Math 615: Lecture of April 6, 2007

We next want to prove unique factorization in all regular local rings, and we shall use an entirely different method. We first discuss the basic facts about the divisor class group $\mathcal{C}\ell\,(R)$ of a normal Noetherian domain R.

Primary decomposition of principal ideals in a normal Noetherian domain has a particularly simple form: there are no embedded primes, and so if $0 \neq a \in P$ the P-primary component is unique, and corresponds to the contraction of an ideal primary to the maximal ideal in R_P, a discrete valuation ring. But the only ideals primary to PR_P in R_P are the powers of PR_P, and so every P-primary ideal has the form $P^{(n)}$ for a unique positive integer n, where $P^{(n)}$ denotes the n th sybolic power of P, the contraction of P^nR_P to R. Thus, if $a \neq 0$ is not a unit, then aR is uniquely an intersection

$$P_1^{(k_1)} \cap \cdots \cap P_n^{(k_n)}.$$

Form the free abelian group G on generators that are taken either to be the height one primes of R (as we shall do) or elements in bijective correspondence with the height one primes of R. The elements of G are called *divisors*. If the ideal aR has the primary decomposition indicated, the element $\sum_{i=1}^n k_iP_i$ is called the *divisor* of a, and denoted $\mathrm{div}\,(a)$. The coefficient of P is the same as the order of a in the discrete valuation ring R_P. By convention, the divisor of a unit of R is 0. The quotient of G by the span of all the divisors is called the *divisor class group* of R, and denoted $\mathcal{C}\ell\,(R)$. It turns out to vanish if and only if R is a UFD. In fact, P maps to 0 in $\mathcal{C}\ell\,(R)$ iff P is principal. One can say something even more general. An ideal I of a Noetherian ring R is said to have *pure height* h if all associated primes of I as an ideal have height h. The unit ideal, which has no associated primes, satisfies this condition by default. If I is an ideal of a Noetherian normal domain of pure height one, then I has a primary decomposition $P_1^{(k_1)} \cap \cdots \cap P_n^{(k_n)}$, and so there is a divisor $\mathrm{div}\,(I)$ associated with I, namely $\sum_{i=1}^n k_iP_i$. If $I = R$ is the unit ideal, we define $\mathrm{div}\,(I) = 0$.

Theorem. *Let R be a Noetherian normal domain. If I has pure height one, then so does fI for every nonzero element f of R, and $\mathrm{div}\,(fI) = \mathrm{div}\,(f) + \mathrm{div}\,(I)$. For any two ideals I and J of pure height one, $\mathrm{div}\,(I) = \mathrm{div}\,(J)$ iff $I = J$, while the images of $\mathrm{div}\,(I)$ and $\mathrm{div}\,(J)$ in $\mathcal{C}\ell\,(R)$ are the same iff there are nonzero elements f, g of R such that $fI = gJ$. This holds iff I and J are isomorphic as R-modules. In particular, I is principal if and only if $\mathrm{div}\,(I)$ is 0 in the divisor class group. Hence, R is a UFD if and only if $\mathcal{C}\ell\,(R) = 0$.*

The elements of $\mathcal{C}\ell\,(R)$ are in bijective correspondence with isomorphism classes of pure height one ideals considered as R-modules, and the inverse of the element represented by $\mathrm{div}\,(I)$ is given by $\mathrm{div}\,(J)$, for a pure height one ideal $J \cong \mathrm{Hom}_R(I, R)$. In fact, if $g \in I - \{0\}$, we may take $J = gR :_R I$.

