ANALOGUES OF THE JORDAN–HÖLDER THEOREM FOR TRANSITIVE G-SETS

GREG KUPERBERG, RICHARD LYONS, AND MICHAEL E. ZIEVE

ABSTRACT. Let G be a transitive group of permutations of a finite set Ω, and suppose that some element of G has at most two orbits on Ω. We prove that any two maximal chains of groups between G and a point-stabilizer of G have the same length, and the same sequence of relative indices between consecutive groups (up to permutation). We also deduce the same conclusion when G has a transitive quasi-Hamiltonian subgroup.

1. Introduction

One of the few mistakes in Jordan's classic *Traité des substitutions* is an assertion that would now be called the Jordan–Hölder theorem for transitive G-sets. Specifically, he asserted in [7, §51, p. 38] that, for every subgroup H of a finite group G, the pair (G, H) has the following property:

Definition 1.1. *Let H be a finite-index subgroup of a group G. We say the pair (G, H) has the* Jordan property *when the following holds: if $A_1 \subsetneqq \cdots \subsetneqq A_a$ and $B_1 \subsetneqq \cdots \subsetneqq B_b$ are maximal chains of groups between H and G, then $a = b$ and the sequence $([A_2 : A_1], \ldots, [A_a : A_{a-1}])$ is a permutation of $([B_2 : B_1], \ldots, [B_b : B_{b-1}])$.*

Jordan realized his mistake soon after publication, and retracted his assertion [6]; the smallest counterexample is $(A_4, 1)$, in which $1 < C_2 < V_4 < A_4$ and $1 < C_3 < A_4$ are maximal chains having distinct lengths. A half-century later, Ritt discovered that (G, H) has the Jordan property if $G = HI$ for some finite cyclic subgroup I of G; this was a key ingredient in Ritt's work on functional equations, yielding a fundamental invariant of functional decompositions of a complex polynomial. After another sixty years, Müller showed that (G, H) has the Jordan property if $G = HI$ for some finite abelian subgroup I of G. We will give a simpler proof of Müller's result, while also extending it to a larger class of groups:

Proposition 1.2. *If H is a subgroup of a group G, and $G = HI$ for some finite subgroup I of G such that*

$(*)$ *any two subgroups I_1, I_2 of I are permutable (i.e., $I_1I_2 = I_2I_1$),*

then (G, H) has the Jordan property.

Note that $I_1I_2 = I_2I_1$ if and only if I_1I_2 is a group, or equivalently $\#\langle I_1, I_2\rangle = (\#I_1)[I_2 : I_1 \cap I_2]$. Abelian groups I satisfy $(*)$, as do Hamiltonian groups (i.e., nonabelian groups with no nonnormal subgroups). As shown by Dedekind [3], the finite Hamiltonian groups consist of the direct products of the order-8 quaternion group with an abelian group containing no elements of order 4. There is a similar but less known classification of finite groups satisfying $(*)$ (called quasi-Hamiltonian groups), due to Pic [17].

Our main result says that (G, H) has the Jordan property if some cyclic subgroup I of G has two orbits on the set of cosets of H in G:

The authors thank Peter Neumann for valuable correspondence. The first author was supported by the National Science Foundation under Grant No. 0606795.

Theorem 1.3. *Let H be a subgroup of a group G, and let I be a finite cyclic subgroup of G such that $G = IH \cup IgH$ for some $g \in G$. Then (G, H) has the Jordan property.*

By means of a now-standard inductive argument due to Netto (cf. Lemma 2.1), this result is a consequence of the following:

Theorem 1.4. *Let G be a transitive group of permutations of a finite set Ω, fix $\omega \in \Omega$, and suppose some element of G has at most two cycles on Ω. If A and B are distinct maximal subgroups of G for which $H := A \cap B$ contains G_ω, then one of the following holds:*

(1.4.1) *H is a maximal subgroup of both A and B, and $G = AB$; or*

(1.4.2) *$G/\operatorname{core}_G(H)$ is dihedral of order $2r$, with r prime, and both A and B have order 2 images in $G/\operatorname{core}_G(H)$.*

Here, as usual, $\operatorname{core}_G(H)$ is the maximal normal subgroup of G contained in H. Possibility (1.4.2) illustrates a phenomenon not arising in Proposition 1.2: if G contains a transitive quasi-Hamiltonian subgroup, then (1.4.1) holds.

