xv,w\rangle+(-1)^{ab}\langle v,xw\rangle=0 \quad \forall v\in V_{\bar b}, b=0,\text{ or }1,\forall w\in V\Big\}.$$

Then $\mathfrak{p}(n)=\mathfrak{p}(n)_{\bar 0}\oplus\mathfrak{p}(n)_{\bar 1}$ is a subsuperalgebra of $gl(n,n)$.

Since the bilinear form is nondegenerate on V, there exists a basis $B=B_0\cup B_1$ for V such that $B_0=\{e_1,\dots,e_n\}$ is a basis for $V_{\bar 0}$ and $B_1=\{e_{n+1},\dots,e_{n+n}\}$ is a basis for $V_{\bar 1}$, and

$$\langle e_{n+i},e_j\rangle=\langle e_j,e_{n+i}\rangle=\delta_{i,j},\quad \langle e_i,e_j\rangle=\langle e_{n+i},e_{n+j}\rangle=0,$$

for $i,j=1,2,\dots,n$. In other words e_i and e_{n+i} are dual to each other with respect to the bilinear form. So we will use the notation $e_i{}^*:=e_{n+i}$ and $e_{n+i}{}^*:=e_i$, for $i=1,\dots,n$.

The matrix of the bilinear form relative to the basis B is given by

$$\mathcal{F}_B=(\langle e_i,e_j\rangle)_{1\le i,j\le 2n}=\begin{pmatrix}0 & I_n\\ I_n & 0\end{pmatrix}.$$

Using $\mathcal{F}_B$, we can see that $\mathfrak{p}(n)$ can be represented as

$$\mathfrak{p}(n)=\left\{\begin{pmatrix}A & B\\ C & -A^T\end{pmatrix}\in \mathrm{M}_{2n\times 2n}(\mathbb{C})\;\middle|\;\begin{matrix}A,\,B,\,C\in gl(n),\\ B^T=B,\quad C^T=-C\end{matrix}\right\}$$

Here A^T denotes the usual matrix transpose of A.

In [**7**] Kac showed that

$$\begin{aligned}\mathfrak{sp}(n)&=\mathfrak{p}(n)\cap sl(n,n)\\ &=\left\{\begin{pmatrix}A & B\\ C & -A^T\end{pmatrix}\in \mathrm{M}_{2n\times 2n}(\mathbb{C})\;\middle|\;\begin{matrix}A\in sl(n) & B,\,C\in gl(n),\\ B^T=B, & C^T=-C\end{matrix}\right\}\end{aligned}$$

is a simple Lie superalgebra provided $n\ge 3$.

Let E_{st} denote the standard matrix unit which has 1 in the (s,t)-position and 0 elsewhere. We will denote homogeneous basis elements a_{ij}, b_{ij}, c_{ij} of $\mathfrak{p}(n)$ by

$$a_{ij} := E_{ij} - E_{j+n\, i+n} \in \left\{ \begin{pmatrix} A & 0 \\ 0 & -A^T \end{pmatrix} \middle| \, A \in gl(n) \right\} \qquad \text{for } 1 \le i, j \le n$$

$$b_{ij} := E_{i\, j+n} + E_{j\, i+n} \in \left\{ \begin{pmatrix} 0 & B \\ 0 & 0 \end{pmatrix} \middle| \, B \in gl(n),\ B^T = B \right\} \quad \text{for } 1 \le i \le j \le n$$

$$c_{ij} := E_{i+n\, j} - E_{j+n\, i} \in \left\{ \begin{pmatrix} 0 & 0 \\ C & 0 \end{pmatrix} \middle| \, C \in gl(n),\ C^T = -C \right\} \text{for } 1 \le i < j \le n.$$

For a semisimple Lie algebra, the Killing form, which is nondegenerate, plays an essential role in the theory of highest weight modules. A classical Lie superalgebra L is called *basic* when L has an even nondegenerate invariant bilinear form. The basic classical Lie superalgebras are close to the ordinary classical Lie algebras in many respects (for more information, see [**8**]). But it can be shown that there does not exist any nonzero invariant bilinear form on $\mathfrak{p}(n)$ if $n \ge 3$ (see for example [**7**] or [**15**]). Therefore we need a more general theory to construct the highest weight modules for Lie superalgebras which are not basic classical.

I. Penkov and V. Serganova developed a general way to construct highest weight modules of arbitrary finite-dimensional Lie superalgebras [**14**]. We fix $\mathfrak{h}$, the set of all the diagonal matrices in $\mathfrak{p}(n)$, as a Cartan subalgebra of $\mathfrak{p}(n)$. A linear functional $\alpha \in \mathfrak{h}^*$ is a *root* of $\mathfrak{p}(n)$ if and only if $\mathfrak{p}(n)_\alpha = \{x \in \mathfrak{p}(n) | [h,x] = \alpha(h)x,\ \forall h \in \mathfrak{h}\} \ne (0)$. Then $\mathfrak{p}(n)$ has the root space decomposition relative to $\mathfrak{h}$,

$$\mathfrak{p}(n) = \mathfrak{h} \oplus \bigoplus_{\alpha \in \mathfrak{h}^*} \mathfrak{p}(n)_\alpha$$

The set $\Delta = \{\alpha \in \mathfrak{h}^* \setminus 0 | \mathfrak{p}(n)_\alpha \ne (0)\}$ is the *set of roots* of $\mathfrak{p}(n)$. Penkov and Serganova developed a way to construct generalized triangular decompositions of $\mathfrak{p}(n)$, even though we cannot define simple roots of $\mathfrak{p}(n)$. From [**14**] we have the following triangular decomposition of $\mathfrak{p}(n)$;

THEOREM 1.1. [**14**] *There is a decomposition of $\Delta = \Delta_+ \cup \Delta_-$ such that*

$$\mathfrak{p}(n) = \mathfrak{p}(n)_- \oplus \mathfrak{h} \oplus \mathfrak{p}(n)_+,$$

$\mathfrak{p}(n)_+ = \bigoplus_{\alpha \in \Delta_+} \mathfrak{p}(n)_\alpha$ *is the* $\mathbb{C}$*-span of* $\{a_{ij} | 1 \le i < j \le n\} \cup \{b_{ij} | 1 \le i \le j \le n\}$,
$\mathfrak{h}$ *is the set of diagonal matrices in* $\mathfrak{p}(n)$ *which is the* $\mathbb{C}$*-span of* $\{a_{ii} | i = 1, \dots n\}$ *and*
$\mathfrak{p}(n)_- = \bigoplus_{\alpha \in \Delta_-} \mathfrak{p}(n)_\alpha$ *is the* $\mathbb{C}$*-span of* $\{a_{ij} | 1 \le j < i \le n\} \cup \{c_{ij} | 1 \le i < j \le n\}$.

Here we note that there is no automorphism τ of $\mathfrak{p}(n)$ so that $\tau(\mathfrak{p}(n)_+) = \mathfrak{p}(n)_-$ and $\tau(\mathfrak{p}(n)_-) = \mathfrak{p}(n)_+$. In fact these spaces have different dimensions.

DEFINITION 1.2. A $\mathfrak{p}(n)$-module V is a highest weight module if and only if V is generated over $\mathfrak{p}(n)$ by a weight vector $v_+ \in V$ such that $\mathfrak{p}(n)_+ \cdot v_+ = (0)$. We say $\lambda \in \mathfrak{h}^*$ is the weight of v_+ if $h \cdot v_+ = \lambda(h) v_+$, for all $h \in \mathfrak{h}$.

From now on we will adopt the convention on parities that $p(x) = a$ if $0 \ne x \in \mathfrak{p}(n)_{\bar{a}}$ and $p(v) = b$ if $0 \ne v \in V_{\bar{b}}$.

2. The centralizer algebra of $\mathfrak{p}(n)$ on $V^{\otimes k}$

We describe the full centralizer algebra of $\mathfrak{p}(n)$ on $V^{\otimes k}$ in this section.

Consider V^*, the dual vector space of V. Then V^* is also $\mathbb{Z}_2$-graded so $V^* = (V^*)_{\bar{0}} \oplus (V^*)_{\bar{1}}$, where $(V^*)_{\bar{i}} = (V_{\bar{i}})^*$, and V^* is a $\mathfrak{p}(n)$-module by

$$(x \cdot g)(w) = -(-1)^{p(x)p(g)} g(x \cdot w), \quad \forall w \in V,$$

for $x \in \mathfrak{p}(n)$ and $g \in V^*$.

Define a linear map $f : V \longrightarrow V^*, \quad v \longmapsto f_v$ by $f_v(w) = \langle v, w\rangle$, for $v, w \in V$. Then f is $\mathfrak{p}(n)$-module isomorphism i.e.,

$$x \cdot f_v = (-1)^{a \cdot 1} f_{x \cdot v}, \quad x \in \mathfrak{p}(n)_{\bar{a}}$$

Moreover we see $f : V_{\bar{0}} \longrightarrow (V^*)_{\bar{1}}$, and $V_{\bar{1}} \longrightarrow (V^*)_{\bar{0}}$, i.e., f is a $\mathfrak{p}(n)$-module isomorphism of parity 1.

There is also a $\mathfrak{p}(n)$-module structure on $\mathrm{End}(V)$ defined by

$$(x \cdot \varphi)(w) = x \cdot \varphi(w) - (-1)^{p(x)p(\varphi)} \varphi(x \cdot w),$$

for $x \in \mathfrak{p}(n)$ and $\varphi \in \mathrm{End}(V)$. Also we have that $V \otimes V^*$ is isomorphic to $\mathrm{End}(V)$ by

$$V \otimes V^* \longrightarrow \mathrm{End}(V), \qquad v \otimes g \mapsto \varphi_{v,g},$$

where for all $w \in V$, $\varphi_{v,g}(w) = g(w)v$. By this series of $\mathfrak{p}(n)$-module isomorphisms, $V \otimes V$ is isomorphic to $\mathrm{End}(V)$:

$$\begin{array}{ccccc} V \otimes V & \xrightarrow{1 \otimes f} & V \otimes V^* & \longrightarrow & \mathrm{End}(V) \\ e_i \otimes {e_j}^* & \longmapsto & (-1)^{p(e_i)} e_i \otimes f_{e_j^*} & \longmapsto & (-1)^{p(e_i)} E_{ij} \\ & & & & \\ \sum_{i=1}^{2n} (-1)^{p(e_i)} e_i \otimes {e_i}^* & \longmapsto & & \longrightarrow & I_V \end{array}$$

Because the identity map I_V on V is a $\mathfrak{p}(n)$ invariant, $\sum_{i=1}^{2n} (-1)^{p(e_i)} e_i \otimes {e_i}^*$ is a $\mathfrak{p}(n)$ invariant.

Define the *contraction* map $c \in \mathrm{End}(V^{\otimes 2})$ by

$$c(v_1 \otimes v_2) = \langle v_1, v_2\rangle \sum_{i=1}^{2n} (-1)^{p(e_i)} e_i \otimes e_i^*.$$

Since a $\mathfrak{p}(n)$-module invariant is killed by $\mathfrak{p}(n)$, it's easy to show

$$x \cdot c(v_1 \otimes v_2) = 0 = c \cdot x(v_1 \otimes v_2).$$

So $c \in \mathrm{End}_{\mathfrak{p}(n)}(V^{\otimes 2})$ and $c(V^{\otimes 2})$ is 1-dimensional submodule of $V \otimes V$.

Let s be the action of $(12) \in S_2$ on $V^{\otimes 2}$, so

$$s(v_1 \otimes v_2) = (-1)^{p(v_1)p(v_2)} v_2 \otimes v_1.$$

Then $s \in \mathrm{End}_{\mathfrak{p}(n)}(V^{\otimes 2})$ since the action of S_2 commutes with the action of $\mathfrak{p}(n)$ on $V^{\otimes 2}$.

Define $\mathfrak{e}_i, \mathfrak{s}_i, \in \mathrm{End}_{\mathfrak{p}(n)}(V^{\otimes k})$, $i = 1, 2, \ldots, k-1$, by

$$\mathfrak{e}_i = {I_V}^{\otimes (i-1)} \otimes c \otimes {I_V}^{\otimes (k-i-1)}$$

$$\mathfrak{s}_i = {I_V}^{\otimes (i-1)} \otimes s \otimes {I_V}^{\otimes (k-i-1)}$$

PROPOSITION 2.1. *$\mathfrak{e}_i$ and $\mathfrak{s}_i$ satisfy the following relations:*

$$\begin{aligned} {\mathfrak{s}_i}^2 = 1, \quad {\mathfrak{e}_i}^2 = 0, \quad \mathfrak{e}_i\mathfrak{s}_i = -\mathfrak{e}_i, \quad \mathfrak{s}_i\mathfrak{e}_i = \mathfrak{e}_i, &\qquad 1 \le i \le k-1, \\ \mathfrak{s}_i\mathfrak{s}_j = \mathfrak{s}_j\mathfrak{s}_i,\ \mathfrak{s}_i\mathfrak{e}_j = \mathfrak{e}_j\mathfrak{s}_i,\ \mathfrak{e}_i\mathfrak{e}_j = \mathfrak{e}_j\mathfrak{e}_i, &\qquad |i-j| \ge 2, \\ \mathfrak{s}_i\mathfrak{s}_{i+1}\mathfrak{s}_i = \mathfrak{s}_{i+1}\mathfrak{s}_i\mathfrak{s}_{i+1},\ \mathfrak{e}_{i+1}\mathfrak{e}_i\mathfrak{e}_{i+1} = -\mathfrak{e}_{i+1},\ \mathfrak{e}_i\mathfrak{e}_{i+1}\mathfrak{e}_i = -\mathfrak{e}_i, &\qquad 1 \le i \le k-2, \\ \mathfrak{s}_i\mathfrak{e}_{i+1}\mathfrak{e}_i = -\mathfrak{s}_{i+1}\mathfrak{e}_i,\ \mathfrak{e}_{i+1}\mathfrak{e}_i\mathfrak{s}_{i+1} = -\mathfrak{e}_{i+1}\mathfrak{s}_i &\qquad 1 \le i \le k-2. \end{aligned}$$

DEFINITION 2.2. Let A_k be the unital associative algebras generated by $\mathfrak{x}_1, \dots, \mathfrak{x}_{k-1}, \mathfrak{y}_1, \dots, \mathfrak{y}_{k-1}$ with defining relations

$$\begin{aligned} {\mathfrak{x}_i}^2 = 1,\ {\mathfrak{y}_i}^2 = 0,\ \mathfrak{y}_i\mathfrak{x}_i = -\mathfrak{y}_i,\ \mathfrak{x}_i\mathfrak{y}_i = \mathfrak{y}_i, &\qquad 1 \le i \le k-1, \\ \mathfrak{x}_i\mathfrak{x}_j = \mathfrak{x}_j\mathfrak{x}_i,\ \mathfrak{x}_i\mathfrak{y}_j = \mathfrak{y}_j\mathfrak{x}_i,\ \mathfrak{y}_i\mathfrak{y}_j = \mathfrak{y}_j\mathfrak{y}_i, &\qquad |i-j| \ge 2, \\ \mathfrak{x}_i\mathfrak{x}_{i+1}\mathfrak{x}_i = \mathfrak{x}_{i+1}\mathfrak{x}_i\mathfrak{x}_{i+1},\ \mathfrak{y}_{i+1}\mathfrak{y}_i\mathfrak{y}_{i+1} = -\mathfrak{y}_{i+1},\ \mathfrak{y}_i\mathfrak{y}_{i+1}\mathfrak{y}_i = -\mathfrak{y}_i, &\qquad 1 \le i \le k-2, \\ \mathfrak{x}_i\mathfrak{y}_{i+1}\mathfrak{y}_i = -\mathfrak{x}_{i+1}\mathfrak{y}_i,\ \mathfrak{y}_{i+1}\mathfrak{y}_i\mathfrak{x}_{i+1} = -\mathfrak{y}_{i+1}\mathfrak{x}_i &\qquad 1 \le i \le k-2. \end{aligned}$$

Note that the defining relations for $\mathfrak{x}_i$, $i = 1, \dots, k-1$ in Definition 2.2 are those of the symmetric group S_k. Hence we see that there is a copy of $\mathbb{C}S_k$ in A_k.

PROPOSITION 2.3. *There is a representation $\Psi\colon A_k \longrightarrow \mathrm{End}_{\mathfrak{p}(n)}(V^{\otimes k})$ of A_k given by $\Psi(\mathfrak{x}_i) = \mathfrak{s}_i$ and $\Psi(\mathfrak{y}_i) = \mathfrak{e}_i$.*

A *k-diagram* is a graph with two rows of k vertices each, one above the other, and k edges such that each vertex is incident to precisely one edge. The k-diagrams form a basis for the Brauer algebra $B_k(\eta)$. Because the relations in A_k are very similar to the relations for the Brauer algebra $B_k(0)$ (with $\eta = 0$), we guess that there should be a close relation between these two algebras. In particular, we would hope to represent the basis elements of A_k using k-diagrams, as in the case of the Brauer algebra.

Let $\mathcal{F}$ denote the free associative algebra with 1 on a set $x_1, x_2, \dots, x_m$ over a field k. Give the set X of all monomials in $x_1, \dots, x_m$ the lexicographic ordering $\le$. Let S be a set of pairs of the form $\sigma = (w_\sigma, f_\sigma)$, where $w_\sigma \in X$ and $f_\sigma \in \mathcal{F}$ being a linear combination of monomials $< w_\sigma$. For any $\sigma \in S$ and $A, B \in X$, let $r_{A\sigma B}$ denote the linear map sending $Aw_\sigma B$ to $Af_\sigma B$ and fixing all other monomials. Let R denote the semigroup generated by the $\{r_{A\sigma B} | \sigma \in S,\ A, B \in X\}$. Call $x \in X$ reduced if $r(x) = x$ for all $r \in R$. Let us call a 5-tuple $(\sigma, \tau; A, B, C) \in S^2 \times X^3$ for which $w_\sigma = AB$, $w_\tau = BC$, an *ambiguity* of S. An ambiguity is resolvable if there exists $r, r' \in R$ such that $r(f_\sigma C) = r'(Af_\tau)$.

LEMMA 2.4. *(The Diamond Lemma)*[**4**]
All ambiguities of S are resolvable if and only if the reduced elements under R form a k-basis for the quotient algebra $\mathcal{F}/\langle w_\sigma - f_\sigma : \sigma \in S\rangle$.

Generally it is not true that two algebras, which have the same generating elements and similar generating relations, have similar structures. However, in our case, we use Lemma 2.4 to prove

THEOREM 2.5.

$$\dim_{\mathbb{C}} A_k = (2k-1)!! = (2k-1)(2k-3)\cdots 3 \cdot 1 = \dim_{\mathbb{C}} B_k(0).$$

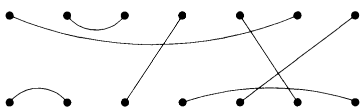
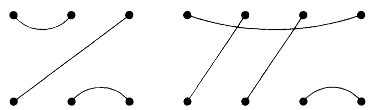
Moreover the k-diagrams form a basis for $B_k(0)$ and for A_k, and the product of two k-diagrams in A_k can be found using their product in $B_k(0)$. More precisely, let d_1 , d_2 be any two k-diagrams. Then the product $d_1 * d_2$ in A_k can be written as

$$d_1 * d_2 = \pm d_1 \circ d_2,$$

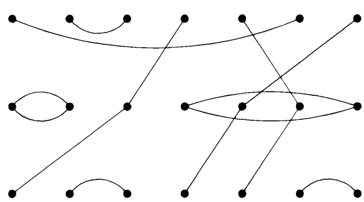
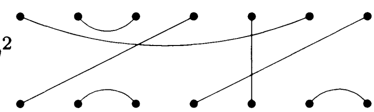
where $d_1 \circ d_2$ is the multiplication in $B_k(0)$. We have not succeeded yet in determining a closed form formula for the sign. But there is a way to figure out the sign for any two of k-diagrams given to us. We present an example below.

