INVARIANT MAXIMAL IDEALS IN GROUP ALGEBRAS

DANIEL R. FARKAS

ABSTRACT. Given a finitely generated torsion free abelian group A , any group of automorphisms of A extends to a group of algebra automorphisms of the group ring $\mathbb{F}_p[A]$. When the automorphism group is cyclic, Roseblade has proved that $\mathbb{F}_p[A]$ has infinitely many invariant maximal ideals. We count these ideals with a localized generating function which turns out to be rational.

In his famous paper solving Philip Hall's residual finiteness problem [2], Roseblade presents a technical lemma in which he proves that there are infinitely many invariant maximal ideals in a certain group algebra. The purpose of this paper is to count these ideals by a generating function which, I hope, is rational.

Assume that A is a finitely generated free abelian group and have $\mathbb{F}_p$ denote the finite field of p elements (p a prime). Any subgroup $G \subseteq \text{GL}(A)$ extends to a group of algebra automorphisms of $\mathbb{F}_p[A]$, the group algebra. We wish to encode the G -stable maximal ideals of $\mathbb{F}_p[A]$. For example, Roseblade finds a way to count such ideals when G is cyclic, thereby proving that their number is infinite.

In [1] I discuss an equivariant version of Weil's zeta function and explain why it might not be a good choice for a generating function in this context. I also propose an alternative which will be briefly reviewed.

Let $\bar{\mathbb{F}}_p$ be the algebraic closure of $\mathbb{F}_p$. Each maximal ideal of $\bar{\mathbb{F}}_p[A]$ corresponds to a character from A to $\bar{\mathbb{F}}_p^*$ by the Nullstellensatz and, as such, has finite order as a member of the character group. A maximal ideal of $\mathbb{F}_p[A]$ is contained in finitely many maximal ideals of $\bar{\mathbb{F}}_p[A]$; we can then speak of characters "lying over" a maximal ideal of $\mathbb{F}_p[A]$. Let $(\text{CH}(A)/\mathcal{F})^G$ consist of those characters which lie over G -stable maximal ideals of $\mathbb{F}_p[A]$. In order to count these characters, we must index them in an appropriate way. As indicated in [1], the order of a character gives the best layering. Now the cardinality of the collection of characters in $(\text{CH}(A)/\mathcal{F})^G$ with a given order is an arithmetic function of that order. Number theorists frequently "localize" such functions at a fixed prime q and construct the corresponding "Bell series." In our context that means that for each $q \neq p$ we let $\gamma_p(q; f)$ be the cardinality of $\{\chi \in (\text{CH}(A)/\mathcal{F})^G \mid \chi \text{ has order } q^f\}$. Let

$$\Gamma_p(q; T) = \sum_{f=0}^{\infty} \gamma_p(q; T) T^f$$

Received by the editors April 29, 1985 and, in revised form, July 26, 1985.

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 16A27, 11C20, 15A33.

Key words and phrases. Group algebra, characters, matrices over a finite ring.

¹This research was partially supported by a grant from NSF.

©1986 American Mathematical Society
0002-9939/86 \$1.00 + \$.25 per page

be the generating function. Although these local counting functions depend on the parameter q , it will turn out that q appears in a virtually universal manner.

DEFINITION. Assume that Ξ is a set of parameters lying in $\mathbf{Q}$ and that $H(\xi; T) \in \mathbf{Q}(T)$ for each $\xi \in \Xi$. We say that the family of functions $\{H(\xi; T)\}$ is *almost formally independent of ξ* if there are finitely many rational functions in two variables $F_1(Y, T), \dots, F_h(Y, T) \in \mathbf{Q}(Y, T)$ such that for each $\xi \in \Xi$ there is a j with $H(\xi; T) - F_j(\xi, T)$ a polynomial in T .

Notice that when $H(\xi; T)$ and $F_j(\xi, T)$ have power expansions in T , their difference is a polynomial if and only if they agree after finitely many terms.