We will give examples showing that Assertion 1.1 need not hold for transitive groups G containing an element with three cycles, and likewise for transitive groups G containing an abelian subgroup with two orbits. However, in some sense the counterexamples in both situations appear to be bounded, so it may be possible to classify the counterexamples to Theorem 1.4 in these more general situations.

Our work was motivated by geometric applications. Specifically, Theorem 1.3 has the following consequence:

Corollary 1.5. *Let C and D be smooth, projective, geometrically irreducible curves over a field K, and let $f : C \to D$ be a nonconstant separable rational map defined over K. Suppose that some place of D is tamely ramified in f, and lies under at most two places of C. Let $C \to A_1 \to A_2 \to \cdots \to D$ and $C \to B_1 \to B_2 \to \cdots \to D$ be maximal decompositions of f into rational maps of degree more than 1. Then these decompositions have the same length, and (up to permutation) the same sequence of degrees of the involved indecomposable maps.*

The simplest case $C = D = \mathbb{P}^1$ is already interesting: there f is essentially a Laurent polynomial.

Corollary 1.6. *Let $f \in K[x, x^{-1}]$ be a Laurent polynomial over a field K, and assume that neither $x = 0$ nor $x = \infty$ is a pole of f of order divisible by $\operatorname{char}(K)$. Write $f = a_1 \circ \cdots \circ a_r = b_1 \circ \cdots \circ b_s$ where $a_i, b_j \in K(x)$ are indecomposable and have degree more than 1. Then $r = s$, and the sequence $(\deg(a_1), \ldots, \deg(a_r))$ is a permutation of $(\deg(b_1), \ldots, \deg(b_s))$.*

In case $K = \mathbb{C}$, this result was proved in the recent paper [20]; subsequently another proof was given in [15]. Conversely, the $K = \mathbb{C}$ case of Corollary 1.6 is equivalent to some special cases of Theorem 1.3, in view of Riemann's existence theorem and knowledge of the fundamental group of the punctured sphere. Specifically, the $K = \mathbb{C}$ case of Corollary 1.6 is equivalent to Theorem 1.3 for groups G having generators $g_1, \ldots, g_k$ such that $g_1 g_2 \ldots g_k = 1$ and, in the action of G on the set Ω of left cosets of H in G, we have $2\#\Omega - 2 = \sum_i (\#\Omega - \#\operatorname{cycles}(g_i))$ and $\#\operatorname{cycles}(g_1) = 2$.

The proofs in [20] and [15] relied on various algebro-geometric calculations, which were much more complicated than the proof in the present paper. On the other hand, in case $K = \mathbb{C}$, those papers obtained quite precise information about the shape of the indecomposable rational functions a_i and b_j occurring in Corollary 1.6. This precise information relies on the fact that C and D have genus zero, so it is not surprising that geometry is required for the proof. However, since Corollary 1.6 has a group-theoretic interpretation, this result seemed to merit a group-theoretic proof, which we produce in the present paper. As a bonus, this group-theoretic proof implies Corollary 1.6 even for fields of positive characteristic, and also implies Corollary 1.5; essentially, the group-theoretic proof uses just the ramification behavior at one special point, whereas the geometric proofs used the ramification behavior at all points, hence required stronger hypotheses.

Ritt proved Corollary 1.6 in case $K = \mathbb{C}$ and f is a polynomial [18]. He also determined the possibilities for the a_i's and b_j's, and his results have been applied to a wide range of topics (cf. [1, 2, 4, 5, 10, 13, 14, 16, 19], among others). Here we mention just the most recent application, from [5]:

Theorem 1.7 (Ghioca–Tucker–Zieve)**.** *Let $x_0, y_0 \in \mathbb{C}$ and $f, g \in \mathbb{C}[x]$ satisfy $\deg(f), \deg(g) \neq 1$. If the orbits*

$$\{x_0, f(x_0), f(f(x_0)), \dots\} \quad \textit{and} \quad \{y_0, g(y_0), g(g(y_0)), \dots\}$$

have infinite intersection, then f and g have a common iterate.