Assume $\eta \in \mathbb{C}$. The product of two k-diagrams d_1 and d_2 in the Brauer algebra $B_k(\eta)$ is obtained by placing d_1 above d_2 and identifying the vertices in the bottom row of d_1 with the corresponding vertices in the top row of d_2.

EXAMPLE 2.6. If

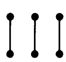
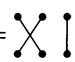
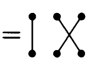
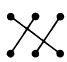
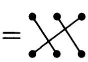
$d_1 =$  , $d_2 =$ 

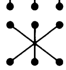
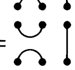
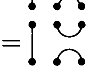
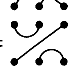
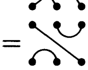
then

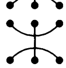
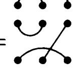
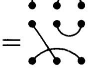
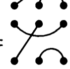
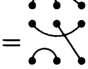
$d_1 \circ d_2 =$  $= \eta^2$ 

The power on η records the number of closed cycles in the middle, which in this example is 2. The algebra $B_k(0)$ has the parameter η specialized to 0. Thus in $B_k(0)$, $d_1 \circ d_2 = 0$ in this example.

Now let's consider A_3. The dimension of A_3 is $3!! = 5 \cdot 3 \cdot 1 = 15$. We assign to each basis element of A_3 with a 3-diagram:

$1 =$ , $\mathfrak{x}_1 =$ , $\mathfrak{x}_2 =$ , $\mathfrak{x}_1\mathfrak{x}_2 =$ , $\mathfrak{x}_2\mathfrak{x}_1 =$ ,

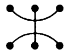
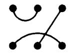
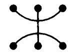
$\mathfrak{x}_1\mathfrak{x}_2\mathfrak{x}_1 =$ , $\mathfrak{y}_1 =$ , $\mathfrak{y}_2 =$ , $\mathfrak{y}_1\mathfrak{y}_2 =$ , $\mathfrak{y}_2\mathfrak{y}_1 =$ ,

$\mathfrak{x}_1\mathfrak{y}_2\mathfrak{x}_1 =$ , $\mathfrak{y}_1\mathfrak{x}_2 =$ , $\mathfrak{y}_2\mathfrak{x}_1 =$ , $\mathfrak{x}_1\mathfrak{y}_2 =$ , $\mathfrak{x}_2\mathfrak{y}_1 =$ .

Applying the procedure described in [**4**], we obtain a reduction system S on the generators $1, \mathfrak{x}_1, \mathfrak{x}_2, \mathfrak{y}_1, \mathfrak{y}_2$ so that all ambiguities of S are resolvable. (For more detailed information, see [**4**].) In this case the reduction system S consists of the following relations:

$$\mathfrak{x}_1^2 = \mathfrak{x}_2^2 = 1, \quad \mathfrak{y}_1^2 = \mathfrak{y}_2^2 = 0, \quad \mathfrak{y}_i\mathfrak{x}_i = -\mathfrak{y}_i, \quad \mathfrak{x}_i\mathfrak{y}_i = \mathfrak{y}_i, \quad \text{for } i = 1, 2$$
$$\mathfrak{x}_2\mathfrak{x}_1\mathfrak{x}_1 = \mathfrak{x}_1\mathfrak{x}_2\mathfrak{x}_1, \quad \mathfrak{y}_1\mathfrak{y}_2\mathfrak{y}_1 = -\mathfrak{y}_1, \quad \mathfrak{y}_2\mathfrak{y}_1\mathfrak{y}_2 = -\mathfrak{y}_2, \quad \mathfrak{x}_1\mathfrak{y}_2\mathfrak{y}_1 = -\mathfrak{x}_2\mathfrak{y}_1$$
$$\mathfrak{y}_2\mathfrak{y}_1\mathfrak{x}_2 = -\mathfrak{y}_2\mathfrak{x}_1, \quad \mathfrak{x}_1\mathfrak{x}_2\mathfrak{y}_1 = -\mathfrak{y}_2\mathfrak{y}_1, \quad \mathfrak{y}_2\mathfrak{x}_1\mathfrak{x}_2 = -\mathfrak{y}_2\mathfrak{y}_1, \quad \mathfrak{y}_1\mathfrak{x}_2\mathfrak{y}_1 = -\mathfrak{y}_1$$
$$\mathfrak{x}_2\mathfrak{x}_1\mathfrak{y}_2 = \mathfrak{y}_1\mathfrak{y}_2, \quad \mathfrak{x}_2\mathfrak{y}_1\mathfrak{y}_2 = \mathfrak{x}_1\mathfrak{y}_2, \quad \mathfrak{y}_2\mathfrak{x}_1\mathfrak{y}_2 = \mathfrak{y}_2, \quad \mathfrak{y}_1\mathfrak{x}_2\mathfrak{x}_1 = \mathfrak{x}_1\mathfrak{x}_2$$
$$\mathfrak{y}_1\mathfrak{y}_2\mathfrak{x}_1 = \mathfrak{y}_1\mathfrak{x}_2, \quad \mathfrak{x}_2\mathfrak{y}_1\mathfrak{x}_2 = \mathfrak{x}_1\mathfrak{y}_2\mathfrak{x}_1.$$

Using this reduction system, we easily get the products of 3-diagrams in A_3. For example,

 $*$ 
$$
\begin{aligned}
&=(\mathfrak{x}_1\mathfrak{y}_2\mathfrak{x}_1)(\mathfrak{y}_1\mathfrak{x}_2) = \mathfrak{x}_1\mathfrak{y}_2(\mathfrak{x}_1\mathfrak{y}_1)\mathfrak{x}_2 \\
&=\mathfrak{x}_1(\mathfrak{y}_2\mathfrak{y}_1\mathfrak{x}_2) = -\mathfrak{x}_1\mathfrak{y}_2\mathfrak{x}_1 \\
&= -
\end{aligned}
$$
.

Note that the even part $\mathfrak{p}(n)_{\bar{0}}$ of $\mathfrak{p}(n)$ is isomorphic to the general Lie algebra $gl(n)$, and as a $\mathfrak{p}(n)_{\bar{0}}$-module V is isomorphic to the direct sum $T \oplus U$, where $T = \mathbb{C}^n$ is the n-dimensional natural representation of $gl(n)$ and $U = T^*$ is the dual of T. The $gl(n)$-invariants of the mixed tensor space $T^{\otimes k} \otimes (T^*)^{\otimes l}$ are determined in [**1**]. Using their results, we can prove a result which could count as an analogue of *Schur-Weyl duality* for the Lie superalgebra $\mathfrak{p}(n)$.

THEOREM 2.7.
(a) $\Psi : A_k \longrightarrow End_{\mathfrak{p}(n)}(V^{\otimes k})$ *is a faithful representation of* A_k *if* $n \geq k$.
(b) $\Psi(A_k)$ *is the full centralizer of* $\mathfrak{p}(n)$, *if* $n \geq k$. *In other words,*

$$End_{\mathfrak{p}(n)}(V^{\otimes k}) = \Psi(A_k).$$

If the centralizer algebra on $V^{\otimes k}$ is semisimple, then $V^{\otimes k}$ decomposes into a sum of indecomposable submodules using minimal idempotents of the centralizer algebra. Therefore it is interesting to know whether A_k is semisimple.

THEOREM 2.8. *A_k is not semisimple for all $k \geq 2$.*

3. Maximal vectors of $\mathfrak{p}(n)$ in $V^{\otimes k}$

In this section we construct maximal vectors of $\mathfrak{p}(n)$ in the tensor space $V^{\otimes k}$ using the centralizer algebra A_k. Note that we regard $\mathbb{C}S_k$ as a subalgebra of A_k

Define the contraction mapping $c_{p,q}$ on the (p,q)-tensor slot by

$$c_{p,q} := \sigma^{-1}\mathfrak{y}_1\sigma.$$

where $\sigma \in \mathbb{C}S_k$ is such that $\sigma(1) = p$, and $\sigma(2) = q$. It is not difficult to show that $c_{p,q}$ is well-defined.

LEMMA 3.1. *$c_{p,q}$ is independent of the choice of σ.*

If $\underline{p} = \{p_1, \dots, p_j\}$ and $\underline{q} = \{q_1, \dots, q_j\}$ are two disjoint ordered subsets of $\{1, \dots, k\}$ such that $p_i < q_i$, for all $i = 1, \dots j$, then we set

$$
\begin{aligned}
c_{\underline{p},\underline{q}} :&= c_{p_1,q_1} \cdots c_{p_j,q_j}, \quad i = 1, \dots, \left\lfloor \frac{k}{2} \right\rfloor \\
c_{\emptyset,\emptyset} :&= \textbf{identity}.
\end{aligned}
$$

Let $(\underline{p},\underline{q}) = \{(p_1,q_1), \dots, (p_j,q_j)\}$, and denote by $p(j)$ the set of all such $(\underline{p},\underline{q})$. Also we set $P = \bigcup_{j=0}^{\lfloor \frac{k}{2} \rfloor} p(j)$.

Let $\mathcal{H}$ be the set of all diagonal matrices in $gl(n,n)$. Note the Cartan subalgebra $\mathfrak{h}$ of $\mathfrak{p}(n)$ is contained in $\mathcal{H}$. For $i = 1, 2, \dots, 2n$, define a linear functional $\varepsilon_i : \mathcal{H} \longrightarrow \mathbb{C}$, by $\varepsilon_i(E_{jj}) = \delta_{ij}$. Let λ be a partition of $l \leq k$. Then we denote by $\ell(\lambda)$ the length of λ, which is the number of nonzero parts of λ. For each partition

$\lambda = (\lambda_1, \lambda_2, \lambda_3, \ldots, \lambda_{2n})$ with length $\ell(\lambda) \leq 2n$, we associate a weight of $\mathfrak{p}(n)$ in the following way;

$$\lambda = \lambda_1\varepsilon_1 + \cdots + \lambda_{2n}\varepsilon_{2n}.$$

A *standard tableau* T of shape λ is obtained by filling in the frame of λ with elements of $1, \ldots, k$ so that the entries increase across the rows from left to right and down the columns. We set $\ell(T) := \ell(\lambda)$. We associate two subgroups in the symmetric group S_k to T. The *row group* R_T consists of all permutations which permute the entries within each row. Similarly, the *column group* C_T is the group consisting of all permutations permuting the entries within the columns. Define s_T, an element of the group algebra $\mathbb{C}(S_k)$, by

$$s_T := \left(\sum_{\psi \in R_T} \psi\right)\left(\sum_{\phi \in C_T} sgn(\phi)\phi\right).$$

Then s_T has the property that there is some $h(\lambda) \in \mathbb{Z}^+$ that only depends on the shape of T such that ${s_T}^2 = h(\lambda)s_T$ (See [**19**]). Now the *Young symmetrizer* determined by T is the idempotent defined by

$$y_T := \frac{1}{h(\lambda)} s_T.$$

EXAMPLE 3.2. Assume $n = 8$, $k = 14$, and $\lambda \vdash 10$. Then

$$\lambda = \ydiagram{4,2,2,1,1} \qquad \begin{matrix} \lambda_1 = 4 \\ \lambda_2 = 2 \\ \lambda_3 = 2 \\ \lambda_4 = 1 \\ \lambda_5 = 1 \end{matrix}. \qquad \text{Let } T = \quad \wedge \ \overset{<}{\begin{ytableau} 1 & 6 & 11 & 14 \\ 2 & 8 \\ 4 & 9 \\ 7 \\ 10 \end{ytableau}}\,.$$

Then $\lambda = 4\varepsilon_1 + 2\varepsilon_2 + 2\varepsilon_3 + \varepsilon_4 + \varepsilon_5$, and $\lambda_6 = \cdots = \lambda_{16} = 0$.

Let $\lambda = (\lambda_1, \ldots, \lambda_{2n}) \vdash l$, a partition of l, where $l = k - 2j$ for $j = 0, \ldots, \lfloor \frac{k}{2} \rfloor$. Let $\mathcal{ST}_\lambda\big((\underline{p} \cup \underline{q})^c\big)$ denote the set of standard tableaux of shape λ with entries in $(\underline{p} \cup \underline{q})^c$, where $(\underline{p}, \underline{q}) \in p(j)$. Fix $T \in \mathcal{ST}_\lambda\big((\underline{p} \cup \underline{q})^c\big)$. Define the associated simple tensor $w_{T,\underline{p},\underline{q}} = w_1 \otimes \cdots \otimes w_k$ by

$$w_i = \begin{cases} e_1 & \text{if } i \in \underline{p}, \\ e_1^* = e_{n+1} & \text{if } i \in \underline{q}, \\ e_j & \text{if } i \in (\underline{p} \cup \underline{q})^c \text{ and } i \text{ is in } j\text{th row of } T. \end{cases}$$

Now define a tensor θ by $\theta := y_T c_{\underline{p},\underline{q}} w_{T,\underline{p},\underline{q}}$, where y_T is the Young symmetrizer determined by T. Then we can show θ is a maximal vector of weight $\lambda = \lambda_1\varepsilon_1 + \cdots + \lambda_{2n}\varepsilon_{2n}$, which means

$$\mathfrak{p}_+(n)\theta = 0, \qquad h \cdot \theta = \lambda(h)\theta, \quad \forall h \in \mathfrak{h}.$$

THEOREM 3.3. *If $n \geq k$, then*

$$\left\{ y_T c_{\underline{p},\underline{q}} w_{T,\underline{p},\underline{q}} \;\middle|\; (\underline{p}, \underline{q}) \in P,\ T \in \mathcal{ST}\Big((\underline{p} \cup \underline{q})^c\Big), \quad \ell(T) \leq n \right\}$$

is a linearly independent set of maximal vectors.

4. The decomposition of $V^{\otimes k}$

In this section we obtain the decomposition of the $\mathfrak{p}(n)$-module $V^{\otimes k}$ for $k = 2$ and 3 into indecomposable modules using the centralizer algebra A_k of $\mathfrak{p}(n)$. For larger values of k, we also hope that this kind of decomposition can be obtained using A_k. We use the decompositions of $V^{\otimes 2}$ and $V^{\otimes 3}$ to conclude that $V^{\otimes k}$ is not completely reducible for any $k \geq 2$.

4.1. Decomposition of $V^{\otimes 2}$.

We note that the centralizer algebra A_2 is not semisimple. In fact the radical $\mathrm{Rad}(A_2)$ of A_2 is equal to $\langle \mathfrak{y}_1 \rangle$. In this case it follows from Theorem 3.3 that

$$\begin{aligned}
\theta_1 &= y_{\boxed{1}\boxed{2}}\, e_1 \otimes e_1 = e_1 \otimes e_1 \\
\theta_2 &= y_{\substack{\boxed{1}\\\boxed{2}}}\, e_1 \otimes e_2 = \frac{1}{2}(e_1 \otimes e_2 - e_2 \otimes e_1) \\
\theta_3 &= c_{1,2} e_1 \otimes {e_1}^* = \sum_{i=1}^{2n} (-1)^{p(e_i)} e_i \otimes {e_i}^*
\end{aligned}$$

are linearly independent maximal vectors of $\mathfrak{p}(n)$ in $V^{\otimes 2}$. By direct computation we can show there are no more maximal vectors.

As a module for $gl(n,n)$ (and hence for $\mathfrak{p}(n)$),

$$V^{\otimes 2} = y_{\boxed{1}\boxed{2}} \left(V^{\otimes 2}\right) \oplus y_{\substack{\boxed{1}\\\boxed{2}}} \left(V^{\otimes 2}\right).$$

Note that $\theta_1 \in y_{\boxed{1}\boxed{2}}(V^{\otimes 2})$ and θ_2, $\theta_3 \in y_{\substack{\boxed{1}\\\boxed{2}}}(V^{\otimes 2})$. These modules are irreducible for $gl(n,n)$, but not for $\mathfrak{p}(n)$. In fact we have the following:

4.1.1. $y_{\boxed{1}\boxed{2}} \left(V^{\otimes 2}\right)$ is an indecomposable $\mathfrak{p}(n)$-module which is not irreducible.

θ_1 is the unique maximal vector (up to scalar multiples) in the submodule $y_{\boxed{1}\boxed{2}} \left(V^{\otimes 2}\right)$ and $\mathcal{U}(L)\theta_1$ is the unique $\mathfrak{p}(n)$-submodule. It has codimension 1. Here $\mathcal{U}(L)$ is the universal enveloping algebra of the Lie superalgebra $L = \mathfrak{p}(n)$. So we have that $\mathcal{U}(L)\theta_1 \cong V(2\varepsilon_1)$ is the irreducible L-module of highest weight $2\varepsilon_1$. We have the following diagram of submodules.

$$\begin{array}{c}
y_{\boxed{1}\boxed{2}} \left(V^{\otimes 2}\right) \\
\Big| \, 1 \\
\mathcal{U}(L)\theta_1 = y_{\boxed{1}\boxed{2}} \left(V^{\otimes 2}\right) \cap \ker c \\
\Big| \, 2n^2 - 1 \\
(0)
\end{array}$$

Therefore we obtain the dimension formula for $V(2\varepsilon_1)$.

$$\begin{aligned}
\dim V(2\varepsilon_1) &= \dim y_{\boxed{1}\boxed{2}} \left(V^{\otimes 2}\right) - 1 \\
&= 2n^2 - 1.
\end{aligned}$$

4.1.2. $y_{\begin{smallmatrix}\boxed{1}\\\boxed{2}\end{smallmatrix}}\left(V^{\otimes 2}\right)$ is an indecomposable $\mathfrak{p}(n)$-module which is not irreducible.

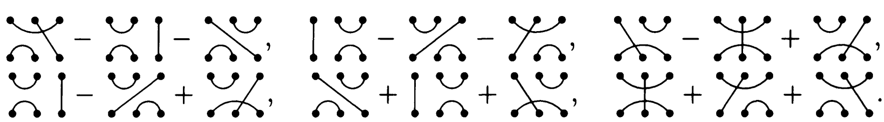
In this case, $\mathcal{U}(L)\theta_2$ is the same as $y_{\begin{smallmatrix}\boxed{1}\\\boxed{2}\end{smallmatrix}}\left(V^{\otimes 2}\right)$. And $\mathcal{U}(L)\theta_3$ is a one-dimensional trivial submodule. So $y_{\begin{smallmatrix}\boxed{1}\\\boxed{2}\end{smallmatrix}}\left(V^{\otimes 2}\right)\big/\mathbb{C}\theta_3 \cong V(\varepsilon_1+\varepsilon_2)$, the irreducible $\mathfrak{p}(n)$-module of highest weight $\varepsilon_1+\varepsilon_2$.

$$\begin{array}{c} y_{\begin{smallmatrix}\boxed{1}\\\boxed{2}\end{smallmatrix}}\left(V^{\otimes 2}\right) = \mathcal{U}(L)\theta_2 \\ \Big| \, 2n^2-1 \\ \mathcal{U}(L)\theta_3 = \mathrm{im}c \\ \Big| \, 1 \\ (0) \end{array}$$

From this we can determine the dimension of the irreducible highest weight module $V(\varepsilon_1+\varepsilon_2)$,

$$\begin{aligned} \dim V(\varepsilon_1+\varepsilon_2) &= \dim y_{\begin{smallmatrix}\boxed{1}\\\boxed{2}\end{smallmatrix}}\left(V^{\otimes 2}\right) - 1 \\ &= 2n^2-1. \end{aligned}$$

4.2. Decomposition of $V^{\otimes 3}$. Note that A_3 is not semisimple. The radical $\mathrm{Rad}(A_3)$ of A_3 is the $\mathbb{C}$-span of



Note the dimension of $\mathrm{Rad}(A_3)$ is 5, so the dimension of $A_3/\mathrm{Rad}(A_3)$ is 10.