The justification for all of this notation lies in the empirical discovery that these local generating functions are well behaved.

RATIONALITY CONJECTURE. Suppose that A is a finitely generated free abelian group and $G \subseteq \mathrm{GL}(A)$. Then:

- (i) $\Gamma_p(q; T)$ is a rational function of T for all primes $q \neq p$.
- (ii) The functions $\Gamma_p(q; T)$ are almost formally independent of q .

This paper provides evidence of the truth of the conjecture. We prove a single result.

THEOREM. Assume that $G \subseteq \mathrm{GL}(A)$ is a cyclic group. Then for all but (possibly) finitely many primes $q \neq p$, $\Gamma_p(q; T)$ is rational and almost formally independent of q .

The proof is broken into three parts. First, we remove all references to group algebras and characters. Next we use the theory of rational canonical forms to reduce the possible cyclic groups G which must be considered, to those with a generator of a specific "primary" type. Finally, in the third section, we make detailed arithmetic calculations of $\Gamma_p(q; T)$ for the special case.

1. An equivalent formulation. We owe the reader an explanation of the notation $(\mathrm{CH}(A)/\mathcal{F})^G$. Fix a basis $x_1, \dots, x_n$ for the free abelian group A . A character χ can be identified with a point in affine n -space over $\mathbf{F}_p$, $\chi \leftrightarrow (\chi(x_1), \dots, \chi(x_n))$, with $\chi(x_j) \neq 0$ for $j = 1, \dots, n$. Conversely, every n -tuple with entries in $\mathbf{F}_p^*$ determines a unique character. It is well known that a finite set of such points corresponds to maximal ideals lying over a maximal ideal of $\mathbf{F}_p[A]$ if and only if these points constitute an orbit under the action of $\mathrm{Gal}(\bar{\mathbf{F}}_p | \mathbf{F}_p)$. So let $\mathcal{F}$ denote the Frobenius acting on characters: $\mathcal{F}(\chi) = \chi^p$. Then $\chi_1, \dots, \chi_w$ lie over a maximal ideal of $\mathbf{F}_p[A]$ precisely when there is a nonnegative integer $m = m(i, j)$ such that

$$\chi_i = \mathcal{F}^m(\chi_j) \quad \text{for all } i \text{ and } j.$$

Suppose G is an arbitrary group of automorphisms of A . Then G acts on characters via

$${}^g\chi(a) = \chi(g^{-1} \cdot a) \quad (g \in G, a \in A).$$

(See [1, §4].) The characters which lie over a G -stable maximal ideal of $\mathbf{F}_p[A]$ comprise an orbit of characters under the action of $\mathcal{F}$ which is fixed by G , whence the symbols $(\mathrm{CH}(A)/\mathcal{F})^G$. In detail, $\chi \in (\mathrm{CH}(A)/\mathcal{F})^G$ provided for each $g \in G$ there is an $e(g) \geq 0$ with ${}^g\chi = \mathcal{F}^{e(g)}(\chi)$.

For each positive integer d relatively prime to p there is a unique subgroup of order d in $\bar{\mathbf{F}}_p^*$. A character χ of order d can be regarded as a homomorphism $\chi: A \rightarrow (\mathbf{Z}/(d), +)$. As above we may fix a basis of n elements for A and identify χ with a vector in $(\mathbf{Z}/(d))^n$ which is unimodular. (This means that the coordinates generate all of $\mathbf{Z}/(d)$ as an ideal.) Since we are particularly interested in $d = q^f$ for a prime $q \neq p$, we will write $\text{UNIM}_n(f)$ for the collection of unimodular vectors in this case.