It would be of great interest to extend this result to Laurent polynomials or more general rational functions. We suspect the group theoretic perspective of the present paper may be useful in this endeavor.

We now summarize the contents of this paper. In the next section we present a version of the diamond lemma, which we use in Section 3 to prove Proposition 1.2. In Section 4 we record the terminology of G-sets needed for the proofs of our main results, and in Section 3 we prove Theorems 1.3 and 1.4. We conclude in the final section with some examples and speculations.

2. Diamond lemma

In order to prove that a pair of groups has the Jordan property, it suffices to consider pairs of chains whose common least element is the intersection of their two second-largest elements. This generalizes an argument due to Netto [11].

Lemma 2.1. *Let $\mathcal{C}$ be a set of pairs (G, H) of a group G and a finite-index subgroup H, and suppose that if $(G, H) \in \mathcal{C}$ and $H < G_0 < G$ then $\mathcal{C}$ contains both (G_0, H) and (G, G_0). Suppose further that, if $(G, H) \in \mathcal{C}$ and A, B are distinct maximal subgroups of G with $H = A \cap B$, then there exist maximal chains of groups $G > A > \cdots > H$ and $G > B > \cdots > H$ such that the sequences of indices in the two chains are the same up to permutation. It follows that every pair in $\mathcal{C}$ has the Jordan property.*

Proof. Pick $(G, H) \in \mathcal{C}$ with $[G : H] = d$, and suppose the result holds for pairs with smaller index. Let $A_0 < A_1 < \cdots < A_r$ and $B_0 < \cdots < B_s$ be maximal chains of groups between H and G. Then $A_r = B_s = G$, and A_{r-1} and B_{s-1} are maximal subgroups of G. If $A_{r-1} = B_{s-1}$ then the result follows from the corresponding result for (A_{r-1}, H). So assume $A_{r-1} \neq B_{s-1}$, and let $K = A_{r-1} \cap B_{s-1}$. The hypothesis for the case (G, K) is that there are maximal chains $G > A_{r-1} > \cdots > K$ and $G > B_{s-1} > \cdots > K$ for which the sequences of indices are the same up to permutation. Pick a maximal chain $K > \cdots > H$, and concatenate with the previous chains to get maximal chains $G > A_{r-1} > \cdots > H$ and $G > B_{s-1} > \cdots > H$ with the same multiset of indices. The result for (A_{r-1}, H) implies that the multiset of indices for the first chain equals that for the A_i chain. The result for (B_{s-1}, H) implies that the multiset for the second chain equals that for the B_j chain. Thus, the A_i chain has the same multiset of indices as does the B_j chain. □

3. Groups with a transitive quasi-Hamiltonian subgroup

In this section we prove Proposition 1.2. In light of Lemma 2.1, it suffices to prove the following:

Proposition 3.1. *Let H be a subgroup of a group G, and suppose that $G = HI$ for some finite subgroup I of G satisfying $(*)$. If A, B are distinct maximal subgroups of G with $A \cap B = H$, then H is maximal in both A and B, and $G = AB$.*

We begin with a general lemma on subgroups of groups of this form.

Lemma 3.2. *Let H and I be subgroups of a group G such that $G = HI$. Then $W \mapsto W \cap I$ is an injective map from the set of groups between G and H to the set of groups between I and $I \cap H$. This map preserves indices between pairs of groups, and its image is closed under intersections and joins (where the join of two groups is the group they generate).*

Proof. Let W be a group between H and G, so W is a union of cosets of H, and each such coset contains an element of I, whence $W = H(W \cap I)$. Thus $[W : H] = [W \cap I : H \cap I]$. If A, B are groups between H and G, write $A = HC$ and $B = HD$ with $C = I \cap A$ and $D = I \cap B$. Then $A \cap B = HE$ with

$$E = I \cap (A \cap B) = (I \cap A) \cap (I \cap B) = C \cap D.$$

Also $H\langle C, D\rangle = \langle C, D\rangle H$, and hence equals $\langle HC, HD\rangle$. □