In this case we can show that all the linearly independent maximal vectors in $V^{\otimes 3}$ can be listed as

$$\begin{aligned} \theta_1 &= c_{1,2}e_1 \otimes {e_1}^* \otimes e_1 \\ \theta_2 &= c_{1,3}e_1 \otimes e_1 \otimes {e_1}^* \\ \theta_3 &= c_{2,3}e_1 \otimes e_1 \otimes {e_1}^* \\ \theta_4 &= y_{\boxed{1}\boxed{2}\boxed{3}}\, e_1 \otimes e_1 \otimes e_1 \\ \theta_5 &= y_{\begin{smallmatrix}\boxed{1}&\boxed{2}\\\boxed{3}&\end{smallmatrix}}\, e_1 \otimes e_1 \otimes e_2 \\ \theta_6 &= y_{\begin{smallmatrix}\boxed{1}&\boxed{3}\\\boxed{2}&\end{smallmatrix}}\, e_1 \otimes e_2 \otimes e_1 \\ \theta_7 &= y_{\begin{smallmatrix}\boxed{1}\\\boxed{2}\\\boxed{3}\end{smallmatrix}}\, e_1 \otimes e_2 \otimes e_3. \end{aligned}$$

As a $\mathfrak{p}(n)$-module, $V^{\otimes 3}$ decomposes as

$$V^{\otimes 3} = y_{\boxed{1}\boxed{2}\boxed{3}}\left(V^{\otimes 3}\right) \oplus y_{\begin{smallmatrix}\boxed{1}&\boxed{2}\\\boxed{3}&\end{smallmatrix}}\left(V^{\otimes 3}\right) \oplus y_{\begin{smallmatrix}\boxed{1}&\boxed{3}\\\boxed{2}&\end{smallmatrix}}\left(V^{\otimes 3}\right) \oplus y_{\begin{smallmatrix}\boxed{1}\\\boxed{2}\\\boxed{3}\end{smallmatrix}}\left(V^{\otimes 3}\right)$$

Also we know how these seven maximal vectors spread over $V^{\otimes 3}$:

$$\begin{aligned}
\theta_4 &\in y_{\ytableaushort{123}}(V^{\otimes 3})\\
\theta_5, \quad \theta_1 + 2\theta_2 + \theta_3 &\in y_{\ytableaushort{12,3}}(V^{\otimes 3})\\
\theta_3, \quad 2\theta_1 + \theta_2 - \theta_3 &\in y_{\ytableaushort{13,2}}(V^{\otimes 3})\\
\theta_7, \quad -\theta_1 + \theta_2 - \theta_3 &\in y_{\ytableaushort{1,2,3}}(V^{\otimes 3}).
\end{aligned}$$

4.2.1. $y_{\ytableaushort{123}}(V^{\otimes 3})$ is an indecomposable $\mathfrak{p}(n)$-module which is not irreducible.

θ_4 is the only maximal vector in this submodule and $\mathcal{U}(L)\theta_4$ is the only submodule of $y_{\ytableaushort{123}}(V^{\otimes 3})$. Therefore $\mathcal{U}(L)\theta_4$ is the unique irreducible $\mathfrak{p}(n)$-module with highest weight $3\varepsilon_1$.

$$\begin{array}{c}
y_{\ytableaushort{123}}\left(V^{\otimes 3}\right)\\
\Big|\\
\mathcal{U}(L)\theta_4 \cong V(3\varepsilon_1)\\
\Big|\\
(0)
\end{array}$$

Moreover

$$y_{\ytableaushort{123}}\left(V^{\otimes 3}\right)\Big/\mathcal{U}(L)\theta_4 \cong V(\varepsilon_1) \cong \mathbb{C}^{n+n}.$$

So we have the dimension of the irreducible highest weight module $V(3\varepsilon_1)$.

$$\begin{aligned}
\dim V(3\varepsilon_1) &= \dim y_{\ytableaushort{123}}\left(V^{\otimes 3}\right) - 2n\\
&= \frac{8n(2n^2+1)}{3} - 2n.
\end{aligned}$$

4.2.2. $y_{\ytableaushort{12,3}}(V^{\otimes 3})$ is a completely reducible $\mathfrak{p}(n)$-module.

We have the irreducible decomposition of $y_{\ytableaushort{12,3}}(V^{\otimes 3})$ in this case,

$$\begin{gathered}
y_{\ytableaushort{12,3}}(V^{\otimes 3}) = \mathcal{U}(L)\theta_5 \oplus \mathcal{U}(L)(\theta_1 + 2\theta_2 + \theta_3),\\
\mathcal{U}(L)\theta_5 \cong V(2\varepsilon_1 + \varepsilon_2) \quad \text{and} \quad \mathcal{U}(L)(\theta_1 + 2\theta_2 + \theta_3) \cong V(\varepsilon_1) \cong V
\end{gathered}$$

So we obtain the dimension of the irreducible highest weight module $V(2\varepsilon_1 + \varepsilon_2)$,

$$\begin{aligned}
\dim V(2\varepsilon_1 + \varepsilon_2) = \dim \mathcal{U}(L)\theta_5 &= \dim y_{\ytableaushort{12,3}}(V^{\otimes 3}) - 2n\\
&= \frac{2n(2n+1)(2n-1)}{3} - 2n.
\end{aligned}$$

4.2.3. $y_{\ytableaushort{13,2}}(V^{\otimes 3})$.

$y_{\ytableaushort{13,2}}(V^{\otimes 3})$ is isomorphic to $y_{\ytableaushort{12,3}}(V^{\otimes 3})$ as $\mathfrak{p}(n)$-modules. So $y_{\ytableaushort{13,2}}(V^{\otimes 3})$ is completely reducible.

4.2.4. $y_{\begin{smallmatrix}\boxed{1}\\ \boxed{2}\\ \boxed{3}\end{smallmatrix}}(V^{\otimes 3})$ is an indecomposable $\mathfrak{p}(n)$-module which is not irreducible.

There are two maximal vectors in this submodule, θ_7 and $-\theta_1+\theta_2-\theta_3$. The vector θ_7 will generate the whole module $y_{\begin{smallmatrix}\boxed{1}\\ \boxed{2}\\ \boxed{3}\end{smallmatrix}}(V^{\otimes 3})$, and $-\theta_1+\theta_2-\theta_3$ is a maximal vector of weight ε_1. So $\mathcal{U}(L)(-\theta_1+\theta_2-\theta_3)$ is an irreducible module which is isomorphic to $V=\mathbb{C}^{n+n}$. There are no other submodules in $y_{\begin{smallmatrix}\boxed{1}\\ \boxed{2}\\ \boxed{3}\end{smallmatrix}}(V^{\otimes 3})$. Therefore, we obtain the following diagram.

$$\begin{array}{c}
y_{\begin{smallmatrix}\boxed{1}\\ \boxed{2}\\ \boxed{3}\end{smallmatrix}}(V^{\otimes 3})=\mathcal{U}(L)\theta_7\\
\Big|\\
\mathcal{U}(L)(-\theta_1+\theta_2-\theta_3)\\
\Big|\,2n\\
(0)
\end{array}$$

$$\mathcal{U}(L)(-\theta_1+\theta_2-\theta_3)\cong V(\varepsilon_1)\cong V,$$
$$y_{\begin{smallmatrix}\boxed{1}\\ \boxed{2}\\ \boxed{3}\end{smallmatrix}}(V^{\otimes 3})\Big/\mathbb{C}(-\theta_1+\theta_2-\theta_3)\cong V(\varepsilon_1+\varepsilon_2+\varepsilon_3).$$

And we may compute the dimension of the irreducible highest weight module $V(\varepsilon_1+\varepsilon_2+\varepsilon_3)$,

$$\begin{aligned}
\dim V(\varepsilon_1+\varepsilon_2+\varepsilon_3) &= \dim y_{\begin{smallmatrix}\boxed{1}\\ \boxed{2}\\ \boxed{3}\end{smallmatrix}}(V^{\otimes 3})-2n\\
&=\frac{8n(2n^2+1)}{3}-2n.
\end{aligned}$$

For any contraction map $c\in\mathrm{End}_{\mathfrak{p}(n)}(V^{\otimes k})$, c maps $V^{\otimes k}$ onto $V^{\otimes k-2}$. So for each k, $V^{\otimes k}$ has a submodule M, which is isomorphic to $V^{\otimes 2}$ if k is even, or to $V^{\otimes 3}$ if k is odd. Since $V^{\otimes 2}$ and $V^{\otimes 3}$ are not completely reducible from our previous arguments, we have the following corollary.

COROLLARY 4.1. *$V^{\otimes k}$ is not completely reducible as a $\mathfrak{p}(n)$-module for any $k\geq 2$.*

References

[1] G. Benkart, M. Chakrabarti, T. Halverson, R. Leduc, C. Lee, and J. Stroomer, *Tensor product representations of general linear groups and their connections with Brauer algebras*, J. Algebra **166** (1994), 529–567.

[2] G. Benkart, C. Lee Shader, and A. Ram, *Tensor product representations for orthosymplectic Lie superalgebras*, to appear in Journal of Pure and Applied Algebra.

[3] A. Berele and A. Regev, *Hook Young diagrams with applications to combinatorics, and to representations of Lie superalgebras*, Adv. in Math. **64** (1987), 118–175.

[4] G. Bergman, *The diamond lemma for ring theory*, Adv. in Math. **29** (1978), 178–218.

[5] R. Brauer, *On algebras which are connected with semisimple Lie groups*, Ann. of Math. **38** (1937), 857–872.

[6] D. Fischman and S. Montgomery, *A Schur double centralizer theorem for cotriangular Hopf algebras and generalized Lie algebras*, J. of Algebra **168** (1994), 594–614.

[7] V. G. Kac, *Lie superalgebras*, Adv. in Math. **26** (1977), 8–96.

[8] V.G. Kac, *Representations of classical Lie superalgebras*, Differential Geometrical Methods in Mathematical Physics II, Lect. Notes in Math., vol. 676, Springer-Verlag, Berlin, Heidelberg, New York, 1978, pp. 597–626.

[9] C. Lee, *Construction of modules for Lie superalgebra of type C*, J. Algebra **176** (1995), no. 1, 249–264.

[10] C. Lee Shader, *Representations for Lie superalgebra* $spo(2m,1)$, to appear.

[11] D. Moon, *The centralizer algebras of Lie color algebras*, to appear in Communications in Algebra.

[12] ———, *Tensor product representations of the Lie superalgebra* $\mathfrak{p}(n)$ *and their centralizers*, submitted.

[13] ———, *Schur-Weyl dualities for Lie superalgebras and Lie color algebras*, Ph.D. thesis, University of Wisconsin-Madison, 1998.

[14] I. Penkov and V. Serganova, *Generic irreducible representations of finite-dimensional Lie superalgebras*, International Journal of Mathematics **5** (1994), 389–419.

[15] M. Scheunert, *The theory of Lie superalgebras*, Lecture Notes in Mathematics, vol. 716, Springer-Verlag, Berlin, 1979.

[16] I. Schur, *Über eine klasse von matrizen, die sich einer gegeben matrix zuordenen lassen*, Ph.D. thesis, 1901, reprinted in Gesamelte Abhandlungen vol. 1, 1-70.

[17] ———, *Über die rationalen Darstellungen der allgemeinen linearen Gruppe*, Preuss. Akad. Wiss. Sitz. (1927), 58–75, reprinted in Gesamelte Abhandlungen vol. 3, 68–85.

[18] A. N. Sergeev, *The tensor algebra of the identity representation as a module over the Lie superalgebras* $Gl(n,m)$ *and* $Q(n)$, Math. USSR Sbornik **51** (1985), no. 2, 419–427.

[19] H. Weyl, *Classical groups, their invariants and representations*, second ed., Princeton Mathematical Series, Princeton University Press, Princeton, 1946.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF WISCONSIN, MADISON, WI 53706 USA

http://dx.doi.org/10.1090/conm/224/03197

Contemporary Mathematics
Volume **224**, 1999

Drinfeld-Anderson Motives and Multicomponent KP Hierarchy

Igor Yu. Potemine

ABSTRACT. We define Drinfeld-Anderson motives and sheaves generalizing Drinfeld modules, Anderson t-motives and Laumon-Rapoport-Stuhler $\mathcal{D}$-elliptic sheaves. The first main result is a proof of an anti-equivalence of the category of Drinfeld-Anderson motives of τ-rank n over L and a certain subcategory of the category of commutative subrings of the matrix ring $\mathrm{M}_n(L[\tau])$ where τ is the Frobenius morphism. The second main result is a classification of Drinfeld-Anderson motives over finite fields. Analogies with (generalizations of) the Burchnall-Chaundy-Krichever theorem as well as the multicomponent KP hierarchy are given.

Introduction

It turns out that commutative subrings of certain non-commutative rings of operators are very important for the arithmetic algebraic geometry, the class field theory as well as integrable systems. Such subrings correspond to algebro-geometric data consisting of torsion-free sheaves on marked algebraic curves with some additional structures (including a sort of local or formal trivialization at marked points). We consider the case of ordinary differential operators in characteristic zero and the case of twisted polynomials of a Frobenius morphism in positive characteristic.

The structure of this paper is the following. The first four sections give a general survey of Burchnall-Chaundy, Krichever-Mulase and Drinfeld results about commutative subrings of non-commutative rings of operators. The next three sections is the original core of this paper. In section 5 Drinfeld-Anderson motives are defined and the first main theorem is proved (theorem 5.3). After that the phenomenon of existence of non-pure commutative subrings is described. We define a notion of pure Drinfeld-Anderson motives and extend it to a geometric definition of pure Drinfeld-Anderson sheaves over an arbitrary $\mathbb{F}_q$-scheme S. Further, a classification of Drinfeld-Anderson motives over finite fields is given (theorem 7.1). It is analogous to the classification of "usual" motives over finite fields in many ways (cf. [**Mi**]) although our motives are with "values in positive characteristic". In section 8 we discuss analogies between the category of Drinfeld-Anderson motives and the

1991 *Mathematics Subject Classification.* Primary 11G09; Secondary 58F07.

Supported by KIAS research grant M-97009.

multicomponent KP hierarchy. Finally, we mention further generalizations in the differential case.

David Goss underlined to the author the importance of an analytic uniformization of Drinfeld-Anderson motives. We do not discuss this topic in the paper only because it could lead us too far from our main purpose. The construction of such an uniformization does not seem to present any additional difficulties with respect to the case of t-motives ([**An1**], §2).

The notion of Drinfeld-Anderson motive seems to be new. Although this paper is self-contained, an interested reader can extract more background from the author's Ph.D. thesis ([**Po**], ch. 1).

Acknowledgments. I am very thankful to the organizers of the conference "Recent Progress in Algebra" for presenting me an opportunity to give a talk on the topic of this article. It is a pleasure for me to thank my colleagues and all members of KIAS for their help and for creating excellent atmosphere in the institute. I would like to thank also David Goss for his stimulating questions concerning analogies between (the category of) Drinfeld modules and KP hierarchy.

1. Krichever modules of rank 1

Let L be a field of characteristic zero and denote $L[[t]][d/dt]$ the ring of ordinary differential operators. The systematic study of commutative subrings of this ring was done for the first time in twenties in the series of papers by Burchnall and Chaundy [**BCh**]. Although some results goes back at least to Wallenberg and Schur (see the introduction to the article [**Mu1**]). Half of century later Krichever [**Kr**] rediscovered the construction of Burchnall and Chaundy and related it to the integration of nonlinear partial differential equations of Korteweg-de Vries and Kadomtsev-Petviashvili type.

Let X be a projective curve over a field L and fix a smooth closed point P on it.

THEOREM 1.1. (Burchnall-Chaundy-Krichever, [**Mum**]) *The category of commutative subrings A of $R = L[[t]][d/dt]$ of rank 1 containing L (called Krichever modules of rank 1) up to the conjugation by invertible elements of $L[[t]]$ is anti-equivalent to the category of quadruples $(X, P, \mathcal{F}, \eta)$ where $\mathcal{F}$ is a torsion-free sheaf on X of rank 1 such that*

$$h^0(\mathcal{F}) = h^1(\mathcal{F}) = 0 \tag{1.1}$$

and $\eta : T_{X,P} \xrightarrow{\sim} L$.

The consideration of torsion-free sheaves as well as the present version of the Burchnall-Chaundy-Krichever result is due to Mumford [**Mum**].

2. Drinfeld modules of rank 1

Let L be a field over $\mathbb{F}_q$, X_0 a projective curve and $X = X_0 \otimes_{\mathbb{F}_q} L$. We fix a smooth closed point P on X. Denote $\tau : c \mapsto c^q$ the Frobenius morphism of L. We consider the ring $L[\tau]$ of twisted polynomials with the commutation rule $\tau c = c^q \tau$ for any $c \in L$. The simplest Drinfeld module[1] of rank 1 :

$$\varphi : T \mapsto T + \tau \tag{2.1}$$

[1]see theorem 2.1 below and (4.2) for the definition

for $X = \mathbb{P}^1_L = \text{Proj } L[T]$ called the *Carlitz module* was studied by L. Carlitz in thirties [**Carl**]. Drinfeld [**Dr1**] discovered more general objects which he called *elliptic modules* while trying to prove the Langlands conjecture (for global function fields).

THEOREM 2.1. (Drinfeld ; [**Dr2**], [**Mum**]) *The category of commutative subrings A of $R = L[\tau]$ of rank 1 containing $\mathbb{F}_q$ (called Drinfeld modules of rank 1) up to the conjugation by elements of L^* is anti-equivalent to the category of quadruples $(X, P, \mathcal{F}, \eta)$ where $\mathcal{F}$ is a torsion-free sheaf on X of rank 1 such that $\chi(\mathcal{F}) = 0$ and*

$$\eta : (\mathrm{Id}_{X_0} \times \tau)^* \mathcal{F} \xrightarrow{\sim} \mathcal{F}(P - Q) \tag{2.2}$$

for a smooth closed point $Q \neq P$.

As Drinfeld remarked ([**Dr2**], [**Mum**, §3], [**An3**, 3.3]) the condition $\chi(\mathcal{F}) = 0$ implies $h^0(\mathcal{F}) = h^1(\mathcal{F}) = 0$.

3. Commentaries

The rank of a commutative subring $A \subset R$ is defined as the g.c.d. of degrees of its elements. If X is smooth curve then any torsion-free sheaf $\mathcal{F}$ of rank 1 is a line bundle and by the Riemann-Roch formula we have :

$$0 = h^0(\mathcal{F}) - h^1(\mathcal{F}) = \chi(\mathcal{F}) = 1 - g + \deg(\mathcal{F}) \Longrightarrow \deg(\mathcal{F}) = g - 1. \tag{3.1}$$

Any element $\mathcal{L} \in \mathrm{Jac}(X) = \mathrm{Pic}^0(X)$ acts by the tensor product on $\mathrm{Pic}^{g-1}(X)$ and on the moduli space M^1 of Drinfeld (Krichever) modules of rank 1. In this way we obtain what is called a *Jacobian flow*. For example (in the differential case), if X is a hyperelliptic curve of genus 2 and P is a Weierstrass point then the Jacobian flow is given (up to a constant) by the Korteweg-de Vries equation :

$$\frac{\partial u}{\partial s} = \frac{\partial^3 u}{\partial t^3} + 6u \frac{\partial u}{\partial t} \tag{3.2}$$

We would like to say few words about the proofs of the theorems quoted above. It is remarkable that the proofs essentially coincide. On the one hand, if $A \subset R$ is a commutative subring as above then formally $X - P = \text{Spec } A$ and the degree map $D \mapsto \deg\ D$ defines a valuation corresponding to P. Moreover, for any $D \in A$ the "eigenspaces" of D glue into a torsion-free sheaf of rank 1.