We have a dictionary. If χ corresponds to $v \in (\mathbf{Z}/(d))^n$, then $\mathcal{F}(\chi)$ corresponds to pv . For $g \in \text{GL}(A) = \text{GL}(n, \mathbf{Z})$ it is not difficult to show that ${}^g\chi$ corresponds to $(g^{-1})^T(v)$ (cf. [1, §4]). (By the way, we use a convention here that will save us some cluttered notation. If M is a matrix with rational entries whose denominators are relatively prime to d then M will also be used for its own image as a matrix over $\mathbf{Z}/(d)$.) We translate the basic terminology.

LEMMA 1. $\gamma_p(q; f)$ is the cardinality of the set of $v \in \text{UNIM}_n(f)$ such that for each $g \in G$ there is an $e(g) \geq 0$ with $(g^T - p^{e(g)})v \equiv 0 \pmod{q^f}$. $\square$

2. Linear algebra: reductions. We shall now restrict attention to the action of a cyclic group G . Suppose $B^T \in \text{GL}(n, \mathbf{Z})$ generates G . Fix a prime $q \neq p$. Once we have $Bv \equiv p^e v \pmod{q^f}$ we get $B^k v \equiv p^{ek} v \pmod{q^f}$ for all $k \in \mathbf{Z}$. Thus the congruence condition of Lemma 1 need only be tested for the single element B^T in G .

Let $P(f)$ denote the multiplicative group generated by the image of p in $\mathbf{Z}/(q^f)$. We frequently use the symbol $|\cdot|$ for cardinality.

LEMMA 2. For each $f > 0$

$$\gamma_p(q; f) = \sum_{r \in P(f)} \left| \{v \in \text{UNIM}_n(f) \mid (B - rI)v \equiv 0 \pmod{q^f}\} \right|.$$

PROOF. We need only check that v cannot be an eigenvector for two different eigenvalues in $P(f)$. However, if v is unimodular then $Bv \equiv rv \equiv r'v \pmod{q^f}$ implies $r \equiv r' \pmod{q^f}$. $\square$

We begin the process of throwing out primes. If S is a finite set of rational numbers, then $\Omega(S)$ denotes the smallest (necessarily finite) set of primes for which there is an $e > 0$ such that $(\prod_{\Omega(S)} q)^e s \in \mathbf{Z}$ for all $s \in S$. In simpler words, $\Omega(S)$ is the set of prime divisors for denominators of numbers in S .

First consider B as a matrix in $\text{GL}(n, \mathbf{Q})$ and let $c(x)$ be its characteristic polynomial. Factor

$$c(x) = \pi_1(x)^{d(1)} \pi_2(x)^{d(2)} \cdots \pi_t(x)^{d(t)}$$

where $\pi_1, \dots, \pi_t$ are the distinct rationally irreducible factors of $c(x)$. A "Sylov decomposition" argument shows that there is a matrix $W \in \text{GL}(n, \mathbf{Q})$ such that

$$WBW^{-1} = \text{blockdiag}(B_1, \dots, B_t)$$

and $\pi_j(x)^{d(j)}$ is the characteristic polynomial of B_j . Let S_1 be the union of entries in W , W^{-1} , $B_1, \dots$, and B_t . If $q \notin \Omega(S_1)$ then W can be treated as a matrix over

$\mathbf{Z}/(q^f)$ for all $f > 0$ in which case $W \in \text{GL}(n, \mathbf{Z}/(q^f))$. Furthermore, for such q we replace B with WBW^{-1} in the previous lemma.