In view of Lemma 3.2, Proposition 3.1 is a consequence of the following result:

Lemma 3.3. *Let I be a finite group satisfying $(*)$, let H be a subgroup of I, and let $\mathcal{I}$ be a set of groups between H and I which includes both H and I, and which is closed under intersections and joins. If A, B are maximal subgroups of I with $A \cap B = H$, then H is maximal in both A and B, and $I = AB$.*

Proof. Let A, B be distinct maximal elements of $\mathcal{I} \setminus \{I\}$. Then $I = AB$, so $[I : B] = [A : A \cap B]$. Also if $J \in \mathcal{I}$ is strictly between $A \cap B$ and A, then $[BJ : B] = [J : A \cap B]$ so BJ is strictly between B and I, contradicting maximality. Therefore both chains $A \cap B < A < I$ and $A \cap B < B < I$ are maximal in $\mathcal{I}$. □

This completes the proof of Proposition 3.1, and so of Proposition 1.2.

Remark. Müller's proof of Proposition 1.2 in the case of abelian groups I is substantially more complicated than the one given above.

4. G-sets

In this section we record some notation and terminology involving G-sets. For standard notions of G-sets, we refer to [12], which we follow when possible; below we give the details of some notions that are not universally used.

Given a group G, by a G-set we mean a nonempty set Ω together with a homomorphism $\rho : G \to \mathrm{Sym}(\Omega)$. For $g \in G$ and $\omega \in \Omega$, we write ω^g for $(\rho(g))(\omega)$. An equivalence relation ϕ on the G-set Ω is said to be G-invariant if

$$\alpha \equiv \beta \pmod{\phi} \Rightarrow \alpha^g \equiv \beta^g \pmod{\phi} \quad \text{for every } g \in G.$$

Such an equivalence relation is called a *congruence* on Ω. If ϕ is a congruence on Ω, then the action of G on Ω naturally induces an action of G on the set Ω/ϕ of ϕ-equivalence classes on Ω; the G-set Ω/ϕ is called the quotient of the G-set Ω by the congruence ϕ. The notions of transitive G-sets, homomorphisms of G-sets, isomorphisms of G-sets, and direct products of G-sets are defined in the usual manner.

Let ϕ and ψ be two congruences on a G-set Ω. We say that ϕ coarsens ψ (or equivalently, ψ refines ϕ) if every ϕ-equivalence class is a union of ψ-equivalence classes. We denote the coarsest common refinement of ϕ and ψ by $\phi \wedge \psi$; thus, each $\phi \wedge \psi$-equivalence class is the intersection of a ϕ-equivalence class and a ψ-equivalence class. We denote the finest common coarsening of ϕ and ψ by $\phi \vee \psi$; each $\phi \vee \psi$-equivalence class is a union of ϕ-equivalence classes, and also a union of ψ-equivalence classes. We write ϕ^ψ for the coarsening of ϕ in which two ϕ-equivalence classes are ϕ^ψ-equivalent if they nontrivially intersect the same ψ-equivalence classes. We emphasize that $\phi \wedge \psi$, $\phi \vee \psi$, and ϕ^ψ are congruences on Ω.

Any G-set Ω comes equipped with two trivial congruences: the *trivial coarse congruence*, in which Ω is itself an equivalence class; and the *trivial fine congruence*, in which every equivalence class contains a single element. Any congruence besides these two is said to be *nontrivial.* We usually identify Ω with its trivial coarse congruence. We say a transitive G-set Ω is *primitive* if it admits no nontrivial congruences.

Let ϕ and ψ be congruences on a transitive G-set Ω. Then Ω/ϕ and Ω/ψ are transitive, so any two ψ-equivalence classes have the same size, and likewise for any two ϕ-equivalence classes. If ϕ coarsens ψ, then every ϕ-equivalence class consists of the same number k of ψ-equivalence classes; we call k the *index* of ψ in ϕ, and denote this by $[\phi : \psi]$.

The following lemma is routine.

