ELSEVIER

Journal of Pure and Applied Algebra 126 (1998) 51–86

JOURNAL OF PURE AND APPLIED ALGEBRA

Abelian Frobenius kernels and modules over number rings

Ron Brown [a,*], David K. Harrison [b]

[a] *Department of Mathematics, University of Hawaii, 2565 The Mall, Honolulu, HI 96822, USA*
[b] *Department of Mathematics, University of Oregon, Eugene, OR 97403, USA*

Communicated by P.J. Freyd; received 19 March 1996

Abstract

Some categories of groups (typically involving groups, possibly infinite, with abelian Frobenius kernels) are shown to be equivalent to categories whose objects are modules over groups and rings. The rings in question are associated with algebraic number fields, and the category equivalences allow some applications of number theory to group theory. In particular the number of isomorphism classes of metabelian Frobenius groups with kernel of order n and complement of order m is calculated in terms of the prime factorization of n and the structure of the Euler group $(\mathbb{Z}/m\mathbb{Z})^*$. © 1998 Elsevier Science B.V.

AMS classification: 11R18; 20J15; 20E99; 20D60

1. Introduction

In this paper we investigate some connections, eventually expressed in terms of category equivalences, between the theory of groups and the theory of rings and modules. The excessively simple prototype example is the equivalence of the category of abelian groups and the category of $\mathbb{Z}$-modules. We will construct related category equivalences involving:

1.1 The full subcategory **Semi** of the category of groups whose objects are finite solvable groups in which every nonabelian subgroup has trivial center (we call such groups *semiabelian groups*).

1.2 The category **Cyclo*** whose objects are nonzero finitely generated torsion modules over rings of the form $R(m) = \mathbb{Z}[e^{2\pi i/m}, 1/m]$ where $0 < m \in \mathbb{Z}$ together with the zero module over $R(1)$; morphisms from an $R(m)$-module A to an $R(n)$-module

* Corresponding author. E-mail: ron@kahuna.math.hawaii.edu.

PII S0022-4049(96)00144-2

B are *semilinear pairs*, i.e., pairs (g, f) where $f : R(m) \longrightarrow R(n)$ is a unitary ring homomorphism, $g : A \longrightarrow B$ is a group homomorphism, and $g(ra) = f(r)g(a)$ for all $r \in R(m)$, $a \in A$.

1.3 A full subcategory **AK** of the category of groups whose objects include all abelian groups, all objects of **Semi**, all (not necessarily torsion) generalized Frobenius groups with abelian Frobenius kernel, and all generalized Frobenius complements.

These category equivalences allow the application of algebraic number theory to problems in group theory, such as the calculation of the exact number of isomorphism classes of metabelian Frobenius groups of order at most, say, 1000. (There are 569.)

Theorem 2.1 in the next section says that **Semi** is equivalent to a category **Cyclo** with the same isomorphism classes of objects as **Cyclo*** above but with more morphisms. The proof of this theorem in Section 6 is based on an analysis of homomorphisms between semidirect products of groups (Section 3) and a study of finite modules of finite cyclic groups acting without fixed points. In Section 4 we show such modules can be regarded as $R(m)$-modules and in Section 5 we show they are precisely the modules arising in a natural way from semiabelian groups.

In Section 7 we give the precise definition of the category **AK** of (1.3) above and state Theorem 7.6 which says this category is naturally equivalent to a category whose objects are pairs (A, H) where H is any group such that a ring R_H naturally associated with H is nontrivial and A is an R_H-module. The proof of Theorem 7.6 is given in Section 10 and depends on the results in Sections 8 and 9 (and Section 3). In Section 8 we examine the implications of a group H having $R_H \neq 0$; such groups turn out to be (generalized) Frobenius complements. The abelian kernels defined in Section 7 are studied in Section 9; for finite groups nontrivial abelian kernels turn out to be precisely the Frobenius kernels [6, p. 320] which are abelian. The major result of this section says that an abelian kernel of a group has a complement, and the Frobenius decomposition theorem is satisfied by the group. (See [6, p. 318] for the decomposition theorem for Frobenius groups and [4, 11] for some generalizations to infinite groups.)