On the other hand, a quadruple $(X, P, \mathcal{F}, \eta)$ defines an isospectral deformation of $\mathcal{F}$ (see [**Mum**, §2, 3] for more details). This deformation is trivial outside (of a small neighborhood) of P and defines an injection $A = \mathrm{H}^0(X - P, \mathcal{O}_X) \hookrightarrow R$.

4. Krichever modules of arbitrary rank and elliptic sheaves

There are several problems arising when one tries to give an analogous description in the case of commutative subrings of arbitrary rank. See [**Mum**, §2] and [**PW**] for discussions of these problems. However, in the case of twisted polynomials, Drinfeld introduced a notion of elliptic sheaf and generalized theorem 2.1 above. The definition of an elliptic sheaf will be given later in more general context.

THEOREM 4.1. (Drinfeld; [**Dr2**], [**Dr3**]) *The category of commutative subrings A of $R = L[\tau]$ of rank r containing $\mathbb{F}_q$ (called Drinfeld modules of rank r) up to the conjugation by elements of L^* is anti-equivalent to the category of triples $(X, P, \mathcal{F})$ where $\mathcal{F}$ is an elliptic sheaf.*

Any Drinfeld module is given, in fact, by an injection

$$\varphi : A = \Gamma(X_0 - P_0, \mathcal{O}_{X_0}) \hookrightarrow L[\tau] \tag{4.1}$$

In particular, if $X_0 = \mathbb{P}^1_{\mathbb{F}_q}$ then it is given by the image of T :

$$\varphi : T \mapsto \sum_{i=0}^{r} a_i \tau^i. \tag{4.2}$$

for some elements $a_i \in L$. See, for instance, the definition of the Carlitz module in section 2.

It is certainly possible to define also Krichever sheaves and to prove an analogous theorem in the differential case (cf. [**Lau2**]). There exists also an another approach due to Mulase.

THEOREM 4.2. (Mulase, [**Mu1**]) *There is a natural bijective correspondence between the set of commutative subrings A of $R = L[[t]][d/dt]$ of rank r containing L (called Krichever modules of rank r) considered up to the conjugation by invertible elements of $L[[t]]$ and the set of quintuples $(X, P, \mathcal{F}, \eta, \pi)$ where $\mathcal{F}$ is a semi-stable torsion-free sheaf on X of rank r and of degree $d = r(g-1)$ having no non-trivial holomorphic global sections, η is a local trivialization of $\mathcal{F}$ near P and π is a local r-sheet covering ramified at P.*

It is remarkable in the both cases that the commutativity of a subring A force it to be elliptic, that is, consisting of operators with invertible leading coefficients.

5. Drinfeld-Anderson motives

Let L be a perfect field over $\mathbb{F}_q$. We would like to go further and describe commutative subrings of the matrix ring $\mathrm{M}_n(L[\tau])$. For this purpose we introduce a notion of Drinfeld-Anderson motives generalizing elliptic sheaves [**Dr3**], Anderson t-motives [**An1**] and Laumon-Rapoport-Stuhler $\mathcal{D}$-elliptic sheaves [**LRS**] over L.

Let $X_0/\mathbb{F}_q$ be a projective curve and P_0 a smooth closed point on X_0. We denote

$$A = \Gamma(X_0 - P_0, \mathcal{O}_{X_0}) \tag{5.1}$$

the ring of functions on X_0 regular outside of P_0. We suppose that L is equipped with a non-zero morphism $\alpha_L : A \to L$.

DEFINITION 5.1. A *Drinfeld-Anderson A-motif M of rank r and τ-rank n* is a left $(A \otimes_{\mathbb{F}_q} L[\tau])$-module verifying the following conditions :

1. M is a free $L[\tau]$-module of rank n
2. M is a torsion-free $(A \otimes_{\mathbb{F}_q} L)$-module of rank r
3. $(a - \alpha_L(a))$ is nilpotent on $M/\tau M$ for any $a \in A$.

A *morphism* of Drinfeld-Anderson motives is an $(A \otimes_{\mathbb{F}_q} L[\tau])$-linear map.

REMARK 5.2. On the one hand, if $n = 1$, our definition of M is equivalent to the Drinfeld definition of an *elliptic sheaf of rank r over L* ([**Dr3**], [**Cara**, sect. 2]). On the other hand, if $X_0 = \mathbb{P}^1_{\mathbb{F}_q}$ and, consequently, $A = \mathbb{F}_q[t]$ then M is nothing else but an *Anderson t-motive* [**An1**]. Furthermore, if M is a $\mathcal{D}$-elliptic sheaf of rank r over L (cf. [**LRS**]) then the underlying $(A \otimes_{\mathbb{F}_q} L[\tau])$-module is a Drinfeld-Anderson motive of rank r^2 and τ-rank r.

We denote $\mathrm{M}_n(L[\tau])$ the ring of square matrices of order n over $L[\tau]$ with the commutation rule $\tau B = B^{(q)}\tau$ where $B^{(q)}$ is the "naïve" qth power of $B \in \mathrm{M}_n(L)$ (with respect to each component). Since $L[\tau]$ is both left and right euclidian any matrix $D \in \mathrm{M}_n(L[\tau])$ is equivalent to a diagonal matrix. We say that D is non-degenerate if it is equivalent to a diagonal matrix without zeros on the principal diagonal. Any D defines an endomorphism u_D of the additive group scheme $\mathbb{G}^n_{\mathrm{a},L}$. If, in addition, D is non-degenerate then the kernel H_D of this endomorphism is a finite group scheme over $\mathbb{F}_q$. We define the *degree of* D by

$$\deg(D) = \log_q\left(\sharp\left(\mathrm{Ker}(D|\overline{L})\right)\right) + \mathrm{ht}(H_D) \tag{5.2}$$

where $\mathrm{ht}(H_D)$ is the height of H_D (cf. [**Lau1**, (2.1)] in the case $n = 1$). For any element $D \in \mathrm{M}_n(L[\tau])$ we have a decomposition :

$$D = \sum_{i=0}^{k} D_i \tau^i. \tag{5.3}$$

where D_i belong to $\mathrm{M}_n(L)$. We would like to consider non-degenerate commutative subrings $A \subset \mathrm{M}_n(L[\tau])$ verifying for any $D \in A$ the following condition :

$$D_0 = D_\alpha + \text{nilpotent matrix} \tag{$\star$}$$

where D_α is proportional to the identity matrix Id_n. If D_α is not equal to zero then $\mathrm{ht}(H_D)$=0 in the formula (5.2). We also assume that A satisfies the following condition of finite generation[2] :

$$\mathrm{Hom}(\mathbb{G}^n_{\mathrm{a},L}, \mathbb{G}_{\mathrm{a},L}) = \sum_{a \in A} V \circ a \tag{$\star\star$}$$

for a certain finite-dimensional L-subspace $V \subset \mathrm{Hom}(\mathbb{G}^n_{\mathrm{a},L}, \mathbb{G}_{\mathrm{a},L})$ (cf. [**An1**], (1.1.3)). Finally, we suppose that A contains $\mathbb{F}_q$ via the diagonal injection $a \mapsto \mathrm{Diag}(a, \ldots, a)$ for any $a \in \mathbb{F}_q$.

THEOREM 5.3. *The category of commutative subrings of* $\mathrm{M}_n(L[\tau])$ *containing* $\mathbb{F}_q$ *and verifying the conditions* ($\star$) *and* ($\star\star$) *up to the conjugation by elements of* $\mathrm{GL}(n, L)$ *is anti-equivalent to the category of Drinfeld-Anderson motives of* τ-*rank* n.

PROOF. First of all, we would like to prove that any commutative non-degenerate subring $A \subset \mathrm{M}_n(L[\tau])$ verifying the conditions above corresponds to a certain pair (X_0, P_0) by formula (5.1). Consider the graded ring

$$\mathcal{A} = \bigoplus_{\ell \geq 0} A_\ell \tag{5.4}$$

where

$$A_\ell = \{D \in A \mid \deg(D) \leq \ell\} \tag{5.5}$$

and put $X_0 = \mathrm{Proj}\ \mathcal{A}$. Let K be the quotient field of A. Then the function $D \mapsto \deg(D)$ defines a valuation of K, that is, a point P_0 on X_0. It is clear now that our commutative subring is given by an injection

$$\varphi : \Gamma(X_0 - P_0, \mathcal{O}_{X_0}) \hookrightarrow \mathrm{M}_n(L[\tau]) \tag{5.6}$$

and the map α_L is defined by $a \mapsto D_\alpha$ where $D = \varphi(a)$.

[2]the author is very grateful to a referee for pointing out that in the higher-dimensional case such a condition can not be avoided even if we suppose that the rank of A (as g.c.d. of degrees of its elements) is finite

Further, the group $M = \mathrm{Hom}(\mathbb{G}^n_{\mathrm{a},L}, \mathbb{G}_{\mathrm{a},L})$ has a natural structure, denoted $M(\varphi)$, of a left $(A \otimes_{\mathbb{F}_q} L[\tau])$-module given by the following rules :

$$(xm)(e) = x(m(e)) \tag{5.7}$$
$$(\tau m)(e) = m(e)^q \tag{5.8}$$
$$(am)(e) = m(D(e)) \text{ where } D = \varphi(a) \tag{5.9}$$

for any $a \in A$, $x \in L$, $e \in \mathbb{G}^n_{\mathrm{a},L}$ and $m \in M$. The condition $(\star\star)$ above implies that M is finitely generated as $(A \otimes_{\mathbb{F}_q} L)$-module.

A left $(A \otimes_{\mathbb{F}_q} L[\tau])$-module, finitely generated as an $(A \otimes_{\mathbb{F}_q} L)$-module and as a left $L[\tau]$-module, is torsion-free over $A \otimes_{\mathbb{F}_q} L$ if and only if it is torsion-free over $L[\tau]$ (cf. [**An1**], Lemma 1.4.5). As a consequence we obtain that $M(\varphi)$ satisfies properties (i) and (ii) in the definition of Drinfeld-Anderson motives. Indeed, $M(\varphi)$ is a free $L[\tau]$-module of finite type by construction and all the more torsion-free. Thus, by the lemma just mentioned, $M(\varphi)$ is also torsion-free over $A \otimes_{\mathbb{F}_q} L$. Moreover, the property $(\star)$ of a ring A implies the condition (iii) in definition 5.1.

Reciprocally, if M is a Drinfeld-Anderson motive of τ-rank n then its structure of $(A \otimes_{\mathbb{F}_q} L)$-module defines a morphism :

$$\varphi(M) : A \to \mathrm{End}_{L[\tau]} M \cong \mathrm{End}(\mathbb{G}^n_{\mathrm{a},L}). \tag{5.10}$$

The image of this morphism is a commutative subring of $\mathrm{M}_n(L[\tau])$ satisfying obviously all required properties.

Finally, it is easy to see that the functors

$$A \mapsto \varphi \mapsto M(\varphi) \quad \text{and} \quad M \mapsto \mathrm{Im}(\varphi(M)) \tag{5.11}$$

define the anti-equivalences of the considered categories (cf. [**An1**], th. 1) □

As corollaries we obtain theorems 2.1 and 4.1 in the case where L is a perfect field. The key point in the proof is to show that our notion of Drinfeld-Anderson motive in those particular cases coincides with the notion of elliptic sheaf over L. In general, elliptic sheaves and $\mathcal{D}$-elliptic sheaves may be defined over any $\mathbb{F}_q$-scheme S. We shall return to this question in the next section while defining a notion of *pure Drinfeld-Anderson sheaf.*

A morphism φ in the theorem above is called a *Drinfeld-Anderson module of rank r and τ-rank n* by analogy with Drinfeld modules and Anderson abelian t-modules ([**An1**], §1).

EXAMPLE 5.4. If φ is a Drinfeld module then $M(\varphi)$ is called a *Drinfeld motive.* It can be described by generators and relations in the following way :

$$M(\varphi) = (A \otimes_{\mathbb{F}_q} L[\tau])/\big(c_1 - \varphi(c_1), \dots, (c_k - \varphi(c_k)\big) \tag{5.12}$$

where $\{c_1, \dots, c_k\}$ is a system of generators of A over $\mathbb{F}_q$.

6. Pure Drinfeld-Anderson motives and sheaves

There is a new phenomenon of existence of "non-pure" commutative subrings[3] of $\mathrm{M}_n(L[\tau])$ when $n > 1$. In this section we define what is a pure Drinfeld-Anderson motive following Anderson's ideas. It turns out that the definition may be extended

[3]this is, in particular, related to the existence of non-multisoliton solutions of the multicomponent KP hierarchy (see [**KvdL**, (0.4)])

to a more general situation where a perfect field L is replaced by an arbitrary $\mathbb{F}_q$-scheme S. In particular, elliptic sheaves of rank r and $\mathcal{D}$-elliptic sheaves of rank r^2 are pure of weight $1/r$.

6.1. Pure DA motives. We use henceforward the traditional notation ∞ for a fixed closed point P_0 on X_0 and ν_∞ for the corresponding additive valuation of the function field K of X_0. This notation is a little misleading since any closed point on X_0 corresponds to a finite place of K.

Let K_∞ be the completion of K at ∞, $\mathcal{O}_\infty$ the valuation ring of K_∞, ϖ_∞ an uniformizer and κ_∞ the residue field. Consider a Drinfeld-Anderson A-motif M and denote $K_\infty(L) = K_\infty \widehat{\otimes}_{\mathbb{F}_q} L$. If the degree d_∞ of ∞ is equal to 1 we have $K_\infty(L) = L((\varpi_\infty))$. Moreover, we shall use the following notations :

$$V(M) = M \bigotimes_{A\otimes_{\mathbb{F}_q} L} (K \otimes_{\mathbb{F}_q} L) \text{ et } V(M)_\infty = M \widehat{\bigotimes_{A\otimes_{\mathbb{F}_q} L}} K_\infty(L). \tag{6.1.1}$$

We put $\sigma = \tau^{d_\infty}$ and we shall equip $V(M)_\infty$ with an unique structure of left $(A \otimes_{\mathbb{F}_q} L[\sigma])$-module extending its structure of $(A \otimes_{\mathbb{F}_q} L)$-module by the formula

$$\sigma\Big(m\otimes\Big(\sum c_i \varpi_\infty^i\Big)\Big) = (\sigma m)\otimes\Big(\sum c_i^{q^{d_\infty}} \varpi_\infty^i\Big)\Big) \tag{6.1.2}$$

for any $m \in M$.

Definition 6.1.1. A Drinfeld-Anderson A-motif M of over L is called *pure of weight* $w = u/v$ if there exists an $(\mathcal{O}_\infty \widehat{\otimes}_{\mathbb{F}_q} L)$-lattice $M_\infty \subset V(M)_\infty$ such that

$$\varpi_\infty^{-u} M_\infty = \sigma^v M_\infty \tag{6.1.3}$$

for certain relatively prime natural integers u et v.

If M is a pure Drinfeld-Anderson motive then

$$w = u/v = n/r \tag{6.1.4}$$

(cf. [**An1**], (1.9.1)).

Proposition 6.1.2. *The category of pure Drinfeld-Anderson A-motives over L is equivalent to the category of* $(A \otimes_{\mathbb{F}_q} L[\tau])$*-modules equipped with an exhaustive filtration :*

$$M_0 \subset M_1 \subset \cdots \subset M_i \subset \cdots \subset M \tag{6.1.5}$$

verifying the following condition :

$$M_i + \varpi_\infty^{-u} M_i = M_{i+1} = M_i + \sigma^v M_i. \tag{6.1.6}$$

Proof. See ([**An1**], prop. 1.9.2)

6.2. Pure DA sheaves. In this subsection we intend to show that the conception of Drinfeld-Anderson motive is, in fact, geometric. All schemes considered here are $\mathbb{F}_q$-schemes. We suppose in addition that $n < r$ and that u, v are relatively prime integers.

DEFINITION 6.2.1. A *pure Drinfeld-Anderson sheaf of pole* ∞, *of rang* r, *of* τ-*rang* n *and of weight* $w = n/r = u/v$ over a scheme S, consists of the following commutative diagram :

$$\begin{tikzcd}
\cdots \arrow[r, hook, "j"] & \mathcal{E}_{i-1} \arrow[r, hook, "j"] & \mathcal{E}_i \arrow[r, hook, "j"] & \mathcal{E}_{i+1} \arrow[r, hook, "j"] & \cdots \\
\cdots \arrow[r, hook, "{}^\tau j"] \arrow[ur, "\varphi"] & {}^\tau\mathcal{E}_{i-1} \arrow[r, hook, "{}^\tau j"] \arrow[ur, "\varphi"] & {}^\tau\mathcal{E}_i \arrow[r, hook, "{}^\tau j"] \arrow[ur, "\varphi"] & {}^\tau\mathcal{E}_{i+1} \arrow[r, hook, "{}^\tau j"] \arrow[ur, "\varphi"] & \cdots
\end{tikzcd} \tag{6.2.1}$$

where for any $i \in \mathbb{Z}$, $\mathcal{E}_i$ is a locally free $\mathcal{O}_{X\times S}$-module of rang r and

$$ {}^\tau\mathcal{E}_i = (\mathrm{id}_X \times \mathrm{Frob}_{S/\mathbb{F}_q})^*\mathcal{E}_i \tag{6.2.2}$$

is the pull-back of $\mathcal{E}_i$ with respect to the Frobenius morphism of S, and where j and φ are $\mathcal{O}_{X\times S}$-linear injections. In addition, these data should satisfy the following conditions :

[Pole]: $\mathcal{E}_i/j(\mathcal{E}_{i-1})$ is the direct image $(\Gamma_\infty)_*\mathcal{A}_i$ of a locally free $\mathcal{O}_S$-module of rang n by the section ∞ :

$$\Gamma_\infty : S \to X \times S, \ s \mapsto (\infty, s). \tag{6.2.3}$$

[Zero]: $\mathcal{E}_i/\varphi({}^\tau\mathcal{E}_{i-1})$ is the direct image $(\Gamma_\alpha)_*\mathcal{B}_i$ of a locally free $\mathcal{O}_S$-module of rang n by a section $\Gamma_\alpha : S \to X \times S$ given by the graph of a morphism $\alpha : S \to X - \{\infty\}$.

[Purity]: $\mathcal{E}_{i+v\cdot d_\infty} = \mathcal{E}_i(\{u\infty\}\times S)$ where the composition of v consecutive morphisms is a natural injection.

[Normalization]: the Euler characteristic $\chi(\mathcal{E}_0|_{X\times s}) \in [0, n[$ for any geometric point s of S.

By the condition [Pole], an injection j identifies $\mathcal{E}_{i+1}$ and $\mathcal{E}_i$ over

$$(X \times S) - \Gamma_\infty \cong \mathrm{Spec}\ A \times S \tag{6.2.4}$$

and φ defines a semi-linear morphism. It implies that the union $\mathcal{E} = \cup\mathcal{E}_i$ is a locally free $\mathcal{O}_{\mathrm{Spec}(A)\times S}$-module equipped with a semi-linear Frobenius morphism $\varphi : \mathcal{E} \to \mathcal{E}$. Such an object is called a φ-*sheaf* (cf. [**TW**], sect. 1). In the case where $S = L$ is a field, this φ-sheaf is clearly an $(A \otimes_{\mathbb{F}_q} L[\tau])$-module. Moreover, diagram (6.2.1) defines filtration (6.1.5), and the purity condition implies (6.1.6). If $S = L$ then φ-sheaves are called φ-modules and was studied by Drinfeld [**Dr4**] (see also the proof of theorem 7.1 (iii)).