Lemma 4.1. *Let Ω be a transitive G-set, and pick $\omega \in \Omega$. Define a map θ from the set of congruences on Ω to the set of groups between G and G_ω as follows: let $\theta(\phi)$ be the stabilizer of the image of ω in the G-set Ω/ϕ. Then*

- *θ is a bijection;*
- *ϕ coarsens ψ if and only if $\theta(\psi)$ is a subgroup of $\theta(\phi)$; and*
- *if ϕ coarsens ψ then $[\phi : \psi] = [\theta(\phi) : \theta(\psi)]$.*

Note that the final two assertions say that θ is order-preserving and index-preserving.

Finally, we remark that the proof in the previous section can be translated to the language of G-sets. Specifically, let I be a finite quasi-Hamiltonian subgroup of a group G, and let A and B be distinct maximal subgroups of G for which $H := A \cap B$ satisfies $G = HI$. Let Ω be the G-set of left cosets of H in G, and let ϕ and ψ be the congruences on Ω corresponding (via Lemma 4.1) to A and B. Then, for $I_1, I_2 \leq I$, the property $I_1I_2 = I_2I_1$ can be restated as the condition that $\phi \vee \psi$ should be the full coset space I/I_1I_2. Thus, the proof in the previous section can be stated either in terms of groups or congruences, with little conceptual difference. On the other hand, in the next section we will find the congruence viewpoint to be more suitable for the problem at hand.

5. Transitive groups with an element having at most two cycles

In this section we prove Theorem 1.4; by Lemma 2.1, this implies Theorem 1.3.

Given a group G and a finite-index subgroup H, let Ω be the transitive G-set of left cosets of H in G. Suppose $g \in G$ has at most two orbits (= cycles) on Ω. Let ϕ and ψ be nontrivial congruences on Ω. Suppose further that ϕ and ψ have no nontrivial common refinement, so any ϕ-equivalence class intersects any ψ-equivalence class in at most one element – thus Ω embeds (as a G-set) into $\Omega/\phi \times \Omega/\psi$. Suppose also that ϕ and ψ have no nontrivial common coarsening. *We maintain the above notation throughout this section.*

By Lemmas 2.1 and 4.1, to prove Theorem 1.4 it suffices to show: if Ω/ϕ and Ω/ψ are primitive, then either $G/\operatorname{core}_G(H)$ is dihedral or $\Omega = \Omega/\phi \times \Omega/\psi$ where both ϕ and ψ are maximally fine nontrivial congruences. It will be convenient to do some arguments without assuming primitivity.

We begin by observing how g-cyles on Ω relate to g-cycles on Ω/ϕ and Ω/ψ.

Lemma 5.1. *Pick $\omega \in \Omega$, and suppose the image ω_ϕ of ω in Ω/ϕ lies in a g-cycle of length a, and the image ω_ψ of ω in Ω/ψ lies in a g-cycle of length b. Then ω lies in a g-cycle of length* $\operatorname{lcm}(a, b)$. *The $g^{\gcd(a,b)}$-orbit of ω is a union of ϕ-equivalence classes, and also is a union of ψ-equivalence classes. The congruence ϕ^ψ nontrivially coarsens ϕ unless either $a = b$ or* $\gcd(a, b) = 1$.

Proof. Plainly g^r fixes ω_ϕ precisely when $a \mid r$, and g^r fixed ω_ψ precisely when $b \mid r$. Since g^r fixes ω if and only if g^r fixes both ω_ϕ and ω_ψ, it follows that ω is in a g-cycle of length $\operatorname{lcm}(a, b)$. The ϕ-equivalence classes on Ω/ϕ are precisely the g^a-cycles; the ψ-equivalence classes are likewise the g^b-cycles. Hence the $g^{\gcd(a,b)}$-orbit of ω is a union of ϕ-equivalence classes, and also a union of ψ-equivalence classes. Finally, the ϕ-equivalence class $\langle g^a\rangle g^i\omega_\phi$ nontrivially intersects just the ψ-equivalence classes $\langle g^b\rangle g^{ar+i}\omega_\psi$, or in other words the classes containing elements of the form $g^{\gcd(a,b)s+i}\omega_\psi$. Thus, two ϕ-classes $\langle g^a\rangle g^{i\omega_\phi}$ and $\langle g^a\rangle g^{j\omega_\phi}$ become equivalent in ϕ^ψ if and only if

$i \equiv j \pmod{\gcd(a,b)}$. Here ϕ^ψ is the trivial coarse partition if $\gcd(a,b) = 1$, and $\phi^\psi = \phi$ if $a \mid b$; in all other situations, ϕ^ψ is a nontrivial coarsening of ϕ. $\square$

We split the proof of Theorem 1.4 into several cases. In the first case we illustrate our method by using it to prove Ritt's result (which is needed to verify the 'closure' hypothesis in Lemma 2.1).