The reader may have recognized that the objects of **Semi** are precisely the finite groups which are either abelian groups or metabelian Frobenius groups. We have not emphasized this fact since in our treatment of **Semi** we need little of the extensive theory of Frobenius groups (the same will not be true of the analysis of **AK**). This treatment is mostly self-contained, though some results of [13] are used.

There is a slight inefficiency in analyzing **Semi** before analyzing **AK**; roughly speaking Theorem 2.1 can be thought of as a special case of Theorem 7.6 combined with a computation of the rings R_H for finite cyclic groups H. (Such rings turn out to be the rings $R(m)$ of (1.2) above; the computation of R_H for arbitrary finite groups will appear elsewhere.) We hope this inefficiency is justified by our special interest in metabelian Frobenius groups. Doubtless, these are very simple objects compared to Frobenius groups in general, but they appear to have their subtleties, and Theorem 2.1 allows the application of the rich arithmetic theory of cyclotomic integers to these groups. In Section 11 we classify the isomorphism classes of metabelian Frobenius groups and, more generally, objects of **Cyclo**, **Cyclo***, and **Semi** in terms of

arithmetic invariants. For any integer $m > 1$ the set $\mathrm{Iso}(m)$ of isomorphism classes of metabelian Frobenius groups with Frobenius complement of order m is shown to be bijective with the set of orbits of the free abelian semigroup on the nonzero primary ideals of $R(m)$ by the action of the group of units $(\mathbb{Z}/m\mathbb{Z})^\bullet$. A $\varphi(m) : 1$ cover of $\mathrm{Iso}(m)$ by a union of free abelian semigroups leads to a formula (Theorem 11.7) expressing the number of elements of $\mathrm{Iso}(m)$ corresponding to groups of order mn in terms of the prime factorization of n and the structure of $(\mathbb{Z}/m\mathbb{Z})^\bullet$. For example, if n is square–free with r prime factors, then this number is $\varphi(m)^{r-1}$ if all the prime factors are congruent to 1 modulo m and zero otherwise, and all the isomorphism classes can be listed quite explicitly. (Each such group is isomorphic to a semidirect product of the form $(\mathbb{Z}[e^{2\pi i/m}]/\mathfrak{b}) \times \langle e^{2\pi i/m}\rangle$ where $\mathfrak{b}$ is a product of distinct maximal ideals not containing m and $e^{2\pi i/m}$ acts on the factor group by multiplication.) In Section 12 we indicate how to compute the set of all morphisms between two semiabelian groups in terms of the basic arithmetic invariants which determine the groups. Finally, in Section 13 we show the category **Cyclo*** of (1.2) above is equivalent to a category with the same isomorphism classes of objects as **Semi** but with fewer morphisms.

Modules over groups appear throughout the paper. We end this introductory section by collecting some relevant definitions. $\mathbb{Z}$ denotes the ring of integers.

Definition 1.4. Let G be a group and A be a module over the integral group ring $\mathbb{Z}G$. We then call A a *G-module* and refer to the map $G \times A \longrightarrow A$ taking each pair (g,a) to $ga := \hat{g}a$ (where $\hat{g}$ is the canonical image of g in $\mathbb{Z}G$) as the *action of G on A*. This action is said to be *without fixed points* if $ga \neq a$ whenever $1 \neq g \in G$ and $0 \neq a \in A$.

We let $S(A,G) = A \times G$ denote the *semidirect product* (not usually the direct product), i.e., the group with operation

$$(a,g)(b,h) = (a + gb, gh).$$

Now let B be an H-module and C be an I-module for some groups H and I. A *morphism from (A,G) to (B,H)* is a quadruple of maps (f,φ,j,λ) such that $\varphi : A \longrightarrow H$ and $\lambda : G \longrightarrow H$ are group homomorphisms with $\varphi \equiv 1$ if $G \neq 1$; $j : G \longrightarrow B$ is a λ-cocycle (i.e., $j(\alpha\beta) = j(\alpha) + \lambda(\alpha)j(\beta)$ for all $\alpha, \beta \in G$); and $f : A \longrightarrow B$ is a λ-semilinear φ-cocycle (i.e., $f(g\alpha) = \lambda(g)f(\alpha)$ and $f(\alpha+\beta) = f(\alpha) + \varphi(\alpha)f(\beta)$ for all $g \in G$ and $\alpha, \beta \in A$). Let $\Delta = (f,\varphi,j,\lambda)$ be such a morphism. We let $S(\Delta)$ denote the map $S(A,G) \longrightarrow S(B,H)$ with