Choose polynomials $\delta_{ij}(x) \in \mathbf{Q}[x]$ for $1 \leq i, j \leq t$ such that $\delta_{ij}(x)\pi_i(x)^{d(i)} + \delta_{ji}(x)\pi_j(x)^{d(j)} = 1$ for each $i < j$. Let S_2 be the set of coefficients which appear in some $\delta_{ij}(x)$, $\pi_1(x), \dots$, or $\pi_t(x)$. Now suppose $v \in \text{UNIM}_n(q^f)$ for $f > 0$ and partition it $v = (v^{(1)}, \dots, v^{(t)})$ according to the sizes of the blocks B_j . At least one $v^{(k)}$ must be unimodular. If $(B - rI)v \equiv 0 \pmod{q^f}$ for $q \notin \Omega(S_1)$, then $(B_j - rI)v^{(j)} \equiv 0 \pmod{q^f}$ for all j . Cramer's rule yields $\det(B_j - rI)v^{(j)} \equiv 0 \pmod{q^f}$. Thus $\pi_j(r)^{d(j)}v^{(j)} \equiv 0 \pmod{q^f}$ for $j = 1, \dots, t$. For the unimodular subvector we singled out, $\pi_k(r)^{d(k)} \equiv 0 \pmod{q^f}$. Now assume $q \notin \Omega(S_2)$. Then for each $j \neq k$,

$$\delta_{jk}(x)\pi_j(x)^{d(j)} + \delta_{kj}(x)\pi_k(x)^{d(k)} \equiv 1 \pmod{q^f},$$

and so, $\pi_j(r)^{d(j)}$ is a unit modulo q^f . We conclude that $v^{(j)} \equiv 0 \pmod{q^f}$ for $j \neq k$.

We have proved that if $q \notin \Omega(S_1 \cup S_2)$ and $f > 0$ then every unimodular solution to $(B - rI)v \equiv 0 \pmod{q^f}$ has the form $v = (0, \dots, 0, v^{(k)}, 0, \dots, 0)$, where $v^{(k)}$ is unimodular and $(B_k - rI)v^{(k)} \equiv 0 \pmod{q^f}$. If we write $\gamma_p^{(j)}(q; f)$ for the counting function corresponding to B_j then we have established that

$$\gamma_p(q; f) = \sum_{j=1}^t \gamma_p^{(j)}(q; f) \quad f > 0, q \notin \Omega(S_1 \cup S_2).$$

This formula reduces the rationality question to a consideration of matrices $B \in \text{GL}(n, \mathbf{Q})$ whose characteristic polynomial has the form $\pi(x)^e$, where $\pi(x) \in \mathbf{Q}[x]$ is irreducible. (Of course, we restrict ourselves to $q \notin \Omega(S_0)$ where S_0 is the set of entries of B .)

The second idea is to “generically” identify the kernel of $B - rI$ up to isomorphism. Let x be an indeterminate and consider $B - xI$ as an $n \times n$ matrix with entries in the principal ideal domain $\mathbf{Q}[x]$. The Invariant Factor Theorem states that by performing elementary row and column operations we can find matrices $D(x)$, $E(x) \in \text{GL}(n, \mathbf{Q}[x])$ of determinant 1 such that

$$D(x)(B - xI)E(x) = \text{diag}(\pi(x)^{a(1)}, \dots, \pi(x)^{a(m)}, \xi(m+1), \dots, \xi(n)).$$

Here $0 < a(1) \leq a(2) \leq \dots \leq a(m)$ and the $\xi(i)$ are rational numbers with $\xi(m+1) \cdots \xi(n) = 1$. (Incidentally, if B is not scalar then $m < n$.) Let S_3 be the union of all coefficients of all polynomial entries of $D(x)$ and $E(x)$ together with $\{\xi(m+1), \dots, \xi(n)\}$. For $q \notin \Omega(S_0 \cup S_3)$ and every integer r , we have $D(r)$, $E(r) \in \text{GL}(n, \mathbf{Z}/(q^f))$ and $\xi(i)$ is invertible modulo q^f for $i = m+1, \dots, n$.

For each integer r there is a bijection from the null space of $D(r)(B - rI)E(r)$ in $(\mathbf{Z}/(q^f))^n$ to the null space of $B - rI$ in $(\mathbf{Z}/(q^f))^n$, namely, $v \rightarrow E(r)v$. Referring to Lemma 2, if we set

$$(*) \quad \#(r; f) = \left| \left\{ v \in \text{UNIM}_m(f) \mid \pi(r)^{a(j)} v_j \equiv 0 \pmod{q^f} \text{ for } 1 \leq j \leq m \right\} \right|,$$

then $\gamma_p(q; f) = \sum_{r \in P(f)} \#(r; f)$. We state our reduced goal.