Case 1. *If g has a single cycle on Ω, and both Ω/ϕ and Ω/ψ are primitive, then $\Omega = \Omega/\phi \times \Omega/\psi$ and both ϕ and ψ are maximally fine nontrivial congruences.*

Proof. Let a and b be the lengths of the cycles of g on Ω/ϕ and Ω/ψ, respectively. Since ϕ and ψ have no nontrivial common coarsening, $\phi \vee \psi$ is trivial, so Lemma 5.1 implies $\gcd(a,b) = 1$. Thus $\Omega = \Omega/\phi \times \Omega/\psi$. If the congruence μ nontrivially refines ψ, then $\Omega \neq \Omega/\phi \times \Omega/\mu$, so μ must not satisfy the same hypotheses as ψ; hence ϕ and μ have a nontrivial common coarsening. This is not possible if Ω/ϕ is primitive. $\square$

Case 2. *If g has two cycles on both Ω/ϕ and Ω/ψ, then $\phi \vee \psi$ is nontrivial.*

Proof. Let ϕ' be the equivalence relation on Ω whose two equivalence classes are the unions of the ϕ-equivalence classes comprising the two cycles of g on Ω/ϕ. Then g acts trivially on Ω/ϕ'. Since g has two cycles on Ω, and each cycle is contained in a ϕ'-equivalence class, the ϕ'-equivalence classes are precisely the g-cycles on Ω. Since the same holds for ψ', it follows that $\phi' = \psi'$ is a nontrivial common coarsening of ϕ and ψ, so $\phi \vee \psi$ is nontrivial. $\square$

Case 3. *Suppose the g-cycles on Ω/ϕ have lengths a_1 and a_2, and Ω/ψ is a g-cycle of length b. Then $\Omega = \Omega/\phi \times \Omega/\psi$, and if Ω/ϕ and Ω/ψ are primitive then both ϕ and ψ are maximally fine nontrivial congruences.*

Proof. By Lemma 5.1, the g-cycles on Ω have lengths $\operatorname{lcm}(a_1, b)$ and $\operatorname{lcm}(a_2, b)$, and consist of a_1 and a_2 ϕ-equivalence classes; since G is transitive on Ω/ϕ, every such equivalence class has the same size, so $\operatorname{lcm}(a_1, b)/a_1 = \operatorname{lcm}(a_2, b)/a_2$ and thus $\gcd(a_1, b) = \gcd(a_2, b)$. Since $\phi \vee \psi$ is nontrivial, Lemma 5.1 implies $\gcd(a_1, b) = 1$, so $\Omega = \Omega/\phi \times \Omega/\psi$.

Let μ be a nontrivial congruence refining ψ; if $\phi \vee \mu$ is nontrivial, then primitivity of Ω/ϕ implies $\phi \vee \mu = \phi$, so μ is a nontrivial common refinement of ϕ and ψ, contradiction. Thus $\phi \vee \mu$ is trivial, so from Case 2 we know that g acts cyclically on Ω/μ. Then the previous paragraph implies $\Omega = \Omega/\phi \times \Omega/\mu$, so $\mu = \psi$. The same argument shows that ϕ is also a maximally fine nontrivial congruence. $\square$

Case 4. *Suppose g is an a-cycle on Ω/ϕ and a b-cycle on Ω/ψ, but g has two cycles on Ω. Then either $\gcd(a,b) > 2$, or both $\gcd(a,b) = 2$ and $\Omega = \Omega/\phi \times \Omega/\psi$.*

Proof. By Lemma 5.1, each g-cycle on Ω has length $\operatorname{lcm}(a,b)$. Since Ω embeds in the G-set $\Omega/\phi \times \Omega/\psi$, which has cardinality ab, it follows that $\gcd(a,b) \geq 2$, with equality if and only if $\Omega = \Omega/\phi \times \Omega/\psi$. $\square$

Henceforth suppose the situation of Case 4 holds, and suppose also that Ω/ϕ and Ω/ψ are primitive.