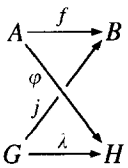
$$S(\Delta)(a,g) = (f(a) + j(g), \varphi(a)\lambda(g)) \tag{1}$$

for all $a \in A$, $g \in G$. If $\Upsilon = (g,\psi,k,\mu)$ is also a morphism from (B,H) to (C,I) then we define the composition of Δ and Υ (which may or may not be a morphism) to be the quadruple

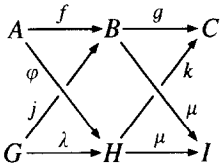
$$\Upsilon\Delta = (gf + k\varphi, (\mu\varphi)(\psi f), gj + k\lambda, (\mu\lambda)(\psi j)). \tag{2}$$

(The operations on maps above are defined pointwise; e.g., if $a \in A$ then $(gf+k\varphi)(a) = g(f(a)) + k(\varphi(a))$ and $((\mu\varphi)(\psi f))(a) = \mu(\varphi(a))\psi(f(a))$.)

Morphisms can be conveniently visualized as diagrams



and the rule for composition read off the juxtaposed diagrams



Another word of explanation. In Definition 1.4 and elsewhere we use 1 to denote either the identity of a multiplicative group or the multiplicative identity of a unitary ring or the trivial multiplicative group or a constant function taking the value 1 ... all depending on context. Similar remarks hold for zero, except that it also can denote the trivial ring! All this is routine, of course, but these conventions are used rather relentlessly here.

Finally, if g is an element of a group G, then let $\langle g \rangle$ denote the cyclic subgroup generated by g; $|g|$ the order of g; $|G|$ the order of G; $C_G(g)$ the centralizer of g in G; G' the commutator subgroup of G; and $G^{\#}$ the set of all elements of G except the identity.

2. A category equivalence for Semi

Suppose $0 < m \in \mathbb{Z}$. We set $\zeta_m = e^{2\pi i/m}$ (a primitive mth root of unity); let $C(m)$ denote the multiplicative group generated by ζ_m, and set $R(m) = \mathbb{Z}[\zeta_m, 1/m]$. If A is a (left) $R(m)$-module we write A_m for A. (This is an adaptation of the standard notation "${}_RB$" for a left R-module B.) We call A_m a *cyclotomic module*. If $m \neq n$, then we regard the zero modules 0_n and 0_m as distinct objects.

Note that if A_m is a cyclotomic module then the scalar multiplication $R(m) \times A_m \longrightarrow A_m$ restricts to an action of $C(m)$ on A_m, making A_m a $C(m)$-module. With this understanding we can apply Definition 1.4 to cyclotomic modules. Thus a *morphism of cyclotomic modules* $\Delta : A_m \longrightarrow B_n$ is just a morphism from $(A_m, C(m))$ to $(B_n, C(n))$ in the sense of Definition 1.4. Given such a morphism Δ we set $S(A_m) = S(A_m, C(m))$ and define $S(\Delta)$ as in Definition 1.4 (cf. Eq (1)). Finally, composition of morphisms is also defined as in Definition 1.4 (cf. Eq. (2)).

Theorem 2.1. *The class of finite cyclotomic modules, with morphisms and composition defined as above, is a category. S is a category equivalence from this category to* **Semi**.

We call the category of cyclotomic modules above "**Cyclo**." The theorem will be proved in Section 6. In that section we will also sketch the construction of a functor C: **Semi** $\longrightarrow$ **Cyclo** such that the compositions CS and SC are naturally equivalent to the respective identity functors. (The first proof of Theorem 2.1 involved constructing the natural equivalences between these compositions and the identity functors.) The construction of C cannot be entirely natural (in the informal sense) since, for example, any semidirect product $A \times C(m)$ has a canonical homomorphism into $C_\infty := \bigcup_n C(n)$, but semiabelian groups do not in general come equipped with such canonical homomorphisms into C_∞.