THEOREM 3. Assume that $\pi(x) \in \mathbf{Q}[x]$ is an irreducible polynomial and $0 < a(1) \leq a(2) \leq \dots \leq a(m)$ are integers. Denote by S the set of coefficients of $\pi(x)$ and for each $q \notin \Omega(S)$ define

$$\bar{\gamma}_p(q; f) = \sum_{r \in P(f)} \#(r; f) \quad (f > 0)$$

where $\#$ is defined as in (*). Then there is a finite set $S' \supseteq S$ such that $\sum_{f=1}^{\infty} \bar{\gamma}_p(q; f) T^f$ is a rational function of T which is almost formally independent of q for all $q \notin \Omega(S')$.

The reductions of this section amount to a proof that when G is cyclic, the rationality conjecture for almost all q is a consequence of Theorem 3. The next section is devoted to intricate calculations which establish the eventual regularity of $\bar{\gamma}_p(q; f)$ as f tends to infinity. As the debris settles, a proof of Theorem 3 will appear.

3. Arithmetic: estimates. We fix two distinct primes p and q . If a is a nonnegative integer let $\nu(a)$ denote the largest power of q dividing a . For example, $\nu(q^f) = f$. If $a \equiv b \pmod{q^f}$, then $q^{\nu(a)} \equiv q^{\nu(b)} \pmod{q^f}$. Consequently ν is well defined on an element r of $\mathbf{Z}/(q^f)$ as long as $\nu(r) < f$.

For the sake of completeness, we provide proofs of the next two lemmas. Their (well-known) thrust is that an infinite closed subgroup of units in the q -adic integers has finite index in the group of all units.

LEMMA 4. (i) If $b \geq 1$ and $r \equiv 1 \pmod{q^b}$, then $r^q \equiv 1 \pmod{q^{b+1}}$.

(ii) If $b \geq 2$ and $r \equiv 1 \pmod{q^b}$, $r \not\equiv 1 \pmod{q^{b+1}}$, then $r^q \not\equiv 1 \pmod{q^{b+2}}$.

PROOF. (i) Assume $r = q^b N + 1$. Then $r^q = q^{b+1} \cdot (\text{something}) + (q^b N) \cdot q + 1$.

(ii) By hypothesis, $\nu(r - 1) = b$. Since $b \geq 2$, $r \equiv 1 \pmod{q^2}$.

It follows that $1 + r + r^2 + \dots + r^{q-1} \equiv q \pmod{q^2}$, and so

$$\nu(1 + r + \dots + r^{q-1}) = 1.$$

Therefore $\nu(r^q - 1) = b + 1$. $\square$

Recall that $P(f)$ is the group of units generated by p modulo q^f .

LEMMA 5. There is a positive integer L_1 such that

$$|P(f+1)| = q|P(f)| \quad \text{for all } f \geq L_1.$$

PROOF. We first observe that $|P(f)| \rightarrow \infty$. Indeed, $p^{|P(f)|} \equiv 1 \pmod{q^f}$. Thus $|P(f)| > q^f$ as soon as $q^f > p - 1$.

Next apply Lemma 4 to $r = p^{|P(b)|}$. According to (i), either $|P(b+1)| = |P(b)|$ or $|P(b+1)| = q|P(b)|$. Part (ii) implies that if the order ever jumps for a single $b \geq 2$, then it will continue to jump from then on. The first paragraph states that $|P(b)|$ must eventually begin jumping. $\square$

Consider $\pi(x) \in \mathbf{Q}[x]$ with two properties:

($\pi 1$) If S is the set of coefficients of $\pi(x)$, then $q \notin \Omega(S)$.