7. Classification over finite fields

In this section we give a partial motivation for the word "motive" applied to the objects defined above. Indeed, the category of Drinfeld-Anderson motives over a finite field $\mathbb{F}$ (or its algebraic closure $\overline{\mathbb{F}}$) is similar to the category of "usual" motives over $\mathbb{F}$ (cf. [**Mi**]). There is a fundamental difference nonetheless between these two categories since our motives are with "values in positive characteristic". It means that their L-functions are with values in the functional Tate field $\mathcal{C}_\infty = \widehat{\overline{K}}_\infty$

corresponding to a point ∞ on a curve X_0 with the function field K (see [**Go1**] or [**TW**] for detailed analysis of these L-functions).

Let $\mathbb{F}$ be a finite field over $\mathbb{F}_q$ equipped with a morphism $\alpha_L : A \to L$. Denote $\mathfrak{p}_{\mathbb{F}}$ the place of K (and the prime ideal of A) corresponding to the kernel of α_L. This place will be called *"divisorial" characteristic* of L. Furthermore, consider a Drinfeld-Anderson A-motive M of τ-rank n and a corresponding commutative subring given by an injection

$$\varphi(M) : A \hookrightarrow \mathrm{M}_n(\mathbb{F}[\tau]). \tag{7.1}$$

Such a motive has the natural Frobenius endomorphism $F = \tau^{[\mathbb{F}:\mathbb{F}_q]}$. Since the image of $\varphi(M)$ consists of non-degenerate matrices it extends to an injection $K \hookrightarrow \mathrm{M}_n(\mathbb{F}(\tau))$ where $K = \mathrm{Quot}(A)$ and $\mathbb{F}(\tau)$ is the quotient skew field of $\mathbb{F}[\tau]$ (well-defined because $\mathbb{F}$ is perfect).

Two Drinfeld-Anderson motives M_1 and M_2 of τ-rank n are *isogenous* if there exists a surjective endomorphism u of $\mathbb{G}^n_{\mathrm{a},L}$ with a finite kernel such that

$$[u\varphi(M_1)](a) = [\varphi(M_2)u](a) \tag{7.2}$$

for any $a \in A$. As we are going to prove now, the category $\mathcal{D}A(\mathbb{F})$ of Drinfeld-Anderson motives over $\mathbb{F}$ (considered up to isogenies) is semi-simple. It makes sense therefore to speak about *simple* Drinfeld-Anderson motives.

THEOREM 7.1. (i) *The category of Drinfeld-Anderson motives (up to isogeny) over $\mathbb{F}$ is abelian, tensor and semi-simple.*
(ii) *("Riemann hypothesis") If M is a pure Drinfeld-Anderson A-motive of weight w over $\mathbb{F}$ then*

$$\deg(\omega) = [\mathbb{F} : \mathbb{F}_q] \cdot w \tag{7.3}$$

for any root ω of the characteristic polynomial $P_M(x)$ of M.
(iii) *If M is a pure simple Drinfeld-Anderson A-motive of rang r, of weight w and of "divisorial" characteristic $\mathfrak{p}_{\mathbb{F}}$ over $\mathbb{F}$ then :*

(a) *$K(F)$ is a field such that $[K(F) : K]$ divide r ;*

(b) *there exist an unique place $\widetilde{\infty}|\infty$ and an unique place $\mathfrak{P}_{\mathbb{F}}|\mathfrak{p}_{\mathbb{F}}$ of $K(F)$;*

(c) *$\mathrm{End}(M) \otimes_A K$ is a central simple algebra of dimension $(r/[K(F) : K])^2$ over $K(F)$ with invariants :*

$$\mathrm{inv}_{\mathfrak{P}} = \begin{cases} w \cdot [K(F) : K] & \text{if } \mathfrak{P} = \mathfrak{P}_{\mathbb{F}} \\ -w \cdot [K(F) : K] & \text{if } \mathfrak{P} = \widetilde{\infty} \\ 0 & \text{otherwise} \end{cases}. \tag{7.4}$$

PROOF. (i) A Drinfeld-Anderson motive has a natural structure of a φ-module as was remarked in the end of the previous section (see also the proof of (7.4) below). Drinfeld proved that the category of φ-motives over $\mathbb{F}$ is abelian and semi-simple [**Dr4**, prop. 2.1.1]. It implies that the analogous assertions for the category $\mathcal{D}A(\mathbb{F})$ also hold. Moreover, for any two Drinfeld-Anderson motives M and M', we define the tensor product $M \otimes M'$ as a left $(A \otimes_{\mathbb{F}_q} L[\tau])$-module coinciding with $M \otimes M'$ as an $(A \otimes_{\mathbb{F}_q} L)$-module and such that :

$$\tau(m \otimes m') \stackrel{\text{def}}{=} (\tau m) \otimes (\tau m') \tag{7.5}$$

for any $m \in M$ and $m' \in M'$ (cf. [**An1**, 1.11]).

(ii) Since any Drinfeld-Anderson motive M over $\mathbb{F}$ is semi-simple there is a decomposition (by the Wedderburn theorem) :

$$\operatorname{End}(M) \otimes_A K = \mathrm{M}_{n_1}(D_1) \oplus \cdots \oplus \mathrm{M}_{n_l}(D_l), \tag{7.6}$$

where D_k, $1 \leq k \leq l$, are division algebras with centers C_k. The characteristic polynomial may be defined by the following formula :

$$P_M(x) = \prod \mathrm{N}_K^{C_k} \circ \mathrm{nr}_k(x - F) \tag{7.7}$$

where $\mathrm{nr}_k : \mathrm{M}_{n_k}(D_k) \to C_k$ denotes the reduced norm. It is easy to see that

$$P_M(0) = \mathfrak{p}_{\mathbb{F}}^{n \cdot [\mathbb{F}:\mathbb{F}_\mathfrak{p}]} \tag{7.8}$$

where $\mathbb{F}_\mathfrak{p} = A/\mathfrak{p}_{\mathbb{F}}$ (cf. [**Ge**, th. 5.1 (ii)] when $n = 1$). Since M is pure the ∞-adic valuations of all its roots are the same ([**Go1**], Lemma 2.2.9). Consequently, we have :

$$\nu_\infty(w) = \nu_\infty(P_M(0))/r = \nu_\infty\left(\mathfrak{p}_{\mathbb{F}}^{n \cdot [\mathbb{F}:\mathbb{F}_\mathfrak{p}]}\right)\Big/ r = -\frac{n \cdot [\mathbb{F} : \mathbb{F}_q]}{r \cdot d_\infty} = -\frac{[\mathbb{F} : \mathbb{F}_q] \cdot w}{d_\infty}.$$

(iii) First of all, $K(F)$ is a field since F commutes with elements of A. The algebra $\mathrm{M}_n(\mathbb{F}(\tau))$ is central simple over $\mathbb{F}_q(F)$ and splits neither at ∞ nor at $\mathfrak{p}_{\mathbb{F}}$. By the centralizer theorem,

$$\operatorname{End}(M) \otimes_A K = \operatorname{Cent}_{\mathrm{M}_n(\mathbb{F}(\tau))}(K) = \operatorname{Cent}_{\mathrm{M}_n(\mathbb{F}(\tau))}(K(F)) \tag{7.9}$$

is a simple algebra over $K(F)$. Since $K(F)$ contains the center $\mathbb{F}_q(F)$ of $\mathrm{M}_n(\mathbb{F}(\tau))$ we have that $K(F)$ is exactly the center of $\operatorname{End}(M) \otimes_A K$ and

$$[K(F) : \mathbb{F}_q(F)] = [\mathrm{M}_n(\mathbb{F}(\tau)) : (\operatorname{End}(M) \otimes_A K)] \tag{7.10}$$

divides

$$\Big([\mathrm{M}_n(\mathbb{F}(\tau)) : \mathbb{F}_q(F)]\Big)^{1/2} = n \cdot [\mathbb{F} : \mathbb{F}_q]. \tag{7.11}$$

and the quotient is $[(\operatorname{End}(M) \otimes_A K) : K(F)]$ (cf. [**Lau1**], proof of prop. 2.2.2). On the other hand, since

$$|F|_\infty = q^{[\mathbb{F}:\mathbb{F}_q] \cdot w} = q^{[\mathbb{F}:\mathbb{F}_q] \cdot n/r} \tag{7.12}$$

we have

$$[K(F) : \mathbb{F}_q(F)] = -\nu_{\widetilde{\infty}}(F) \deg(\widetilde{\infty}) = \frac{n \cdot [\mathbb{F} : \mathbb{F}_q]}{r} \cdot [K(F) : K]. \tag{7.13}$$

(cf. [**Ge**], (2.7)). It implies that

$$[(\operatorname{End}(M) \otimes_A K) : K(F)] = (n \cdot [\mathbb{F} : \mathbb{F}_q]/[K(F) : \mathbb{F}_q(F)])^2 = (r/[K(F) : K])^2.$$

(cf. [**Ge**], sect. 2, [**Lau1**], prop. 2.2.2). As a result we proved (a), (b) and a part of (c).

Finally, we shall prove the formula (7.4) using general Drinfeld results on φ-modules, φ-pairs and Dieudonné modules ([**Dr4**, sect. 2], [**LRS**, App. A,B]). A *φ-module* (V, φ) over $\mathbb{F}$ is, by definition, a $(K \otimes_{\mathbb{F}_q} \mathbb{F})$-vector space V equipped with a $(K \otimes_{\mathbb{F}_q} \tau)$-semi-linear map $\varphi : V \to V$. If M is a Drinfeld-Anderson motive over $\mathbb{F}$ then the pair

$$(V(M), \varphi) \overset{\mathrm{def}}{=} \left(M \bigotimes_{A \otimes_{\mathbb{F}_q} \mathbb{F}} (K \otimes_{\mathbb{F}_q} \mathbb{F}), \tau\right) \tag{7.14}$$

is called the *φ-module associated to M*. Drinfeld proved that there is a bijection $(V, \varphi) \mapsto (K_{(V,\varphi)}, \Pi_{(V,\varphi)})$ between isomorphism classes of φ-modules and φ-pairs (see loc. cit. for the definition of φ-pairs an for the proof of this statement). In the considered case we simply have :

$$(K_{(V(M),\varphi)}, \Pi_{(V(M),\varphi)}) = (K(F), F). \tag{7.15}$$

In addition, the invariants of $(K_{(V,\varphi)}, \Pi_{(V,\varphi)})$ are given by the following formula :

$$\mathrm{inv}_{\mathfrak{P}}(\mathrm{End}(V,\varphi)) = -\deg(\mathfrak{P})\nu_{\mathfrak{P}}(\Pi_{(V,\varphi)}). \tag{7.16}$$

Let $\mathfrak{p}$ be a place of K. A *Dieudonné $K_{\mathfrak{p}}$-module* $(V_{\mathfrak{p}}, \varphi_{\mathfrak{p}})$ is a $(K_{\mathfrak{p}}\widehat{\otimes}_{\mathbb{F}_q}\mathbb{F})$-module $V_{\mathfrak{p}}$ together with a $(K_{\mathfrak{p}}\widehat{\otimes}_{\mathbb{F}_q}\tau)$-semi-linear map $\varphi : V_{\mathfrak{p}} \to V_{\mathfrak{p}}$. We fix an embedding $\kappa(\mathfrak{p}) = A/\mathfrak{p} \hookrightarrow \overline{\mathbb{F}}$ and for integers u, v $(v \geq 1)$ we denote $(V_{\mathfrak{p},v,u}, \varphi_{\mathfrak{p},v,u})$ an irreducible Dieudonné module such that

$$V_{\mathfrak{p},v,u} = \left(K_{\mathfrak{p}}\widehat{\otimes}_{\kappa(\mathfrak{p})}\overline{\mathbb{F}}\right)^{v} \tag{7.17}$$

and

$$\varphi_{\mathfrak{p},v,u}(e_i) = \begin{cases} \varpi_{\mathfrak{p}}^{u} e_v & \text{for } i = 1 \\ e_{i-1} & \text{otherwise} \end{cases} \tag{7.18}$$

where $(e_1, \ldots, e_v)$ is the standard basis of $V_{\mathfrak{p},v,u}$.

Let (V, φ) be an irreducible φ-module, $(\widetilde{K}, \widetilde{\Pi}) = (K_{(V,\varphi)}, \Pi_{(V,\varphi)})$ the corresponding φ-pair and

$$(V_{\mathfrak{p}}, \varphi_{\mathfrak{p}}) = K_{\mathfrak{p}}\widehat{\otimes}_{K}(V,\varphi), \quad (V_{\mathfrak{P}}, \varphi_{\mathfrak{P}}) = \widetilde{K}_{\mathfrak{P}}\widehat{\otimes}_{\widetilde{K}}(V,\varphi) \tag{7.19}$$

the induced Dieudonné modules. Then, always due to Drinfeld results (loc. cit.), there is a decomposition

$$(V_{\mathfrak{p}}, \varphi_{\mathfrak{p}}) = \bigoplus_{\mathfrak{P}|\mathfrak{p}} (V_{\mathfrak{P}}, \varphi_{\mathfrak{P}}) = \bigoplus_{\mathfrak{P}|\mathfrak{p}} \left(N_{\mathfrak{P},v_{\mathfrak{P}},u_{\mathfrak{P}}}, \varphi_{\mathfrak{P},v_{\mathfrak{P}},u_{\mathfrak{P}}}\right)^{s_{\mathfrak{P}}} \tag{7.20}$$

where integers $u_{\mathfrak{P}}, v_{\mathfrak{P}}, s_{\mathfrak{P}}$ are uniquely defined by the following relations :

$$\begin{cases} u_{\mathfrak{P}}, s_{\mathfrak{P}} \geq 1 \\ \gcd(u_{\mathfrak{P}}, v_{\mathfrak{P}}) = 1 \\ u_{\mathfrak{P}}/v_{\mathfrak{P}} = \deg(\mathfrak{P})\nu_{\mathfrak{P}}(\widetilde{\Pi})/\left[\widetilde{K}_{\mathfrak{P}} : K_{\mathfrak{P}}\right] \\ v_{\mathfrak{P}} s_{\mathfrak{P}} = d(\widetilde{\Pi})/\left[\widetilde{K}_{\mathfrak{P}} : K_{\mathfrak{P}}\right] \end{cases} \tag{7.21}$$

Here $d(\widetilde{\Pi})$ denotes the g.c.d. of denominators of rational numbers $\deg(\mathfrak{P})\nu_{\mathfrak{P}}(\widetilde{\Pi})$ for all places $\mathfrak{P}$ of $\widetilde{K}$. In view of equations (7.16) and (7.21) we obtain

$$\mathrm{inv}_{\mathfrak{P}}(\mathrm{End}(M) \otimes_A K) = \mathrm{inv}_{\mathfrak{P}}(\mathrm{End}(V(M), \varphi)) = -(u_{\mathfrak{P}}/v_{\mathfrak{P}})\cdot\left[\widetilde{K}_{\mathfrak{P}} : K_{\mathfrak{P}}\right].$$

which implies (7.4) since, in particular, $\widetilde{\Pi} = F$, $\widetilde{K} = K(F)$ and $u_{\tilde{\infty}}/v_{\tilde{\infty}} = w$ $\square$

8. Multicomponent KP hierarchy

One can interpret Jacobian flows defined in section 3 as flows on (quotients of) the Sato's infinite-dimensional Grassmanian. Moreover, there exists a dynamical system on this Grassmanian (called *KP hierarchy*) such that any Jacobian flow as above is induced by a restriction of this system on a finite-dimensional subspace. From this point of view, Krichever (Drinfeld) modules are solutions of KP hierarchy whose orbits are finite-dimensional. In the differential case, the KP hierarchy is a collection of commuting vector fields given by an infinite set of partial differential equations of Korteweg-de Vries and Kadomtsev-Petviashvili type. In this section we define a *multicomponent KP hierarchy* whose solutions with finite-dimensional orbits are analogous to Drinfeld-Anderson motives.

We say that a map (of vector spaces) is Fredholm if it has both finite kernel and cokernel. For any natural integer k the Sato's infinite-dimensional Grassmanian Gr_k is defined as :

$$\begin{aligned}\mathrm{Gr}_k =\{ &\text{ subspaces } W \subset L((t))^{\oplus k} \mid \text{projection} \\ &\gamma_W : W \to (L((t))/L[[t]]t)^{\oplus k} \text{ is Fredholm}\}\end{aligned} \tag{8.1}$$

In other words, Gr_k is the set of subspaces $W \subset L((t))^{\oplus k}$ comparable to $L[t^{-1}]^{\oplus k}$ (cf. [**Sa**], [**Mu1**, sect. 1], [**AB**, 6.1], [**An3**, 2.1]). The index of a Fredholm map γ is defined by :

$$\operatorname{ind} \gamma = \dim_L \operatorname{Ker} \gamma - \dim_L \operatorname{Coker} \gamma. \tag{8.2}$$

Denote $\mathrm{Gr}_k(0)$ the (sub)Grassmanian of subspaces of index zero. Then

$$\mathrm{Gr}_k^+(0) \stackrel{\text{def}}{=} \{W \in \mathrm{Gr}_k(0) \mid \dim_L \operatorname{Ker} \gamma_W = \dim_L \operatorname{Coker} \gamma_W = 0\} \tag{8.3}$$

is called the *big cell* of $\mathrm{Gr}_k(0)$.

Consider a quintuple $(X, \{P_i\}, \mathcal{F}, t_i, \eta = \{\eta_i\})$ where $\{P_i\}$, $1 \leq i \leq k$, are distinct smooth closed points on X, t_i are local coordinates at P_i and η_i are formal trivializations of a torsion-free sheaf $\mathcal{F}$ at P_i. Then a *multicomponent Krichever map* from the moduli space of quintuples as above to the Sato Grassmanian Gr_k is defined by the formula :

$$(X, \{P_i\}, \mathcal{F}, t_i, \eta = \{\eta_i\}) \mapsto \bigcup_{\{l_i\}} \eta(H^0(X, \mathcal{F}(\oplus l_i P_i)) \subset L((t))^{\oplus k}. \tag{8.4}$$

Finally, the *k-component KP hierarchy* consists of commuting vector fields arising from the natural action of $(L[t^{-1}]t^{-1})^{\oplus k}$ on the quotient $\mathrm{Gr}_k/(L[[t]]^*)^k$ (see [**DM**, 6.1] for more details).

The precise description of the "usual" Krichever map is given by the following functorial version of theorem 4.2.

THEOREM 8.1. ([**Mu1**, th. 3.5]) *The Krichever map defines the anti-equivalence of the category of quintuples as in theorem* 4.2 *and the category of Schur pairs* (A, W) *where* W *is a point of the big cell* $\mathrm{Gr}^+(0)$ *of the Sato Grassmanian and* A *is a subring of* $L((t))$ *stabilizing* W.

A similar description in the multicomponent case certainly exists (cf. [**LM1**]) and is closely related to our main theorem 5.3.

9. Generalizations

Finally, we would like to mention some generalizations in the differential case :

- super Krichever modules and super KP hierarchy ([**MR**], [**Mu2**])
- Drinfeld-Sokolov hierarchies associated to Kac-Moody algebras ([**DS1**] and [**DS2**])
- Beilinson-Drinfeld G-opers where G is a semi-simple Lie algebra over L [**BD**]

To the best of the author's knowledge, the construction of analogous objects in positive characteristic is still an open problem[4].