3. Morphisms of group actions

Suppose G and I are groups and A is a G-module and B is an I-module. We let $\mathscr{M} = \mathrm{Morph}((A,G),(B,I))$ denote the set of all morphisms from (A,G) to (B,I) in the sense of Definition 1.4 and let $\mathscr{H} = \mathrm{Hom}\,((A,G),(B,I))$ denote the set of all group homomorphisms $\psi : A \times G \longrightarrow B \times I$ such that if $G \neq 1$ then $\psi(A \times 1) \subset B \times 1$. (Recall that $A \times G$ denotes the semidirect product, not the direct product.) We now define maps $M : \mathscr{H} \longrightarrow \mathscr{M}$ and $H : \mathscr{M} \longrightarrow \mathscr{H}$ which are inverses of each other.

For each homomorphism $\psi \in \mathscr{H}$ let

$$M(\psi) = (\pi_B \psi\, e_A, \pi_I \psi\, e_A, \pi_B \psi\, e_G, \pi_I \psi\, e_G),$$

where $e_A : A \longrightarrow A \times G$ and $e_G : G \longrightarrow A \times G$ are the usual injections and $\pi_B : B \times I \longrightarrow B$ and $\pi_I : B \times I \longrightarrow I$ are the usual projections. For each $(f,\varphi,j,\lambda) \in \mathscr{M}$ we let

$$H(f,\varphi,j,\lambda) = (e_B f \pi_A)(e_I \varphi \pi_A)(e_B j \pi_G)(e_I \lambda \pi_G),$$

where π_A and π_G are the obvious projections and e_B and e_I the obvious injections. (The reader must from the context distinguish here and below between compositions of maps, as in "$e_B f \pi_A$," and pointwise products of maps, as in "$(e_B f \pi_A)(e_I \varphi \pi_A)$"; in general, only one of these interpretations will make sense.) With the first equation of the next lemma, it is easy to verify that

$$H(f,\varphi,j,\lambda) = S(f,\varphi,j,\lambda) \tag{3}$$

(cf. Definition 1.4).

Lemma 3.1. *Let $(f,\varphi,j,\lambda) \in \mathscr{M}$. For all $a \in A$ and $g \in G$ we have $\varphi(a)j(g) = j(g)$, $\varphi(ga) = \varphi(a)$, and $\lambda(g)\varphi(a) = \varphi(a)\lambda(g)$.*

Proof. Recall that either $G = 1$ (so $g = 1$) or $\varphi \equiv 1$. □

Proposition 3.2. *M maps into $\mathscr{M}$, H maps into $\mathscr{H}$, and M and H are inverses of each other.*

Proof. That H maps into $\mathscr{H}$ is easily checked using Lemma 3.1 and Eq. (3). Now suppose $\psi \in \mathscr{H}$; let $M(\psi) = (f, \varphi, j, \lambda)$. Then φ and λ are group homomorphisms since they are compositions of homomorphisms. j is easily checked to be a λ-cocycle and f a φ-cocycle. Also if $G \neq 1$ then $\psi(A \times 1) \subset B \times 1$ so $(\pi_I \psi e_A)(A) = 1$, i.e., $\varphi \equiv 1$. Further if $a \in A$ and $g \in G$, then using the definition of multiplication in $A \times G$ and $B \times H$ we have

$$\begin{aligned} f(ga) &= \pi_B(\psi(0,g)\psi(a,1)\psi(0,g^{-1})) \\ &= \pi_B\psi(0,g) + \pi_I\psi(0,g)\pi_B\psi(a,1) + \pi_I\psi(0,g)\pi_I\psi(a,1)\pi_B\psi(0,g^{-1}) \\ &= j(g) + \lambda(g)f(a) + \lambda(g)\varphi(a)j(g^{-1}) \\ &= \lambda(g)f(a) + j(gg^{-1}) = \lambda(g)f(a) \end{aligned}$$

since j is a λ-cocycle, and $\varphi(a)j(g^{-1}) = j(g^{-1})$ by Lemma 3.1. Thus M does map into $\mathscr{M}$.