Proof. $I = J$ iff $\operatorname{div}(I) = \operatorname{div}(J)$ because, for pure height one ideals, the associated divisor completely determines the primary decomposition of the ideal. Observe that we have $0 \subseteq fR/fI \subseteq R/fI$ and that the cokernel is isomorphic with R/fR while $fR/fI \cong R/I$. Since $\operatorname{Ass}(R/I)$ contains only height one primes and $\operatorname{Ass}(R/fR)$ contains only height one primes (since R is normal), it follows that $\operatorname{Ass}(R/aI)$ contains only height one primes. The statement that $\operatorname{div}(fI) = \operatorname{div}(f) + \operatorname{div}(I)$ may be checked locally after localizing at each height one prime ideal Q, and is obvious in the case of a discrete valuation ring. In particular, $\operatorname{div}(fg) = \operatorname{div}(f) + \operatorname{div}(g)$ when $f,\, g \in R - \{0\}$. It follows easily that

$$\operatorname{Span}\{\operatorname{div}(f) : f \in R - \{0\}\} = \{\operatorname{div}(g) - \operatorname{div}(f) : f,\, g \in R - \{0\}\}.$$

Thus, if $\operatorname{div}(I) = \operatorname{div}(J)$ in $\mathcal{C}\ell(R)$, then $\operatorname{div}(I) - \operatorname{div}(J) = \operatorname{div}(g) - \operatorname{div}(f)$ and so $\operatorname{div}(fI) = \operatorname{div}(gJ)$ and $fI = gJ$. Then $I \cong fI = gJ \cong J$ as modules. Now suppose $\theta : I \cong J$ as modules (it does not matter whether I, J have pure height one) and let $g \in I - \{0\}$ have image f in J. For all $a \in I$, $g\theta(a) = \theta(ga) = a\theta(g) = af$, and so $\theta(a) = (f/g)a$, and θ is precisely multiplication by f/g. This yields that $(f/g)I = J$ and, hence, $fI = gJ$.

Now fix $I \neq (0)$ and $g \in I - \{0\}$. Any map $I \to R$ is multiplication by a fraction f/g, where f is the image of g in R: thus, $\operatorname{Hom}_R(I,\, R) \cong \{f \in R : (f/g)I \subseteq R\}$, where the homomorphism corresponding to multiplication by f/g is mapped to f. But $(f/g)I \subseteq R$ iff $fI \subseteq gR$, i.e., iff $f \in gR :_R I$. Thus, $\operatorname{Hom}_R(I,\, R) \cong gR :_R I = J$. We claim that J has pure height one (even if I does not) and that if I has pure height one then $\operatorname{div}(J) + \operatorname{div}(I) = \operatorname{div}(g)$, which shows that $\operatorname{div}(J) = -\operatorname{div}(I)$ in $\mathcal{C}\ell(R)$. Let $f_1, \dots, f_k$ generate I. Then we have an exact sequence

$$0 \to gR :_R I \to R \to (R/gR)^{\oplus k}$$

where the map from R sends $r \mapsto (\overline{rf_1}, \dots, \overline{rf_k})$ with the overlines indicating residues modulo gR. It follows that $R/(gR :_R I)$ embeds in $(R/gR)^{\oplus k}$, and so

$$\operatorname{Ass}\big(R/(gR :_R I)\big) \subseteq \operatorname{Ass}\big((R/gR)^{\oplus k}\big) = \operatorname{Ass}(R/gR),$$

which shows that all associated primes of $gR :_R I$ have pure height one. Now localize at any height one prime P to check that $\operatorname{div}(J) + \operatorname{div}(I) = \operatorname{div}(g)$. After localization, if x generates the maximal ideal we have that $I = x^m R$, $g = x^{m+n}R$, where $m,\, n \in \mathbb{N}$, and, since localization commutes with formation of colon ideals, that $J = x^{m+n}R : x^n R$, which is $x^m R$. This is just what we need to show that the coefficients of P in $\operatorname{div}(I)$ and $\operatorname{div}(J)$ sum to the coefficient of P in $\operatorname{div}(g)$.