Case 4a. *If $\gcd(a,b) > 2$ then $G/\operatorname{core}_G(H)$ is dihedral of order twice a prime, and the trivial fine congruence has index 2 in both ϕ and ψ.*

Proof. By Lemma 5.1, ϕ^ψ is nontrivial unless $a \mid b$, and likewise ψ^ϕ is nontrivial unless $b \mid a$. Thus, primitivity implies $a = b$. View Ω as the edges of a bipartite graph Γ whose vertices are Ω/ϕ and Ω/ψ. By the previous inference, Γ is 2-regular. The classes of $\phi \vee \psi$ correspond to the connected components of Γ; so if Ω/ψ is primitive, Γ is connected. Thus Γ is a cycle of length $2a$. Now $G/\operatorname{core}_G(H) \subseteq \operatorname{Aut}(\Gamma)$, where here we only consider the automorphisms that preserve Γ as a *bipartite* graph. But $\operatorname{Aut}(\Gamma) \cong D_a$, and D_a acts freely transitively on Ω. Because $G/\operatorname{core}_G(H)$ acts transitively, it is also isomorphic to D_a. Since Ω/ϕ is primitive, a is prime. $\square$

Case 4b. *If* $\gcd(a, b) = 2$ *and* $\Omega = \Omega/\phi \times \Omega/\psi$*, then both* ϕ *and* ψ *are maximally fine nontrivial congruences.*

Proof. Suppose not, and let $\mu \neq \psi$ be a nontrivial congruence refining ψ. If g has two cycles on Ω/μ then Case 3 provides a contradiction. Thus, g acts as a c-cycle on Ω/μ. Lemma 5.1 implies $a \mid c$. Since μ refines ψ, we also have $b \mid c$. Thus c is divisible by $\operatorname{lcm}(a, b) = ab/2$, and c divides $\#\Omega = ab$. Since μ is nontrivial, we have $c \neq ab$, so $c = ab/2$, and thus each μ-equivalence class has size 2. Finally, $\mu^\phi \vee \psi$ has precisely two equivalence classes (and so is nontrivial) unless $b = 2$ and $c = a$. But if $a = c$ then, as above, $G/\operatorname{core}_G(H)$ is dihedral. However, this cannot happen here, because a is not prime. □

Remark. We stated the diamond lemma (Lemma 2.1) in terms of descending chains of groups (with A and B maximal subgroups of G which meet in H); there is an analogous result in terms of ascending chains (with A and B minimal overgroups of H in G which generate G). However, we do not see how to do the proof this way, since we do not know how to make a congruence that behaves with regard to refining in the same way that ϕ^ψ behaves for coarsening.

6. Data and speculations

Theorem 1.3 is not true if we allow I to be an abelian group with two orbits (on the G-set Ω of left cosets of H in G). For instance, let G be the group of permutations of $\mathbb{F}_9$ of the form $x \mapsto \alpha x + \beta$ with $\beta \in \mathbb{F}_9$ and $\alpha^4 = 1$. Let A and B be the subgroups $\{\pm x + \beta : \beta \in \mathbb{F}_9\}$ and $\{x \mapsto \alpha x : \alpha^4 = 1\}$. Then two maximal chains of groups between $H := \{\pm x\}$ and G are $H < B < G$ and $H < \{\pm x + \beta : \beta \in \mathbb{F}_3\} < A < G$, which have different lengths. However, the abelian group $\{x + \beta : \beta \in \mathbb{F}_9\}$ has two orbits on Ω.

There are also counterexamples to Theorem 1.3 if we allow I to be a cyclic group with three orbits on Ω. For instance, let H be an order-2 subgroup of S_4 which is not contained in A_4; then any cyclic subgroup of order 4 has three cycles on Ω, but two maximal chains of groups between H and G are $H < S_3 < S_4$ and $H < V_4 < D_8 < S_4$.