References

[AB] M.R. Adams, M.J. Bergvelt, *The Krichever map, vector bundles over algebraic curves, and Heisenberg algebras*, Commun. Math. Phys. 154 (1993), 265-305

[An1] G.W. Anderson, *t-Motives*, Duke Math. J. 53, No. 2 (1986), 457-503

[An2] G.W. Anderson, *A two-dimensional analogue of Stickelberger's theorem*, The Arithmetic of Function Fields, D. Goss, D.R. Hayes and M.I. Rosen (eds.), W. de Gruyter, Berlin, 1992, 51-77

[An3] G.W. Anderson, *Rank one elliptic modules and A-harmonic series*, Duke Math. J. 73 (1994), No. 3, 491-541

[An4] G.W. Anderson, *Torsion points on Jacobians of quotients of Fermat curves and p-adic soliton theory*, Invent. Math. 118 (1994), 475-492

[BD] A.A. Beilinson, V.G. Drinfeld, *Quantization of Hitchin's fibration and Langlands program*, Algebraic and Geometric Methods in Mathematical Physics, A. Boutet de Monvel and V. Marchenko (eds.), Kluwer, 1996, 3-7

[BS] A. Blum, U. Stuhler, *Drinfeld modules and elliptic sheaves*, Vector Bundles on Curves – New Directions (editor : M.S. Narasimhan), Lect. Notes in Math. 1649, 1997

[BCh] J.L. Burchnall, T.W. Chaundy, *a) Commutative ordinary differential operators*, Proc. London Math. Soc. 21 (1923), 420-440 ; *b) Commutative ordinary differential operators*, Proc. Royal Soc. London (A) 118 (1928), 557-583 ; *Commutative ordinary differential operators II. The identity* $P^n = Q^m$, Proc. Royal Soc. London (A) 134 (1932), 471-485

[Cara] H. Carayol, *Variétés de Drinfeld compactes d'après Laumon, Rapoport et Stuhler*, Séminaire Bourbaki, 44$^{\text{ème}}$ année, 756 (1991-92), Astérisque 206 (1992), 369-409

[Carl] L. Carlitz, *On certain functions connected with polynomials in a Galois field*, Duke Math. J. 1 (1935), 137-168

[DM] R. Donagi, E. Markman, *Spectral covers, algebraically completely integrable Hamiltonian systems, and moduli of bundles*, Lect. Notes in Math. 1620 (1996), 1-119

[Dr1] V.G. Drinfeld, *Elliptic modules* (in Russian), Mat. Sbornik 94 (1974), 594-627 ; English transl. : Math. USSR-Sb., 23 (1974), 561-592

[Dr2] V.G. Drinfeld, *Commutative subrings of certain noncommutative rings*, Funct. Anal. Appl. 11 (1977), 9-12

[Dr3] V.G. Drinfeld, *Varieties of modules of F-sheaves*, Funct. Anal. Appl. 21 (1987), 107-122

[Dr4] V. G. Drinfeld, *The proof of Petersson's conjecture for* GL(2) *over a global field of characteristic p*, Funct. Anal. Appl. 22 (1988), 28-43

[DS1] V.G. Drinfeld, V.V. Sokolov, *Equations of Korteweg-de Vries type and simple Lie algebras*, Soviet Math. Dokl. 23 (1981), No. 3, 457-462

[DS2] V.G. Drinfeld, V.V. Sokolov, *Lie algebras and equations of Korteweg-de Vries type*, J. Soviet Math. 30 (1985), 1975-2035

[4]see however [**FGKV**, 7.2]

[FGKV] E. Frenkel, D. Gaitsgory, D. Kazhdan and K. Vilonen *Geometric realization of Whittaker functions and the Langlands conjecture*, preprint alg-geom/9703022, 33 p.

[Ge] E.-U. Gekeler, *On finite Drinfeld modules*, J. Algebra, 141 (1991), 187-203.

[Go1] D. Goss, *L-series of t-motives and Drinfeld modules*, The Arithmetic of Function Fields, D. Goss, D.R. Hayes and M.I. Rosen (eds.), W. de Gruyter, Berlin, 1992, 313-402

[Go2] D. Goss, *Basic structures of function fields arithmetic*, Ergebnisse der Math. und ihrer Grenzgebiete, 3. Folge, v. 35, Springer, 1996

[KvdL] V.G. Kac, J.W. van de Leur, *The n-component KP hierarchy and representation theory*, Important Developments in Soliton Theory, Springer Series in Nonlinear Dynamics, Springer, 1993, 302-343

[Kr] I.M. Krichever, *Methods of algebraic geometry in the theory of nonlinear equations* (in Russian), Uspekhi Mat. Nauk 33, 6 (1977), 183-207 ; English transl. : Russian Math. Surveys 32 (1977), 185-213

[KN] I.M. Krichever, S.P. Novikov, *Holomorphic bundles over algebraic curves and nonlinear equations*, Russian Math. Surveys 35 (1980)

[Lau1] G. Laumon, *Cohomology of Drinfeld Modular Varieties. Part 1 : Geometry, counting of points and local harmonic analysis*, Cambridge Stud. Adv. Math. 41, Cambridge University Press, 1996

[Lau2] G. Laumon, *Sur les modules de Krichever*, preprint

[LRS] G. Laumon, M. Rapoport, U. Stuhler, *$\mathcal{D}$-elliptic sheaves and the Langlands correspondence*, Invent. Math. 113, 217-338 (1993)

[LM1] Yi. Li, M. Mulase, *Category of morphisms of algebraic curves and a characterization of Prym varieties*, Max-Planck-Institut preprint MPI/92-24

[LM2] Yi. Li, M. Mulase, *Hitchin systems and KP equations*, Int. J. Math. 7 (1996), No. 2, 227-244

[Mi] J.S. Milne, *Motives over finite fields*, Proc. Sympos. Pure Math. 55 (1994), Part 1, 401-459

[MR] Yu. I. Manin, A. O. Radul, *A supersymmetric extension of the Kadomtsev-Petviashvili hierarchy*, Commun. Math. Phys. 98 (1985), 65-77

[Mu1] M. Mulase, *Category of vector bundles on algebraic curves and infinite dimensional Grassmanians*, Int. J. Math. 1, No. 3 (1990), 293-342

[Mu2] M. Mulase, *A new super KP system and a characterization of the jacobians of arbitrary algebraic super curves*, J. Diff. Geom. 34 (1991), 651-680

[Mum] D. Mumford, *An algebro-geometric construction of commuting operators and of solutions of the Toda lattice equations, Korteweg-de Vries equation and related non-linear equations*, Int. Sympos. Alg. Geom. (Kyoto 1977), Kinokuniya, Tokyo, 1977, 115-153

[Po] I.Yu. Potemine, *Arithmétique des corps globaux de fonctions et géométrie des schemas modulaires de Drinfeld*, Ph.D. Thesis, Joseph Fourier University, Grenoble (France), 1997

[PW] E. Previato, G. Wilson, *Vector bundles over curves and solutions of the KP equations*, Theta Functions Bowdoin 1987, Proc. Sympos. Pure Math. 49 (1989), part 1, Amer. Math. Soc., Providence, RI, 553-569

[Sa] M. Sato, *The KP hierarchy and infinite-dimensional Grassman manifolds*, Theta Functions Bowdoin 1987, Proc. Sympos. Pure Math. 49 (1989), part 1, Amer. Math. Soc., Providence, RI, 51-66

[SW] G. Segal, G. Wilson, *Loop groups and equations of KdV type*, Publ. Math. I.H.E.S. 61 (1985), 5-65

[Sh] T. Shiota, *The KP equation and the Schottky problem*, Sugaku Exp. vol. 3, No. 2 (1990), 183-211

[TW] Y. Taguchi, D. Wan, *L-functions of φ-sheaves and Drinfeld modules*, J. Amer. Math. Soc. 9, No. 3 (1996), 755-781

Korea Institute for Advanced Study (KIAS), 207-43 Cheongryangri-dong, Dongdaemun-gu, Seoul 130-012, Korea

E-mail address: igor@kias.kaist.ac.kr

This page intentionally left blank

http://dx.doi.org/10.1090/conm/224/03198

Contemporary Mathematics
Volume **224**, 1999

Weil classes and Rosati involutions on complex abelian varieties

Yu.G. Zarhin* and B.J.J. Moonen

1. Abelian varieties, polarizations and divisor classes

Consider a complex torus $X = \mathfrak{t}/\Gamma$, where $\mathfrak{t} \cong \mathbb{C}^g$ is a complex vector space of finite dimension g and $\Gamma \cong \mathbb{Z}^{2g}$ a discrete lattice in $\mathfrak{t}$ of (maximal) rank $2g$. We say that X is an *abelian variety* if it admits a *polarization*, by which we mean a positive definite Hermitian form

$$H : \mathfrak{t} \times \mathfrak{t} \to \mathbb{C}$$

whose imaginary part

$$L = \Im(H) : \mathfrak{t} \times \mathfrak{t} \to \mathbb{R}$$

takes integral values on Γ. Clearly, a sum of two polarizations is also a polarization. In particular, we can multiply a polarization by a positive integer to obtain another one.

There exists a polarization on X if and only if X (as a complex-analytic manifold) is algebraizable, which condition in turn is equivalent to the existence of a projective embedding $X \hookrightarrow \mathbb{P}^m$ for some m. We refer to Mumford's book [**11**] for the basic theory of abelian varieties.

EXAMPLE 1.1 (elliptic curves). Every 1-dimensional complex torus $X = \mathbb{C}/\Gamma$ admits a polarization. Namely, if $\Gamma = \mathbb{Z} \cdot \omega_1 + \mathbb{Z} \cdot \omega_2$ with $\omega_1/\omega_2 \notin \mathbb{R}$ then for each positive integer n the Hermitian form

$$(z, w) \mapsto n \cdot \frac{z\bar{w}}{|\,\Im(\omega_1\bar{\omega_2})\,|}$$

defines a polarization on X. One can check that all polarizations on X are of this form.

It should be mentioned that, for $g \geq 2$, "most" complex tori do not admit a polarization.

From now on, assume that X is an abelian variety and that H is a polarization. The form $L = L_H := \Im(H)$ is a non-degenerate skew-symmetric $\mathbb{R}$-bilinear form on $\mathfrak{t}$ such that

$$L(zx, zy) = L(x, y) \quad \forall x, y \in \mathfrak{t}\,; z \in \mathbb{S}\,,$$

1991 *Mathematics Subject Classification.* Primary 14C30, Secondary 14K20, 14K22.

* Supported by the National Science Foundation.

where

$$\mathbb{S} = \{z \in \mathbb{C}^* \mid z\bar{z} = 1\}.$$

In other words, L is $\mathbb{S}$-invariant. Conversely, if φ is an $\mathbb{S}$-invariant skew-symmetric $\mathbb{R}$-bilinear form on $\mathfrak{t}$, then $H_\varphi(x,y) = \varphi(ix,y) + i \cdot \varphi(x,y)$ defines a Hermitian form on $\mathfrak{t}$ with $\Im(H_\varphi) = \varphi$. If in addition $\varphi(\Gamma,\Gamma) \subseteq \mathbb{Z}$ then there are polarizations H_1 and H_2 such that

$$\varphi = \Im(H_1) - \Im(H_2).$$

Indeed, one may take $H_1 = nH + H_\varphi$ and $H_2 = nH$ for a sufficiently large positive integer n.

The natural map $\Gamma \otimes \mathbb{R} \to \mathfrak{t}$ is an isomorphism of real vector spaces, which we will take as an identification. Now consider the $\mathbb{Q}$-vector space $V = V_X := \Gamma \otimes \mathbb{Q}$. One may view V as a $\mathbb{Q}$-lattice in $V_\mathbb{R} := V \otimes_\mathbb{Q} \mathbb{R} = \Gamma \otimes \mathbb{R} = \mathfrak{t}$. We have

$$\Gamma \subset V \subset V_\mathbb{R} = \mathfrak{t}.$$

We will consider $\mathfrak{t} = V_\mathbb{R}$ as a real vector space provided with a $\mathbb{Q}$-lattice V and an action of $\mathbb{S}$ which gives it the structure of a complex vector space.

Let

$$\varphi : V \times V \to \mathbb{Q}$$

be a skew-symmetric $\mathbb{Q}$-bilinear form on V. Let us extend φ by $\mathbb{R}$-linearity to the skew-symmetric $\mathbb{R}$-bilinear form

$$\varphi_\mathbb{R} : V \times V \to \mathbb{R}.$$

We call φ a *divisor class* if $\varphi_\mathbb{R}$ is $\mathbb{S}$-invariant. Clearly, the set $\mathcal{D}(X)$ of divisor classes is a $\mathbb{Q}$-vector subspace of $\mathrm{Hom}_\mathbb{Q}(\wedge^2_\mathbb{Q} V, \mathbb{Q})$; in particular it is finite-dimensional. By what was said before, if φ is a divisor class then $\varphi = \Im(H_\varphi)$ for some Hermitian form H_φ on $\mathfrak{t} = V_\mathbb{R}$. It readily follows that φ is a divisor class if and only if it can be presented as a $\mathbb{Q}$-linear combination of imaginary parts of polarizations.

There is another way to describe the divisor classes, which involves the endomorphism algebra and Rosati involutions. First, notice that the endomorphism ring $\mathrm{End}(X)$ of the complex torus X is the ring of all $\mathbb{C}$-linear maps $u : \mathfrak{t} \to \mathfrak{t}$ such that $u(\Gamma) \subseteq \Gamma$. Here is an obvious alternative description: the ring $\mathrm{End}(X)$ consists of the homomorphisms $v : \Gamma \to \Gamma$ whose $\mathbb{R}$-linear extensions $v_\mathbb{R} : \mathfrak{t} \to \mathfrak{t}$ (identifying $\Gamma \otimes \mathbb{R}$ and $\mathfrak{t}$) commute with the action of $\mathbb{S}$. This last description allows us to identify the *endomorphism algebra* $\mathrm{End}^0(X) := \mathrm{End}(X) \otimes \mathbb{Q}$ with a $\mathbb{Q}$-subalgebra of $\mathrm{End}_\mathbb{Q}(V)$. It is known (see [**11**], p. 178, for example) that if X is an abelian variety, then $\mathrm{End}^0(X)$ is a semi-simple $\mathbb{Q}$-algebra.

Associated to H, there is an involution $v \mapsto v'$ on $\mathrm{End}^0(X)$, called the *Rosati involution* and characterized by

$$L(vx,y) = L(x,v'y) \quad \forall v \in \mathrm{End}^0(X)\,; x,y \in V_\mathbb{R}.$$

Since $H(x,y) = L(ix,y) + i \cdot L(x,y)$, and since the $v \in \mathrm{End}^0(X)$ commute with the action of $\mathbb{S}$, we also have

$$H(vx,y) = H(x,v'y) \quad \forall v \in \mathrm{End}^0(X)\,; x,y \in V_\mathbb{R}.$$

This implies that the Rosati involution is a positive involution. In particular, the center of $\mathrm{End}^0(X)$ is a product of totally real number fields and of CM-fields. (Recall that a CM-field is a totally imaginary quadratic extension of a totally real number field).

For example, assume that $\mathrm{End}^0(X)$ is a number field. Then there are two possibilities:

- $F = \mathrm{End}^0(X)$ is a totally real number field. The only positive involution on F is the identity map. Therefore, the Rosati involution on $\mathrm{End}^0(X)$ is the identity map.
- $F = \mathrm{End}^0(X)$ is a totally imaginary quadratic extension of a totally real number field F_0. The only positive involution on F is the "complex conjugation" (the non-trivial automorphism of F over F_0). Therefore, the Rosati involution is the complex conjugation.

Now the description of the divisor classes in terms of a Rosati involution on the endomorphism algebra goes as follows. Start with one polarization form H, with imaginary part L and associated Rosati involution $v \mapsto v'$ on $\mathrm{End}^0(X)$. Then one can show that the map which sends $u \in \mathrm{End}^0(X)$ to the $\mathbb{Q}$-bilinear form

$$(x, y) \mapsto L(ux, y)$$

on V induces a bijection

$$\{u \in \mathrm{End}^0(X) \mid u' = u\} \xrightarrow{\sim} \mathcal{D}(X).$$

2. Hodge classes and Weil classes

DEFINITION 2.1. Let n be a positive integer, and consider a skew-symmetric $\mathbb{Q}$-multilinear form $\psi \in \mathrm{Hom}_{\mathbb{Q}}(\wedge^{2n}_{\mathbb{Q}} V, \mathbb{Q})$. Extend ψ by $\mathbb{R}$-linearity to a form $\psi_{\mathbb{R}} \in \mathrm{Hom}_{\mathbb{R}}(\wedge^{2n}_{\mathbb{R}} V_{\mathbb{R}}, \mathbb{R})$. We call ψ a *Hodge class* (in degree $2n$) if $\psi_{\mathbb{R}}$ is $\mathbb{S}$-invariant.

REMARK 2.2. Clearly, a skew-symmetric $\mathbb{Q}$-bilinear form on V (with $n = 1$) is a Hodge class if and only if it is a divisor class. It is also clear that a linear combination of Hodge classes of the same degree $2n$ is a Hodge class of degree $2n$ and that the exterior product of Hodge classes $\psi_1, \ldots, \psi_k$ of degrees $2n_1, \ldots, 2n_k$ is again a Hodge class, of degree $2(n_1 + \cdots + n_k)$.

DEFINITION 2.3. A Hodge class is called *decomposable* if it can be written as a $\mathbb{Q}$-linear combination of exterior products of divisor classes. Otherwise, it is called *exceptional.*

Easy linear algebra arguments imply that if $\dim(X) \leq 3$ then all Hodge classes are decomposable. For instance, assume $\dim(X) = 3$. Then every form $\psi \in \mathrm{Hom}_{\mathbb{Q}}(\wedge^4_{\mathbb{Q}} V, \mathbb{Q})$ can be uniquely written as the exterior product of L and a skew-symmetric $\mathbb{Q}$-bilinear form on V, since $\dim(V) = 6$ and $L : V \times V \to \mathbb{Q}$ is non-degenerate. This implies that every Hodge class in degree 4 is of the form $L \wedge \varphi$ where φ is a divisor class.

It was Mumford who first gave an example of an abelian fourfold X with an exceptional Hodge class of degree 4; see [**13**]. In his examples $\mathrm{End}^0(X)$ is a CM-field of degree 8 over $\mathbb{Q}$ (i.e., X is an abelian fourfold of CM-type) which contains an imaginary quadratic subfield k. The action of k on V must satisfy the following condition: it gives rise to the natural action of $k \otimes_{\mathbb{Q}} \mathbb{C}$ on $V_{\mathbb{R}} = \mathfrak{t}$ and this action makes $\mathfrak{t}$ a free $k \otimes_{\mathbb{Q}} \mathbb{C} = \mathbb{C} \oplus \mathbb{C}$-module of rank 2. This condition may be restated as follows: if $k = \mathbb{Q}(\alpha)$ where $\alpha^2 = -d \in \mathbb{Z}_{<0}$, and if H is a polarization on X, then the Hermitian form

$$(x, y) \mapsto \frac{H(\alpha x, y)}{\sqrt{-d}}$$

on $\mathfrak{t}$ has signature $(2,2)$. (This does not depend on the choice of $\sqrt{-d} \in \mathbb{C}$.)

In [22], A. Weil proposed a different approach to the construction of exceptional Hodge classes. His construction and its natural generalization proved to be useful in various aspects of arithmetic and geometry of abelian varieties; see for example [1], [2], [4], [6], [8], [15], [19], [18], [23]. Weil's construction from [4], in its generalized form, works as follows.

Suppose E is a CM-field, and that there is a given ring homomorphism $E \hookrightarrow \mathrm{End}^0(X)$. Then V becomes a E-vector space of dimension $m = 2g/[E:\mathbb{Q}]$. The trace map $\mathrm{Tr}_{E/\mathbb{Q}} : E \to \mathbb{Q}$ gives rise to an isomorphism

$$\mathrm{Hom}_E(\wedge_E^m V, E) \overset{\mathrm{Tr}_{E/\mathbb{Q}}}{\cong} \mathrm{Hom}_{\mathbb{Q}}(\wedge_E^m V, \mathbb{Q}),$$

which yields an embedding

$$\mathrm{Hom}_E(\wedge_E^m V, E) \overset{\mathrm{Tr}_{E/\mathbb{Q}}}{\cong} \mathrm{Hom}_{\mathbb{Q}}(\wedge_E^m V, \mathbb{Q}) \subset \mathrm{Hom}_{\mathbb{Q}}(\wedge_{\mathbb{Q}}^m V, \mathbb{Q}).$$

Let $W = W_E \subset \mathrm{Hom}_{\mathbb{Q}}(\wedge_{\mathbb{Q}}^m V, \mathbb{Q})$ be the image of this embedding; it is the set of all skew-symmetric m-linear forms ϕ on the $\mathbb{Q}$-vector space V such that

$$\phi(ex_1, x_2, \ldots, x_m) = \phi(x_1, ex_2, \ldots, x_m) = \cdots = \phi(x_1, x_2, \ldots, ex_m)$$

for all $e \in E$ and $x_1, x_2, \ldots, x_m \in V$.