It remains only to show that every element of $\mathcal{C}\ell(R)$ is represented by $\operatorname{div}(I)$ for some ideal I. But this is clear, since the paragraph above shows that inverses of elements like $[P]$ are represented by divisors of ideals. $\square$

Remarks. A further related result is that a finitely generated torsion-free module M of torsion-free rank one over a Noetherian normal domain R is isomorphic with a pure height one ideal if and only if it is a *reflexive* R-module, i.e, if and only if the natural map $M \to M^{**}$ is an isomorphism, where $\_^*$ indicates $\mathrm{Hom}(\_, R)$, and the natural map sends $u \in M$ to the map $M^* \to R$ whose value on $f \in M^*$ is $f(u)$. In fact, a finitely generated torsion-free module of rank one over a Noetherian domain is always isomorphic to an ideal $I \neq 0$ of R, and if R is normal, I^{**} may be identified with the intersection of the primary components of I corresponding to height one minimal primes of I. (If there are no such minimal primes then I^{**} may be identified with R.) One can define the divisor class group of the Noetherian normal domain R to be the isomorphism classes of rank one reflexive R-modules with multiplication given by $[I][J] = [(I \otimes_R J)^{**}]$. See the Lecture Notes for March 29 and p. 1 for March 31 from Math 615, Winter 2004 for an analysis of the behavior of reflexive modules over a normal Noetherian domain and a proof that the rank one reflexive modules coincide, up to isomorphism, with the ideals of pure height one.

Our next objective is to construct the divisor class group in a different way, using Grothendieck groups. The second point of view gives information that is not readily available directly.

Let R be a Noetherian ring. Let $\mathcal{M}$ denote the set of modules

$$\{R^n/M : n \in \mathbb{N},\, M \subseteq R^n\}.$$

Every finitely generated R-module is isomorphic to one in $\mathcal{M}$, which is all that we really need about $\mathcal{M}$: we can also start with some other set of modules with this property without affecting the Grothendieck group, but we use this one for definiteness.

Consider the free abelian group with basis $\mathcal{M}$, and kill the subgroup generated by all elements of the form $M - M' - M''$ where

$$0 \to M' \to M \to M'' \to 0$$

is a short exact sequence of elements of $\mathcal{M}$. The quotient group is called the *Grothendieck group* $G_0(R)$ of R. It is an abelian group generated by the elements $[M]$, where $[M]$ denotes the image of $M \in \mathcal{M}$ in $G_0(R)$. Note that if $M' \cong M$ we have a short exact sequence

$$0 \to M' \to M \to 0 \to 0,$$

so that $[M] = [M'] + [0] = [M']$, i.e., isomorphic modules represent the same class in $G_0(R)$.

A map L from $\mathcal{M}$ to an abelian group $(A, +)$ is called *additive* if whenever

$$0 \to M' \to M \to M'' \to 0$$

is exact, then $L(M) = L(M') + L(M'')$. The map θ sending M to $[M] \in G_0(R)$ is additive, and is a universal additive map in the following sense: given any additive map $L : \mathcal{M} \to A$, there is a unique homomorphism $h : G_0(M) \to A$ such that $L = h \circ \theta$. Since we need $L(M) = h([M])$, if there is such a map it must be induced by the map from the free abelian group with basis $\mathcal{M}$ to A that sends M to $h(M)$. Since h is additive, the elements $M - M' - M''$ coming from short exact sequences

$$0 \to M' \to M \to M'' \to 0$$

are killed, and so there is an induced map $h : G_0(R) \to A$. This is obviously the only possible choice for h.

Over a field K, every finitely generated module is isomorphic with $K^{\oplus n}$ for some $n \in \mathbb{N}$. It follows that $G_0(K)$ is generated by $\gamma = [K]$, and in fact it is $\mathbb{Z}\gamma$, the free abelian group on one generator. The additive map associated with the Grothendieck group sends M to $\dim_K(M)\gamma$. If we identify $\mathbb{Z}\gamma$ with $\mathbb{Z}$ by sending $\gamma \mapsto 1$, this is the (K-vector space) dimension map.

If R is a domain with fraction field $\mathcal{F}$, we have an additive map to $\mathbb{Z}$ that sends M to $\dim_{\mathcal{F}} \mathcal{F} \otimes_R M$, which is called the *torsion-free rank* of M. This induces a surjective map $G_0(R) \to \mathbb{Z}$. If R is a domain and *if* $\gamma = [R]$ generates $G_0(R)$, then $G_0(R) \cong \mathbb{Z}\gamma \cong \mathbb{Z}$, with the isomorphism given by the torsion-free rank map.