($\pi 2$) $\pi(x)$ and $\pi'(x)$ have no common zeroes in $\mathbf{Z}/(q)$.

Hensel's Lemma states that every root of $\pi(x)$ in $\mathbf{Z}/(q)$ lifts to a unique root in the q -adics $\mathbf{Z}_q$. In fact, there is a one-to-one correspondence between the zeroes in $\mathbf{Z}/(q)$ and $\mathbf{Z}_q$ (and none are repeated).

Let $\lambda_1, \dots, \lambda_C$ be the zeroes of $\pi(x)$ in $\mathbb{Z}_q$ which also lie in the closure of the multiplicative monoid generated by p . (It may be that this list is empty, in which case we set $C = 0$.) When we map $\mathbb{Z}_q$ to the various $\mathbb{Z}/(q^f)$, we see that there is a positive integer L_2 such that for $f \geq L_2$,

$$\pi(r) \equiv 0 \pmod{q^f} \text{ for } r \in P(f) \leftrightarrow r \equiv \lambda_j \pmod{q^f} \text{ for some } j.$$

LEMMA 6. Assume $f > h \geq \max(L_1, L_2)$. Then

$$|\{r \in P(f) \mid \nu\pi(r) = h\}| = C(q-1)q^{f-h-1}.$$

PROOF. Since $\nu\pi(r) = h$ implies $\pi(r) \equiv 0 \pmod{q^h}$, it suffices to fix a particular λ_j and calculate the cardinality of

$$(\diamond) \quad \{r \in P(f) \mid r \equiv \lambda_j \pmod{q^h} \text{ and } \nu\pi(r) = h\}.$$

First notice that there is exactly one element in $P(h)$ congruent to λ_j . By Lemma 5 this element lifts to exactly q elements in $P(h+1)$. Of these, one is congruent to λ_j and the other $q-1$ elements *do not* satisfy $\pi(x) \equiv 0 \pmod{q^{h+1}}$. Consequently $\nu\pi(r) \geq h+1$ for one lift $r \in P(h+1)$ and $\nu\pi(r) = h$ for $q-1$ lifts.

A second application of Lemma 5 shows that each member of $P(h+1)$ has $q^{f-(h+1)}$ lifts to $P(f)$. If $s \in P(f)$ lifts an $r \in P(h+1)$ with $\nu\pi(r) < f$ (for instance, $\nu\pi(r) = h$), then $\nu\pi(r) = \nu\pi(s)$. It follows that the set $(\diamond)$ has cardinality $(q-1)q^{f-h-1}$. $\square$

To be candid, the counting that lies ahead is a mess. We are forced to “layer” $P(f)$ according to data from the matrix in §2. Assume we are given integers $0 < a(1) \leq a(2) < \dots \leq a(m)$. Let ψ denote the ceiling function for nonnegative rational numbers which rounds a nonwhole number up. It is possible to find a large positive number L_3 such that $a(j) \neq a(j+1)$ implies $\psi(f/a(j)) \neq \psi(f/a(j+1))$ for all $f \geq L_3$. Set $L = \max(L_1, L_2, L_3)$.

Assume, for the remainder of this section, that $f/a(m) > L$. We partition the half-open interval $[\psi(f/a(m)), f)$ into m subintervals (some of which may be empty):

$$I_1 = [\psi(f/a(1)), f), \quad I_j = [\psi(f/a(j)), \psi(f/a(j-1))), \quad j = 2, \dots, m.$$

Notice that an I_j is empty if and only if $j = 1$ and $a(1) = 1$ or $j > 1$ and $a(j) = a(j-1)$. In what follows, we assume that such intervals are discarded. More important, if $t \in [\psi(f/a(m)), f)$, then $t \in I_j$, where j is the earliest number such that $ta(j) \geq f$.