REMARK 2.4. The $[E:\mathbb{Q}]$-dimensional $\mathbb{Q}$-vector space W_E has a natural structure of one-dimensional E-vector space, given by

$$(e\phi)(x_1, x_2, \ldots, x_m) := \phi(ex_1, x_2, \ldots, x_m).$$

Note also that

$$(e^m\phi)(x_1, x_2, \ldots, x_m) = \phi(ex_1, ex_2, \ldots, ex_m).$$

REMARKS 2.5. (i) Let r be a positive integer and let

$$\psi : V \times \cdots \times V \to \mathbb{Q}$$

be an r-linear form on V which is not identically zero and such that

$$\psi(ex_1, x_2, \ldots, x_r) = \psi(x_1, ex_2, \ldots, x_r) = \cdots = \psi(x_1, x_2, \ldots, ex_r)$$

for all $e \in E$ and $x_1, x_2, \ldots, x_r \in V$. If $e \in E^*$ is not an rth root of unity then there exist $y_1, y_2, \ldots, y_r \in V$ such that

$$\psi(ey_1, ey_2, \ldots, ey_r) \neq \psi(y_1, y_2, \ldots, y_m).$$

To see this, first remark that

$$\psi(e^r x_1, x_2, \ldots, x_r) = \psi(ex_1, ey_2, \ldots, ex_m)$$

for all $x_1, x_2, \ldots, x_r \in V$. Now, choosing $x_1, x_2, \ldots, x_r \in V$ such that $\psi(x_1, x_2, \cdots, x_r) \neq 0$, and putting

$$y_1 = (e^r - 1)^{-1} x_1, y_2 = x_2, \ldots, y_r = x_r,$$

we have

$$\psi(ey_1, ey_2, \ldots, ey_r) - \psi(y_1, y_2, \ldots, y_r) = \psi(e^r y_1, y_2, \ldots, y_r) - \psi(y_1, y_2, \ldots, y_r) =$$
$$= \psi((e^r - 1)y_1, y_2, \ldots, y_r) = \psi(x_1, x_2, \ldots, x_r) \neq 0.$$

(ii) Applying Remark 2.4, we obtain that if ϕ is a non-zero element of W_E and $e \in E^*$ is *not* a root of unity, then there exist $x_1, x_2 \ldots, x_m \in V$ such that

$$\phi(ex_1, ex_2, \ldots, ex_m) \neq \phi(x_1, x_2, \ldots, x_m).$$

We call the (non-zero) elements of $W = W_E$ *Weil classes*, or Weil classes w.r.t. E. One easily checks that $W_{\mathbb{R}} = W \otimes_{\mathbb{Q}} \mathbb{R}$ is an $\mathbb{S}$-stable subspace of

$$\mathrm{Hom}_{\mathbb{Q}}(\wedge_{\mathbb{Q}}^m V, \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{R} = \mathrm{Hom}_{\mathbb{R}}(\wedge_{\mathbb{R}}^m V_{\mathbb{R}}, \mathbb{R}).$$

It is shown in [**4**] that $W_{\mathbb{R}}$ consists of $\mathbb{S}$-*invariant* elements (which, by definition, means that all elements of W are Hodge classes) if and only if the following condition holds: *The action of E on V gives rise to the natural action of $E \otimes_{\mathbb{Q}} \mathbb{C}$ on $V_{\mathbb{R}} = \mathfrak{t}$ and under this action $\mathfrak{t}$ becomes a free $E \otimes_{\mathbb{Q}} \mathbb{C}$-module.* If this holds then, since $\mathfrak{t}$ has rank $n = m/2$ over $E \otimes_{\mathbb{Q}} \mathbb{C}$, the number m must be even and n divides g.

It seems that most (but not all!) known examples of exceptional Hodge classes on abelian varieties, e.g. those discussed in [**12**], [**13**], [**15**], and [**17**], are *Weil classes*. For instance, if X is an abelian fourfold then each Hodge class can be presented as a linear combination of decomposable classes and Weil classes (if there are any), see [**8**], [**10**]. In Mumford's example mentioned above, the exceptional Hodge classes are Weil classes w.r.t. the imaginary quadratic field $k \subset E$.

It is natural to ask when Weil's construction leads to exceptional classes. (It is easy to see that if *some* non-zero element of W_E is exceptional then in fact *all* non-zero elements of W_E are exceptional.) Weil himself considered the case of (imaginary) quadratic fields E and proved that in this case Weil classes are exceptional for "generic" X (where the genericness includes the condition that $E = \mathrm{End}^0(X)$). In a recent paper [**9**] the authors have given an explicit necessary and sufficient condition for (non-zero) Weil classes to be exceptional. This condition is formulated in terms of the endomorphism algebra of X and uses Albert's classification of semi-simple finite-dimensional $\mathbb{Q}$-algebras with a positive involution.

3. Cohomological interpretation

Let us now explain the relevance of the above considerations in slightly different terminology. First, the lattice Γ is the first integral homology group $\mathrm{H}_1(X, \mathbb{Z})$ of X, and also we have natural isomorphisms $V = \mathrm{H}_1(X, \mathbb{Q})$ and $V_{\mathbb{R}} = \mathrm{H}_1(X, \mathbb{R})$. The fact that X is a torus then implies that $\mathrm{Hom}_{\mathbb{Q}}(\wedge_{\mathbb{Q}}^r V, \mathbb{Q}) \cong \mathrm{H}^r(X, \mathbb{Q})$ and $\mathrm{Hom}_{\mathbb{R}}(\wedge_{\mathbb{R}}^r V_{\mathbb{R}}, \mathbb{R}) \cong \mathrm{H}^r(X, \mathbb{R})$. The exterior product of forms corresponds to the cup-product of cohomology classes. The forms $L = L_H \in \mathrm{Hom}_{\mathbb{Q}}(\wedge_{\mathbb{Q}}^2 V, \mathbb{Q}) = \mathrm{H}^2(X, \mathbb{Q})$ are rational multiples of the cohomology classes of hyperplane sections of X and each class of a hyperplane section coincide with L_H for some polarization H. The subspace

$$\mathcal{D}(X) \subset \mathrm{Hom}_{\mathbb{Q}}(\wedge_{\mathbb{Q}}^2 V, \mathbb{Q}) = \mathrm{H}^2(X, \mathbb{Q})$$

is the set of rational multiples of cohomology classes of divisors on X.

For even r the identification

$$\mathrm{Hom}_{\mathbb{Q}}(\wedge_{\mathbb{Q}}^r V, \mathbb{Q}) = \mathrm{H}^r(X, \mathbb{Q})$$

identifies Hodge classes as defined here with conventional ones [**3**],[**4**],[**11**]. A celebrated conjecture of Hodge [**20**] asserts that all Hodge classes are algebraic (the converse is known to be true). For decomposable classes this is a consequence of Lefschetz' theorem on $(1,1)$-classes (see e.g. [**5**], Ch. 1, Sect. 2), and Weil suggested his construction as a source of possible counterexamples to the Hodge conjecture. See [**17**], [**15**], [**16**] and [**21**] for some rare examples where the algebraicity of exceptional Weil classes is proven.

4. Main results

The motivation of the present paper is to give an explanation, in completely elementary terms, why in the examples of Mumford and Weil one gets *exceptional* Weil classes. Namely, we prove the following statement.

THEOREM 4.1. *Consider a complex abelian variety X with a given inclusion $E \hookrightarrow \mathrm{End}^0(X)$ of a CM-field E in its endomorphism algebra (sending $1 \in E$ to the identity on X). Assume that E is stable under all Rosati involutions on* $\mathrm{End}^0(X)$ *and that $\mathfrak{t}$ is a* free *$E \otimes_{\mathbb{Q}} \mathbb{C}$-module. Then all non-zero elements of $W = W_E$ are exceptional Hodge classes.*

REMARK 4.2. If Rosati involution leaves E stable then it acts on E as the complex conjugation.

REMARK 4.3. If $\mathrm{End}^0(X)$ is a CM-field then there is only one Rosati involution, namely the complex conjugation. In particular, if $\mathrm{End}^0(X)$ contains an imaginary quadratic subfield k (e.g., $\mathrm{End}^0(X) = k$) then the Rosati involution leaves k stable and, assuming that $\mathfrak{t} = V_{\mathbb{R}}$ is a *free* $E \otimes_{\mathbb{Q}} \mathbb{C}$-module, we get the exceptionality of all non-zero Weil classes. This explains the examples of Mumford and Weil. In fact, in the situation considered by Weil we slightly improve the result, since we only need the equality $\mathrm{End}^0(X) = k$.

Theorem 4.1 is an immediate corollary of the following statement.

THEOREM 4.4. *Let Pol_E be set of all polarizations H on X such that E is stable under the associated Rosati involution. Let*

$$\mathcal{D}_E := \{\Im(H) \in \mathcal{D}(X) \subset \mathrm{Hom}_{\mathbb{Q}}(\wedge^2_{\mathbb{Q}} V, \mathbb{Q}) \mid H \in \mathrm{Pol}_E\}$$

be the set of their imaginary parts, viewed as divisor classes. Let r be an even positive integer and let $\psi \in \mathrm{Hom}_{\mathbb{Q}}(\wedge^r_{\mathbb{Q}} V, \mathbb{Q})$ be a non-zero skew-symmetric form with

$$\psi(ex_1, x_2, \dots, x_r) = \psi(x_1, ex_2, \dots, x_r) = \cdots = \psi(x_1, x_2, \dots, ex_r)$$

for all $e \in E$ and all $x_1, x_2 \dots, x_r \in V$. (This is the case, for example, if $r = m := \dim_E(V)$ and $\psi \in W_E$ is a non-zero Weil class). Then ψ is not a $\mathbb{Q}$-linear combination of exterior products of bilinear forms L_H ($H \in \mathrm{Pol}_E$).

REMARK 4.5. It is shown in [**7**], Lemma 9.2, that the set Pol_E is always non-empty.

PROOF OF THEOREM 4.4. Choose a polarization $H \in \mathrm{Pol}_E$ and let

$$L_H = \Im(H) : V \times V \to \mathbb{Q}$$

be its imaginary part, viewed as a skew-symmetric $\mathbb{Q}$-bilinear form on V. The assumption that E is stable under the Rosati involution $u \mapsto u'$ attached to H means that $u' = \bar{u}$ is the complex conjugate of u and

$$L_H(ux, y) = L_H(x, \bar{u}y) \quad \forall u \in E; x, y \in V\,.$$

Consider the multiplicative subgroup

$$\mathbb{U}_E = \{u \in E^* \mid u\bar{u} = 1\}\,.$$

Since E is a CM-field, $\mathbb{U}_E$ is infinite. Since E contains only finitely many roots of unity, $\mathbb{U}_E$ contains an element e which is *not* a root of unity. Since $e \in \mathbb{U}_E$, we have

$$L_H(ex, ey) = L_H(x, \bar{e}ey) = L_H(x, y) \quad \forall x, y \in V.$$

This implies that if an alternating r-linear form ω on V can be presented as a linear combination of exterior products of bilinear forms L_H $(H \in \mathrm{Pol}_E)$ then

$$\omega(ex_1, ex_2, \dots, ex_r) = \omega(x_1, x_2, \dots, x_r) \quad \forall x_1, x_2, \dots, x_m \in V.$$

Since e is not a root of unity, it follows from Remark 2.5(i) that there exist $y_1, y_2, \cdots, y_r \in V$ such that

$$\psi(ey_1, ey_2, \dots ey_r) \neq \psi(y_1, y_2, \dots y_r).$$

$\square$

Acknowledgements. The first named author (Y. Z.) would like to thank the organizers of the conference for fantastic warm hospitality.

References

[1] Y. André. *Une remarque à propos de cycles de Hodge de type CM.* Seminaire de Théorie des Nombres, Paris, 1989-90, Progress in Math. 102 (1992), 1–7.

[2] Y. André. *Sur une théorie inconditionelle des motifs.* Publ. Math. de l'I.H.E.S. 83 (1996), 5–49.

[3] P. Deligne. *Théorie de Hodge II.* Publ. Math. de l'I.H.E.S. 40 (1972), 5–57.

[4] P. Deligne. *Hodge cycles on abelian varieties (notes by J.S. Milne).* Lecture Notes in Math. 900 (1982), 9–100.

[5] P. Griffiths and J. Harris. Principles of Algebraic Geometry. John Wiley and Sons, New York, 1978.

[6] B. Gross. *On periods of abelian integrals and a formula of Chowla-Selberg.* Invent. Math. 45 (1978), 193–211.

[7] R.E. Kottwitz. *Points on some Shimura varieties over finite fields.* J. Amer. Math. Soc. 5 (1992), 373–444.

[8] B.J.J. Moonen and Yu.G. Zarhin. *Hodge classes and Tate classes on simple abelian fourfolds.* Duke Math. J. 77 (1995), 553–581.

[9] B.J.J. Moonen and Yu.G. Zarhin. *Weil classes on abelian varieties.* J. reine angew. Math. 496 (1998), 83–92.

[10] B.J.J. Moonen and Yu.G. Zarhin. *Hodge classes and Tate classes on abelian fourfolds*, in preparation.

[11] D. Mumford. Abelian varieties (second edition). Oxford University Press, Oxford, 1974.

[12] V.K. Murty. *Exceptional Hodge classes on certain abelian varieties.* Math. Ann. 268 (1984), 197–206.

[13] H. Pohlman. *Algebraic cycles on abelian varieties of complex multiplication type.* Ann. of Math. 88 (1968), 161–180.

[14] K. Ribet. *Hodge classes on certain types of abelian varieties.* Amer. J. of Math. 105 (1983), 523–538.

[15] C. Schoen. *Hodge classes on self-products of a variety with an automorphism.* Compositio Math. 65 (1988), 3–32.

[16] C. Schoen. *Addendum to: Hodge classes on self-products of a variety with an automorphism*, to appear.

[17] T. Shioda. *Algebraic cycles on abelian varieties of Fermat type.* Math. Ann. 258 (1981), 65–80.

[18] A. Silverberg and Yu.G. Zarhin. *Connectedness extensions for abelian varieties.* Math. Z. 228 (1998), 387–403.

[19] A. Silverberg and Yu.G. Zarhin. *Hodge groups of abelian varieties with purely multiplicative reduction.* Izvestija RAN 56 (1996), 149–158; Izvestiya:Mathematics **60**:2, 379–389.

[20] J. Tate. *Algebraic cycles and poles of zeta functions.* Arithmetical Algebraic Geometry, Harper and Row, New York (1965), 93-110.

[21] B. van Geemen. *Theta functions and cycles on some abelian fourfolds.* Math. Z. 221 (1996), 617–631.

[22] A. Weil. *Abelian varieties and the Hodge ring.* Collected papers, Vol. III, 421–429.

[23] Yu. G. Zarhin *Torsion of abelian varieties, Weil classes and cyclotomic extensions.* Math. Proc. Cambridge Phil. Soc., to appear.

DEPARTMENT OF MATHEMATICS, PENNSYLVANIA STATE UNIVERSITY, UNIVERSITY PARK, PA 16802, USA

E-mail address: `zarhin@math.psu.edu`

DEPARTMENT OF MATHEMATICS, PRINCETON UNIVERSITY, PRINCETON, NJ 08544, USA

E-mail address: `moonen@math.Princeton.edu`

http://dx.doi.org/10.1090/conm/224/03192

Contemporary Mathematics
Volume **224**, 1999

ON SOME OPEN PROBLEMS RELATED TO THE RESTRICTED BURNSIDE PROBLEM

EFIM ZELMANOV[1]

Yale University
Department of Mathematics
New Haven, CT 06520-8283

and

KIAS
207-43 Cheongryangri-dong
Seoul 130-012
South Korea

Dedicated to Hyo Chul Myung on the occasion of his 60th birthday

In this short survey I will try to review some recently found connections between the Restricted Burnside Problem and some still open problems in Algebra and Geometry.

An element g of a group G is called periodic if there exists $n \geq 1$ such that $g^n = 1$. The smallest number n with this property is called the order of g. A group G is periodic if every element of G is periodic.

A group G is said to be periodic of bounded exponent if orders of all elements are uniformly bounded from above. In other words, G is periodic of bounded exponent if there exists $n \geq 1$ such that $g^n = 1$ for an arbitrary element $g \in G$. The smallest number n with this property is called the exponent of G, $n = \exp(G)$.

In 1902 W. Burnside formulated the following problem.

The Burnside Problem. Is it true that a finitely generated group of bounded exponent is finite?

Clearly, a finite group is finitely generated and of bounded exponent. The question is if the reverse is true, that is, if these two properties are enough to make a group finite? R. Bruck put the question in more general terms:

What makes a group finite?

[1]Partially supported by NSF Grant DMS-9704132

1991 Mathematics Subject Classification: Primary 20F50. Secondary 20F40, 20F45.

If $\exp(G) = 2$ then the group G is abelian and the problem is trivial.

W. Burnside [6], I.N. Sanov [23] and M. Hall [9] solved The Burnside Problem positively for groups of exponents 3, 4, 6 respectively. However, in 1968 P.S. Novikov and S.I. Adian [21] constructed for an arbitrary odd number $n \geq 4381$ an infinite 2-generated group of exponent n. This was the negative solution of The Burnside Problem.

In 1994, S. Ivanov [11] constructed infinite 2-generated groups of exponent $n = 2^k$ for sufficiently large k (for improved bounds see also I. Lysenok [16]). Hence, now we can say that the Burnside Problem has negative solution for groups of a sufficiently large exponent n whether odd or even.

In the late 30's a somewhat weaker version of The Burnside Problem was formulated (see [8, 20, 28]). It became known as the Restricted Burnside Problem.

The Restricted Burnside Problem. Is it true that for given $m \geq 1, n \geq 1$ there are only finitely many finite m generated groups of exponent n?

Let us discuss how these two problems are related.

Let F_m denote the free group on m free generators $x_1, \dots, x_m$. Let F_m^n be the subgroup of F_m generated by all n-th powers $a^n, a \in F_m$. The quotient group $B(m,n) = F_m/F_m^n$ is the universal m generated group of exponent n and all other m generated groups of exponent n are homomorphic images of $B(m,n)$. Thus The Burnside Problem is the problem whether groups $B(m,n)$ are finite or infinite.

The Restricted Burnside Problem asks if the group $B(m,n)$ (whether finite or infinite) has finitely many finite homomorphic images or, equivalently, if $B(m,n)$ has finitely many subgroups of finite index. If the answer is "yes" then the intersection $H_0 = \cap\{H \mid [B(m,n) : H] < \infty\}$ is a subgroup of finite index. Then $B_0(m,n) = B(m,n)/H_0$ is the universal m generated finite group of exponent n. All other finite m generated groups of exponent n are homomorphic images of $B_0(m,n)$. Thus the Restricted Burnside Problem is the problem whether there exists a universal m generated finite group of exponent n.

In 1956 P. Hall and G. Higman [10] proved the Reduction Theorem: let $n = p_1^{k_1} \cdots p_r^{k_r}$ be a product of powers of distinct prime numbers. If (1) for every factor $p_i^{k_i}$ the Restricted Burnside Problem for groups of exponent $p_i^{k_i}$ has positive solution, (2) there are finitely many finite m generated simple groups of exponent n, (3) for each of these simple groups the Schreier Conjecture is valid, then the Restricted Burnside Problem for groups of exponent n also has positive solution.