Notice that if L is additive and

$$0 \to M_n \to \cdots \to M_1 \to M_0 \to 0$$

is exact, then

$$L(M_0) - L(M_1) + \cdots + (-1)^n L(M_n) = 0.$$

If $n \leq 2$, this follows from the definition. We use induction. In the general case note that we have a short exact sequence

$$0 \to N \to M_1 \to M_0 \to 0$$

and an exact sequence

$$0 \to M_n \to \cdots \to M_3 \to M_2 \to N \to 0,$$

since

$$\mathrm{Coker}\,(M_3 \to M_2) \cong \mathrm{Ker}\,(M_1 \to M_0) = N.$$

Then

$$(*) \quad L(M_0) - L(M_1) + L(N) = 0,$$

and

$$(**) \quad L(N) - L(M_2) + \cdots + (-1)^{n-1} L(M_n) = 0$$

by the induction hypothesis. Subtracting $(**)$ from $(*)$ yields the result. $\square$

Our proof of unique factorization in arbitrary regular local rings is based on the following two theorems, whose proofs we postpone momentarily.

To state the first of these theorems, observe that we can define a filtration of $G_0(R)$ by letting $\langle G_0(R)\rangle_i$ denote the subgroup spanned by classes of primes P such that height $(P) \geq i$. This filtration decreases as i increases. From it, we obtain an associated graded group: we write

$$[G_0(R)]_i = \langle G_0(R)\rangle_i / \langle G_0(R)\rangle_{i+1}.$$

Theorem (M. P. Murthy). *If R is a normal domain, then $\mathcal{C}\ell\,(R) \cong [G_0(R)]_1$ in such a way that the generator of $\mathcal{C}\ell\,(R)$ corresponding to a height one prime P is mapped to the image of R/P in $[G_0(R)]_1$.*

The second of these theorems is the following, which is a local version of the Hilbert syzygy theorem.

Theorem (Hilbert syzygy theorem for regular local rings). *Let (R, m, K) be a regular local ring of Krull dimension n, and let M be a finitely generated R-module. Then M is free if and only if $\operatorname{depth}(M) = n$. If M is not free and M_1 is any first module of syzygies of M, $\operatorname{depth}(M_1) = \operatorname{depth}(M) + 1$. Hence, M has a finite free resolution by finitely generated free modules, and any shortest such free resolution of M has length $n - \operatorname{depth}(M)$.*

Once we have proved this, we have:

Corollary. *If R is a regular local ring, $G_0(R) = \mathbb{Z}\gamma$, where $\gamma = [R]$, and so for every finitely generated module M, $[M] \in G_0(R)$ is* rank $(M)\gamma$*, where rank indicates torsion-free rank. In particular, if M is a torsion-module, $[M] = 0$, and so $[R/P] = 0$ for every prime ideal P with height $P \geq 1$.*

Proof. R is a domain, and we have the additive map given by torsion-free rank. It will suffice to show that $[R]$ generates $G_0(R)$. But if M is any finitely generated R-module, we know that M has a finite free resolution

$$0 \to R^{b_k} \to \cdots \to R^{b_1} \to R^{b_0} \to M \to 0,$$

and so the element $[M]$ may be expressed as

$$[R^{b_0}] - [R^{b_1}] + \cdots + (-1)^k [R^{b_k}] = b_0\gamma - b_1\gamma + \cdots + (-1)^k b_k\gamma = (b_0 - b_1 + \cdots + (-1)^k b_k)\gamma$$

□

Hence:

Corollary (Auslander-Buchsbaum). *Every regular local ring is a UFD.*

Proof. (M. P. Murthy) The universal additive map is the same as torsion-free rank, so that if $P \neq (0)$, we have that $[R/P] = 0$ in $G_0(R)$. It follows that $\langle G_0(R) \rangle_i = 0$ for all $i \geq 1$, and, hence, $\mathcal{C}\ell\,(R) = [G_0(R)]_1 = 0$. $\square$

It remains to prove the local version of the Hilbert syzygy theorem and Murthy's characterization of the divisor class group.