Our aim is to fix $r \in P(f)$ and find the number $\#(r; f)$ of unimodular rows $(v_1, \dots, v_m) \in (\mathbb{Z}/(q^f))^m$ such that $\pi(r)^{a(j)}v_i \equiv 0 \pmod{q^f}$ for $i = 1, \dots, m$. If we find such a row, then certainly $\pi(r)^{a(m)}v_i \equiv 0 \pmod{q^f}$ for all i , so, by unimodularity, $\pi(r)^{a(m)} \equiv 0 \pmod{q^f}$. That is, $\nu\pi(r) \geq \psi(f/a(m))$. Also, if $\pi(r) \equiv 0 \pmod{q^f}$, then $\#(r; f)$ is the full number of unimodular vectors, $q^{mf} - q^{m(f-1)}$. Thus we may limit ourselves to examining $r \in P(f)$ with $\nu\pi(r) \in [\psi(f/a(m)), f)$.

LEMMA 7. (i) If $\nu\pi(r) \in I_1$, then $\#(r; f) = q^{mf-m(f-1)}$.

(ii) If $\nu\pi(r) \in I_j$ for $j > 1$, then

$$\#(r; f) = q^{\nu\pi(r)(a(1) + \dots + a(j-1))} (q^{(m-j+1)f} - q^{(m-j+1)(f-1)}).$$

PROOF. Set $t = \nu\pi(r)$.

(i) In this case $ta(1) \geq f$, from which it follows that $ta(j) \geq f$ for all j . Consequently $\pi(r)^{a(j)} \equiv 0 \pmod{q^f}$ for $j = 1, \dots, m$. Hence every unimodular row is a solution to our problem.

(ii) In this case $\pi(r)^{a(l)} \equiv 0 \pmod{q^f}$ for $l \geq j$ but $\nu(\pi(r)^{a(k)}) = ta(k) < f$ for $k = 1, \dots, j-1$. In particular, $q^{f-ta(k)}$ "divides" the k th coordinate for any solution to our simultaneous congruence problem ($1 \leq k \leq j-1$). Clearly, then, any unimodular solution is unimodular in the last $m-j+1$ coordinates. One sees that

$$\#(r; f) = q^{t(a(1) + \dots + a(j-1))} (q^{(m-j+1)f} - q^{(m-j+1)(f-1)}). \quad \square$$

LEMMA 8. Set $\Sigma(j) = a(1) + \dots + a(j-1)$. Then

$$\sum_{\nu\pi(r) \in I_j} \#(r; f) = C \cdot (q^{mf} - q^{m(f-1)}) (q^{f-\psi(f/a(1))} - 1) \quad \text{if } j = 1,$$

or

$$C \cdot (q-1) q^{f-1} (q^{(m-j+1)f} - q^{(m-j+1)(f-1)}) \left(\psi\left(\frac{f}{a(j-1)}\right) - \psi\left(\frac{f}{a(j)}\right) \right) \\ \text{if } j = 2 \text{ and } a(1) = 1,$$

or

$$C \cdot \frac{(q-1)q^{f-1}}{(q^{\Sigma(j)} - 1)} (q^{(m-j+1)f} - q^{(m-j+1)(f-1)}) (q^{\psi(f/a(j-1))\Sigma(j)} - q^{\psi(f/a(j))\Sigma(j)})$$

for all other j .

PROOF. Suppose $j = 1$. Combining Lemmas 6 and 7 we obtain

$$\sum_{\nu\pi(r) \in I_1} \#(r; f) = \sum_{t=\psi(f/a(1))}^{f-1} C \cdot (q-1) q^{f-t-1} (q^{mf} - q^{m(f-1)}).$$

Sum the geometric series. Similarly, suppose $j > 1$.