From the announced classification of Finite Simple Groups it follows that (2) and (3) are always true. Thus the problem gets reduced to p-power exponents.

In 1958 A.I. Kostrikin [12,13] solved the Restricted Burnside Problem for groups of prime exponent. Let G be a finite p-group, let $G = G_1 > G_2 > \cdots$ be its lower central series. The abelian group $L(G) = \bigoplus_{i \geq 1} G_i/G_{i+1}$ with the bracket $[a_i G_{i+1}, b_j G_{j+1}] = (a_i, b_j) G_{i+j+1}$ (here (a_i, b_j) is the group commutator of the elements a_i, b_j) is a Lie ring. If the group G has exponent p then G_i/G_{i+1} are elementary abelian p-groups and therefore $L(G)$ is an algebra over the field $\mathbb{Z}/p\mathbb{Z}$. Moreover, under this assumption the Lie algebra $L(G)$ satisfies the Engel identity $[\dots \underbrace{[x,y],y],\dots,y]}_{p-1} = 0 (E_{p-1})$.

If $a_1, \dots, a_m$ generate G then $L(G)$ is generated by $a_1G_2, \dots, a_mG_2 \in G_1/G_2$. A.I. Kostrikin proved that an m generated Lie algebra over a field of characteristic p (or 0) satisfying the Engel identity (E_{p-1}) is nilpotent. This implied a positive solution of The Restricted Burnside Problem for groups of prime exponent.

In [29, 30] this theorem was generalized to arbitrary Lie rings satisfying an Engel identity which implied (though in a less straightforward way than in the case of groups of prime exponent) a positive solution of The Restricted Burnside Problem for groups of prime-power exponent. Together with the Reduction Theorem it settles the general case.

Now let us look at this problem from a different point of view. A group G is said to be *residually finite* if there exists a system of homomorphisms $\varphi_i : G \to G_i$, such that all groups G_i are finite and $\bigcap\limits_i \ker \varphi_i = (1)$. The system of subgroups of finite index $\ker \varphi_i$ can be taken for a basis of neighborhoods of 1 thus making G a topological group. If G is complete in this topology then G is said to be a *profinite* group. A profinite group can be defined also as an inverse limit of finite groups. Clearly, any residually finite group can be embedded into its profinite completion. For an arbitrary group G the quotient group $G/\cap\{H \mid [G:H] < \infty\}$ is residually finite. Its completion is called the profinite completion of G. We will denote it as $\hat{G}$.

It is easy to see that

$$\begin{aligned} &\text{The Restricted Burnside Problem} \\ \Leftrightarrow\ &\text{The Burnside Problem for residually finite groups} \\ \Leftrightarrow\ &\text{The Burnside Problem for profinite groups.} \end{aligned}$$

The free group F_m is residually finite. Its profinite completion $\hat{F}_m$ is called the free profinite group. It deserves this name because an arbitrary mapping of the free generators $x_1, \dots, x_m$ into a profinite group G can be uniquely extended to a continuous homomorphism $\hat{F}_m \to G$.

As above, let $\hat{F}_m^n$ be the (abstract) subgroup of $\hat{F}_m$ generated by all n-th powers $a^n, a \in \hat{F}_m$. Let $c\ell(\hat{F}_m^n)$ be the closure of $\hat{F}_m^n$ in $\hat{F}_m$. It is not difficult to see that

$$B_0(m,n) \cong \hat{F}_m / c\ell(\hat{F}_m^n).$$

1. Primitive Elements

A number of open problems related to The Restricted Burnside Problem can be formulated as follows: what happens if we impose periodicity not on all elements of a group but on some of them?

To be more precise, let M be a subset of the free group F_m. Let $H(M^n)$ denote the closed normal subgroup generated by the subset $\{a^n, a \in M\}$ in $\hat{F}_m$.

The first subset M that we will discuss is the set of all primitive elements of F_m.

Definition. An element $v \in F_m$ is said to be *primitive* if there exists an automorphism $\varphi \in \operatorname{Aut} F_m$ such that $v = \varphi(x_1)$.

In other words, v is a primitive element if it can be included into a system of m free generators of F_m.

Problem 1. Let $m \geq 3$. Is the group $\hat{F}_m/H(M^n)$ solvable-by-finite?

The finitary version of this problem is

Problem 1'. Do there exist functions $N(m,n), S(m,n)$ such that, if G is a finite group generated by $m \geq 3$ elements $a_1, \ldots, a_m$ and for an arbitrary primitive element $v(x_1, \ldots, x_m) \in F_m$ we have $v(a_1, \ldots, a_m)^n = 1$, then G contains a normal subgroup of index $\leq N(m,n)$ which is solvable of degree $\leq S(m,n)$?

The group $\hat{F}_m/H(M^n)$ does not have, however, to be finite.

Example (see [4]). Let V be a vector space over a field F of zero characteristic and let G be a finite subgroup of $GL(V)$ which acts fixed-point-freely, i.e. for arbitrary elements $a \in V, g \in G$ $ag = a$ implies $a = 0$ or $g = 1$. This means that G can be realized as a Frobenius complement and so its structure is determined by classical works of W. Burnside and H. Zassenhaus (see [6], [27]).

For an element $a \in V$ let $T_a : V \to V$ denote the translation $T_a : b \to b+a, b \in V$. Consider the semidirect product $T_V G$. Let $|G| = n$. For arbitrary elements $a \in V$, $1 \neq g \in G$ we have $(T_a g)^n = T_{a+ag+\cdots+ag^{n-1}} T_g n = T_0 1 = 1$, because the element $a(1 + g + \cdots + g^{n-1})$ is fixed by g.

Now suppose that G is generated by elements $g_1, \ldots, g_k$ and no $k-1$ elements generate G. Then for an arbitrary primitive element $v \in M$ $v(g_1, \ldots, g_k) \neq 1$. Hence, for arbitrary elements $a_1, \ldots, a_k \in V$ we have $v(T_{a_1} g_1, \ldots, T_{a_k} g_k)^n = 1$. It is easy to see that there exist elements $a_1, \ldots, a_k \in V$ such that $\langle T_{a_1} g_1, \ldots, T_{a_k} g_k \rangle \cap T_V \neq (1)$. Hence the group $H = \langle T_{a_1} g_1, \ldots, T_{a_k} g_k \rangle$ is infinite. H, however, is abelian-by-finite, hence linear, hence residually finite. The profinite completion $\hat{H}$ is a homomorphic image of the group $\hat{F}_m/H(M^n)$.

Theorems of W. Burnside, H. Zassenhause, J. Thompson, and G. Higman do not allow to develop this construction into a counterexample to Problem 1.

Let $T_m = \langle x_1, \ldots, x_m, y_1, \ldots, y_m \mid (x_1, y_1) \cdots (x_m, y_m) = 1 \rangle$ be a surface group. An element $v \in \Gamma_m$ is said to be primitive if there exists an automorphism $\varphi \in$ Aut Γ_m such that $v = \varphi(x_1)$. Let M be the set of all primitive elements of Γ_m. Let $\hat{\Gamma}_m$ be the profinite completion of Γ_m and let $H(M^n)$ be the closed normal subgroup of $\hat{\Gamma}_m$ generated by $M^n = \{v^n, v \in M\}$.

Problem 2. Let $m \geq 3$. Is the group $\hat{\Gamma}/H(M^n)$ soluble-by-finite?

In the work [4], F. Bogomolov and L. Katzarkov interpreted Burnside groups in the fundamental groups of smooth complex projective surfaces. If Problem 2 has positive solution then the Bogomolov-Katzarkov construction yields examples of smooth projective complex surfaces with rather wild fundamental groups.

The same construction (see [4]) establishes an interesting connection between The Shafarevich Conjecture and The Burnside Problem. The Shafarevich Conjecture states that the universal covering $\tilde{X}$ of a smooth complex projective variety is holomorphically convex, meaning that for every infinite sequence of points without limit points in $\tilde{X}$ there exists a holomorphic function unbounded on this sequence.

In [4] it is shown that if The Shafarevich Conjecture is valid then for an arbitrary $n \geq 1$ all groups $B(m,n), m \geq 2$, are simultaneously finite or simultaneously infinite. Thus, if for some exponent n the group $B(2,n)$ were finite while a group $B(m,n)$ on larger number of generators were infinite, that would provide a counterexample to The Shafarevich Conjecture.

There is another reason to be interested in Problems 1,2.

In 1990 E. Formanek and C. Procesi [7] proved that for $m \geq 3$ the automorphism group $\mathrm{Aut}(F_m)$ is not linear. The problem of linearity of the group $\mathrm{Aut}(F_2)$ is open, as it is open for braid groups and mapping class groups.

Let $\rho : \mathrm{Aut}(F_m) \to GL(n, F)$ be a linear representation. The group F_m is embedded into $\mathrm{Aut}(F_m)$ via inner automorphisms. Since an arbitrary primitive element $v \in F_m$ is conjugate to x_1 in $\mathrm{Aut}(F_m)$ it follows that $\rho(v) = v(\rho(x_1), \ldots, \rho(x_m))$ is conjugate to $\rho(x_1)$ in $GL(n, F)$. Let $f(t)$ be the characteristic polynomial of $\rho(x_n)$. For an arbitrary primitive element $v \in F_m$ we have $f(v(\rho(x_1), \ldots, \rho(x_n\ ) = 0$.

Problem 3. Let G be a subgroup of $GL(n, F)$ generated by m elements $g_1, \ldots, g_m, m \geq 3$. Suppose that there exists a polynomial $f(t)$ such that for an arbitrary primitive element $v \in F_m$ we have $f(v(g_1, \ldots, g_m)) = 0$. Is it true that the group G is solvable-by-finite?

If there exists a polynomial $f(t)$ such that for an arbitrary element $g \in G \leq GL(n, F)$ there holds $f(g) = 0$ then the original argument of W. Burnside [6] implies that G is unipotent-by-finite.

2. Finitely Presented Profinite Groups

A. Yu. Ol'Shansky [15] (and independently E. Rips) raised the following question.

Problem 4. Does there exist a finite subset $M \subseteq F_m$ such that the group $\hat{F}_m / H(M^n)$ is finite?

The finitary version of this problem is

Problem 4'. Does there exist a function $N(m, n)$ such that, if G is a finite group generated by m elements $a_1, \ldots, a_m$ and for an arbitrary product $a_{i_1}^{\pm 1} \cdots a_{i_k}^{\pm 1}$ of length $k \leq N(m, n)$; $1 \leq i_1, \ldots, i_k \leq m$; we have $(a_{i_1}^{\pm 1} \cdots a_{i_k}^{\pm 1})^n = 1$, then $g^n = 1$ for an arbitrary element $g \in G$?

The existence of such a function $N(m, p)$ for a sufficiently large prime number p would imply the existence of a nonresidually finite hyperbolic group which was conjectured by M. Gromov. Indeed, S.I. Adian and I. Lysenok [2] proved that for a sufficiently large prime number p and $m \geq 2$ a group that has a presentation $\langle x_1, \ldots, x_m \mid v_1^p = 1, \ldots, v_r^p = 1 \rangle$, where $v_1, \ldots, v_r$ are arbitrary elements from F_m, is hyperbolic. Suppose that the number $N(m, p)$ exists and let $v_1, \ldots, v_r$ be all words of length $\leq N(m, p)$. Let $G = \langle x_1, \ldots, x_m | v_1^p = 1, \ldots, v_r^p = 1 \rangle$. Let $\varphi : G \to G'$ be a homomorphism onto a finite group. The group G' is generated by $\varphi(x_1), \ldots, \varphi(x_m)$ and for an arbitrary word v of length $\leq N(m, p)$ we have $v(\varphi(x_1), \ldots, \varphi(x_m))^p = 1$. Hence, the whole grop G' has exponent p. In view of the positive solution of the Restricted Burnside Problem there are finitely many finite m generated groups of exponent p. Hence, G has only finitely many finite homomorphic images. Hence, the profinite completion $\hat{G}$ is finite. On the other hand for $p > 665$ the group G is infinite by the results of P.S. Novikov and S.I. Adian ([21], [1]).

If The Burnside group $B(m, n) = F_m / F_m^n$ is finite then the Problem 4 has positive solution as well. Indeed, the subgroup of finite index F_m^n in F_m is finitely generated. It is sufficient to let $N(m,n)$ be the maximum of lengths of these generators.

C. Martinez [17] proved the existence of such a function $N_s(m,n)$ for solvable groups.

Theorem (C. Martinez, [17]. *There exists a function $N_s(m,n)$ such that if G is a finite solvable group generated by m elements $a_1,\dots,a_m$ and for an arbitrary product $a_{i_1}^{\pm 1}\cdots a_{i_k}^{\pm 1}, k \le N_s(m,n)$ we have $(a_{i_1}^{\pm 1}\cdots a_{i_k}^{\pm 1})^n = 1$ then $G^n = (1)$.*

The Proglem 4' has been reduced in [17] to the question if there exists such a function $N_{si}(m,n)$ for finite simple groups. However, it is open even for alternating groups. I will risk formulating the following question for exponent 5, since 5 is the smallest number for which The Burnside Problem is open.

Problem 4". Does there exist a number N with the following property: for any two generators a_1, a_2 of an alternating group $A_n, n \ge 2$, there exists a product $b = a_{i_1}^{\pm 1}\cdots a_{i_k}^{\pm 1}, k \le N, 1 \le i_1,\dots,i_k \le 2$ such that $b^5 \ne 1$?

3. Products of Powers

In our discussion of the Restricted Burnside Problem we stressed that $B_0(m,n) = \hat{F}_m/c\ell(\hat{F}_m^n)$. What happens if we forget to take the closure of $\hat{F}_m^n$?

Problem 5. Let G be a (topologically) finitely generated profinite group. Is the group G^n which is (abstractly) generated by all n-th powers $a^n, a \in G$, closed?

Here is the finitary version of the problem.

Problem 5'. Does there exist a function $N(m,n)$ such that if G is a finite m generated group then $G^n = \{a_1^n \cdots a_{N(m,n)}^n \mid a_1,\dots,a_{N(m,n)} \in G\}$?

It has been known for some time (see, for example, [25]) that a positive answer to this question would imply the positive answer to the following question of J.-P. Serre: is it true that in a finitely generated profinite group every subgroup of finite index is closed?

Suppose that Problem 5 has positive solution. Let G be a finitely generated profinite group, let H be a subgroup of finite index, let $n = |G:H|!$ Then $G^n \subseteq H$. If the subgroup G^n is closed in G then it is legal to consider the quotient group G/G^n which is a profinite group. As The Restricted Burnside Problem is The Burnside Problem for profinite groups and it has positive solution we conclude that the group G/G^n is finite. Hence, H is a finite union of cosets of G^n and thus is closed.

J.-P. Serre proved the conjecture for pro-p groups [24]. For further generalizations see [3, 22].

Speaking of problems 5, 5', in the already mentioned work [17] of C. Martinez the existence of a funciton $N_i(m,n)$ was proved for all nilpotent groups. In [18] this result was extended to solvable groups of bounded Fitting height. Finally, in [19] the existence of a bound was established for finite simple groups. The problem, however, is still open for solvable groups.

References

1. S.I. Adian, *The Burnside Problem and Identities in Groups*, Ergebnisse der Mathematik und ihrer Grenzgebiete 95, Springer-Verlag, Berlin, 1979.
2. S.I. Adian, I.G. Lysenok, *The method of classification of periodic words and the Burnside Problem*, Contemporary Math **131** (1992), 13–28.
3. M.P. Anderson, *Subgroups of finite index in profinite groups*, Pacific J. Math **62** (1976), 19–28.
4. F. Bogomolov, L. Katzarkov, *Complex projective surfaces and infinite groups*, preprint.
5. W. Burnside, *On an unsettled question in the theory of discontinuous groups*, Quart. J.Pure Appl. Math. **33** (1902), 230–237.
6. ______, *Theory of groups of finite order, 2nd edition*, Cambridge Univ. Press, Cambridge, 1911.
7. E. Formanek, C. Procesi, *The automorphism group of a free group is not linear*, J. of Algebra **149** (1992), 494–499.
8. O. Grün, *Zusammenhang zwischen Potenz bildung und kommutator bildung*, J. Reine Angew Math. **182** (1940), 158–177.
9. M. Hall, *Solution of The Burnside problem for exponent ∂*, Proc. Nat. Acad. Sci. USA **43** (1957), 751–753.
10. P. Hall, G. Higman, *On the p-length of p-soluble groups and reduction theorems for Burnside's problem*, Proc. London Math. Soc. **6** (1956), 1–42.
11. S. Ivanov, *The free Burnside groups of sufficiently large exponents*, Intern. J. Algebra and Computation **4, no. 1& 2** (1994), 1–308.
12. A.I. Kostrikin, *On The Burnside problem*, Izvestia AN ´R **23, no. 1** (1959), 3–34.
13. ______, *Sanwiches in Lie algebras*, Matem. Sb. **110** (1979), 3–12.
14. ______Around Brunside, Ergebnisse der Mathematik und ihrer Grenzgebiete, Berlin, 1990.
15. *Kourovka Notebook (Unsolved problems in Group Theory)*, Novosibirsk, 1993.
16. I.G. Lysenok, *Infinite Burnside groups of even exponent*, Izvestia of the Academy of Sciences **60, no. 3** (1996), 3–224.
17. C. Martinez, *On power subgroups of profinite groups*, Trans. AMS **345** (1994), 865–889.
18. ______, *Power subgroups of pro(finite solvable) groups*, Bull. London Math. Soc. **28, no. 134** (1996), 481–487.
19. C. Martinez, E. Zelmanov, *Products of powers in finite simple groups*, Israel J. Math **96** (1996), 469–479.
20. W. Magnus, *Über Gruppen und zugeordnete Liesche Ringe*, J. Reine Angew Mth. **182** (1940), 142–158.
21. P.S. Novikov, S.I. Adian, *On infinite periodic groups I,II,*, Izvestia AN ´R **32, no. 1** (1968), 212–244 (I), 251–254 (II), 709–731 ( ).
22. B.C. Oltikor, L. Ribes, *Commutators of certain finitely generated soluble groups*, Canad. J. Math. **21** (1969), 1160–1164.
23. I.N. Sanov, *Solution of The Burnside problem for exponent 4*, Uch. Zapiski, Leningrad State University **10** (1940), 166-170.
24. J.-P. Serre, *Cohomoloigy Galoisienne*, Springer, Berlin, 1964.
25. A. Shalev, *Finite p-groups, in finite and locally finite groups*, NATO ASI Series, Kluwer, 1995, 401–450.
26. J.G. Thompson, *Finite groups with fixed-point-free automorphisms of prime order*, Proc. Nat. Acad. Sci. USA **45** (1959), 578–581.
27. H. Zassenhaus, Abh. Math. Sem. Univ. Hamburg **11** (1936), 17–44 paper Kennzeichnung endlicher linearer Gruppen als Permutationsgruppen.
28. ______, *Ein verfahren, jeder endlichen p-Gruppe einem Lie-Ring mit der Charakteristik p zuzuordnen*, Abh. Math. Sem. Univ. Hamburg **13** (1940), 200–207.
29. E.I. Zelmanov, *The solution of the restricted Burnside problem for groups of odd exponent*, Math. USSR Izv. **36** (1990), 41–60.
30. ______, *The solution of the restricted Burnside problem for 2-groups*, Matem. Sbornik **182** (1991), 568–592.

This page intentionally left blank

Selected Titles in This Series

(Continued from the front of this publication)

(See the AMS catalog for earlier titles)

This page intentionally left blank

ISBN 0-8218-0972-5

AMS on the Web
www.ams.org