However, computer searches on small groups suggest there are extremely few examples in these situations. In fact, it may be that there are only finitely many finite groups G containing a core-free subgroup H such that (G, H) does not have the Jordan property, but G contains an element having precisely three cycles on the coset space Ω. As yet we have not been able to extend the methods of this paper to analyze such a situation.

References

[1] R. M. Beals, J. L. Wetherell and M. E. Zieve, *Polynomials with a common composite*, submitted for publication. arXiv:0707.1552 [math.AG]

[2] Y. F. Bilu and R. F. Tichy, *The Diophantine equation* $f(x) = g(y)$, Acta Arith. **95** (2000), 261–288.

[3] R. Dedekind, *Ueber Gruppen, deren sämmtliche Theiler Normaltheiler sind*, Math. Ann. **48** (1897), 548–561.

[4] D. Ghioca, T. J. Tucker and M. E. Zieve, *Intersections of polynomial orbits, and a dynamical Mordell-Lang conjecture*, Invent. Math., to appear. arXiv:0705.1954 [math.NT]

[5] D. Ghioca, T. J. Tucker and M. E. Zieve, *Linear relations between polynomial orbits*, in preparation.

[6] C. Jordan, *Note sur la théorie des substitutions*, Giorn. di mat. **X** (1872), 116. (= Œuvres, v. I, no. 55, p. 362)

[7] C. Jordan, Traité des substitutions et des équations algébriques, Gauthier-Villars, Paris, 1870.

[8] P. Müller, *Primitive monodromy groups of polynomials*, in: Recent Developments in the Inverse Galois Problem 385–401, Amer. Math. Soc., Providence, RI, 1995.

[9] P. Müller and M. E. Zieve, *On Ritt's decomposition theorems for polynomials*, in preparation.

[10] M. Muzychuk and F. Pakovich, *Solution of the polynomial moment problem*, submitted for publication. arXiv:0710.4085 [math.CV]

[11] E. Netto, *Zur Theorie der zusammengesetzten Gruppen*, J. reine angew. Math. **78** (1874), 81–92.

[12] P. M. Neumann, G. A. Stoy, and E. C. Thompson, Groups and Geometry, Oxford University Press, Oxford, 1994.

[13] F. Pakovich, *On polynomials sharing preimages of compact sets, and related questions*, Geom. Funct. Anal., to appear. arXiv:math/0603452 [math.DS]

[14] F. Pakovich, *On the functional equation $F(A(z)) = G(B(z))$, where A, B are polynomials and F, G are continuous functions*, Math. Proc. Cambridge Philos. Soc., to appear. arXiv:math/0605016 [math.CV]
[15] F. Pakovich, *Prime and composite Laurent polynomials*, submitted for publication. arXiv:0710.3860 [math.CV]
[16] F. Pakovich, N. Roytvarf and Y. Yomdin, *Cauchy-type integrals of algebraic functions*, Israel J. Math. **144** (2004), 221–291. arXiv:math/0312353 [math.CA]
[17] G. Pic, *On the structure of quasi-Hamiltonian groups*, Acad. Repub. Pop. Române. Bul. Ştti. A. **1** (1949), 973–979.
[18] J. F. Ritt, *Prime and composite polynomials*, Trans. Amer. Math. Soc. **23** (1922), 51–66.
[19] U. Zannier, *On a functional equation relating a Laurent series $f(x)$ to $f(x^m)$*, Aequat. Math. **55** (1998), 15–43.
[20] M. E. Zieve, *Decompositions of Laurent polynomials*, submitted for publication. arXiv:0710.1902 [math.NT]

Department of Mathematics, University of California, Davis, CA 95616
E-mail address: greg@math.ucdavis.edu
URL: www.math.ucdavis.edu/~greg/

Department of Mathematics, Rutgers University, 110 Frelinghuysen Road, Piscataway, NJ 08854
E-mail address: lyons@math.rutgers.edu

Department of Mathematics, University of Michigan, 530 Church Street, Ann Arbor, MI 48109-1043
E-mail address: zieve@umich.edu
URL: www.math.lsa.umich.edu/~zieve/