$$\sum_{\nu\pi(r) \in I_j} \#(r; f) = \sum C \cdot (q-1) q^{f-t-1} q^{t(a(1) + \dots + a(j-1))} (q^{(m-j+1)f} - q^{(m-j+1)(f-1)})$$

where the sum ranges from $t = \psi(f/a(j))$ to $\psi(f/a(j-1)) - 1$. There are two cases, depending on whether or not $a(1) + \dots + a(j-1) = 1$. $\square$

In addition we have

$$\sum_{\pi(r) \equiv 0} \#(r; f) = C \cdot (q^{mf} - q^{m(f-1)}).$$

We are finally ready to analyze $\bar{\gamma}_p(q; f) = \sum_{r \in P(f)} \#(r; f)$ as a function of f (for $f \geq L$). By Lemma 8 the formal power series $\sum_{f \geq L} \bar{\gamma}_p(q; f) T^f$ is a polynomial plus a

finite linear combination of power series of the following types:

- (I) $\sum_f q^{bf} T^f, \quad b \in \mathbf{Z},$
 (II) $\sum_f q^{bf+c\psi(f/a)} T^f, \quad a, b, c \in \mathbf{Z}, a > 0, \text{ and}$
 (III) $\sum_f q^{bf} \psi(f/a) T^f, \quad a, b \in \mathbf{Z}, a > 0.$

As to (I), $\sum q^{bf} T^f = 1/(1 - q^b T)$. For the other two series we break up the sums according to the remainder of f on dividing by a ,

$$\sum_f = \sum_{\rho=1}^a \sum_{f \equiv \rho \pmod{a}}.$$

Then

$$\sum_{f \equiv \rho \pmod{a}} q^{bf+c\psi(f/a)} T^f = \sum_h q^{b(ha+\rho)+c(h+1)} T^{ha+\rho} = \frac{q^{b\rho+cT^\rho}}{1 - q^{ba} T^a},$$

another rational function. We leave it as an exercise that series of type (III) are also rational. It is time to summarize.

THEOREM 9. *Let $\pi(x) \in \mathbf{Q}[x]$ have properties $(\pi 1)$ and $(\pi 2)$ with respect to q . Suppose $0 < a(1) \leq a(2) \leq \dots \leq a(m)$ is a sequence of integers which is used, together with $\pi(x)$, to define $\bar{\gamma}_p(q; f)$. Then $\sum_f \bar{\gamma}_p(q; f) T^f$ is a rational function of T .*
 $\square$

PROOF OF THEOREM 3. We are given an irreducible rational polynomial $\pi(x)$ with coefficient set S . There are rational polynomials $\alpha(x)$ and $\beta(x)$ such that $\alpha(x)\pi(x) + \beta(x)\pi'(x) = 1$. Let S' be the union of S with the coefficients of $\alpha(x)$ and $\beta(x)$. If $q \notin \Omega(S')$ then the equation $\alpha(x)\pi(x) + \beta(x)\pi'(x) \equiv 1 \pmod{q}$ makes sense. Thus $(\pi 1)$ and $(\pi 2)$ hold for q .

It follows from Theorem 9 that $\sum_f \bar{\gamma}_p(q; f) T^f$ is rational for $q \notin \Omega(S')$. In what sense are these generating functions dependent on q ? Except for the appearance of C , the formulae in Lemma 8 depend only on the symbol q and not on any of its properties. However, there are only finitely many choices for the integer C because $0 \leq C \leq \deg \pi(x)$. As a consequence, the generating functions are almost formally independent of q . $\square$

REFERENCES

1. D. R. Farkas, *Toward multiplicative invariant theory*, Group Actions on Rings, Contemp. Math., vol. 43, Amer. Math. Soc., Providence, R. I., 1985.
2. J. E. Roseblade, *Group rings of polycyclic groups*, J. Pure Appl. Algebra **3** (1973), 307–328.

DEPARTMENT OF MATHEMATICS, VIRGINIA POLYTECHNIC INSTITUTE AND STATE UNIVERSITY, BLACKSBURG, VIRGINIA 24061