Next note $\pi_A e_A$ is the identity map on A and $(e_A\pi_A)$ $(e_G\pi_G)$ is the identity on $A \times G$, and $\pi_G e_A$ and $\pi_A e_G$ are trivial. Using these identities and our definitions of M and H, a straightforward computation shows M and H are inverses. For example, if $\Delta = (f, \varphi, j, \lambda) \in \mathscr{M}$ then the first coordinate of $MH(\Delta)$ is by definition $\pi_B((e_B f \pi_A)(e_I \varphi \pi_A)(e_B j \pi_G)(e_I \lambda \pi_G))e_A = (\pi_B e_B f \pi_A e_A) = f$, as required, and for all $\psi \in \mathscr{H}$ we have

$$\begin{aligned} (HM)(\psi) &= (e_B\pi_B\psi e_A\pi_A)(e_I\pi_I\psi e_A\pi_A)(e_B\pi_B\psi e_G\pi_G)(e_I\pi_I\psi e_G\pi_G) \\ &= ((e_B\pi_B)(e_I\pi_I))\psi((e_A\pi_A)(e_G\pi_G)) = \psi. \end{aligned}$$ □

Now let J be a group and D be a J-module. Proceeding as above we have bijections $M' : \mathrm{Hom}((A,G),(D,J)) \longrightarrow \mathrm{Morph}((A,G),(D,J))$ and $H' : \mathrm{Morph}((B,I),(D,J)) \longrightarrow \mathrm{Hom}((B,I),(D,J))$.

Proposition 3.3. *Suppose $\Phi \in \mathrm{Morph}((A,G),(B,I))$ and $\Psi \in \mathrm{Morph}((B,I),(D,J))$ and $H'(\Psi)H(\Phi) \in \mathrm{Hom}((A,G),(D,J))$. Then*

$$M'(H'(\Psi)H(\Phi)) = \Psi\Phi.$$

Proof. The proof of Proposition 3.3 is a routine computation. For example, note that if $\Phi = (f, \varphi, j, \lambda)$ and $\Psi = (g, \psi, k, \mu)$, then the first coordinate of $M'(H'(\Psi)H(\Phi))$ is by definition $\pi_D(H'(\Psi)H(\Phi))e_A$, which maps any $a \in A$ to

$$\pi_D H'(\Psi)(f(a), \varphi(a)) = gf(a) + k\varphi(a) = (gf + k\varphi)(a).$$ □

The hypothesis on the composition $H'(\Psi)H(\Phi)$ above was made only because we did not define M' to be a map on all of $\mathrm{Hom}(A \times G, D \times J)$. (We could have done so, but then M' would have had a larger image.)

4. Group actions and cyclotomic modules

The main result of this section is the following.

Theorem 4.1. *Let A be a finite $C(m)$–module. There is an extension of the action $C(m) \times A \longrightarrow A$ to a map $R(m) \times A \longrightarrow A$ making A an $R(m)$–module if and only if the action of $C(m)$ on A is without fixed points.*

Our proof of Theorem 4.1 is surprisingly complicated for so plausible a result. The proof motivates the definition of the truncated group rings which play a central role in Sections 7–10. We begin with two preliminary results.

Lemma 4.2. *Suppose $1 \neq \zeta \in C(m)$. Then $1 - \zeta$ is a unit in $R(m)$.*

Proof. Since the polynomial $x - \zeta$ is a factor of $\Phi(x) = 1 + x + \cdots + x^{m-1}$ in $R(m)[x]$, then $1 - \zeta$ is a factor of $\Phi(1) = m$, which is a unit of $R(m)$. Hence $1 - \zeta$ is also a unit of $R(m)$. □

Lemma 4.3. *Suppose a finite group G acts without fixed points on a torsion abelian group A. Then the order of G is relatively prime to the order of every element of A.*

Proof. Suppose there exists $a \in A$ and $g \in G$ with the same prime order p. Let $\hat{g}$ denote the image of g in $\mathbb{Z}G$. Then $0 = (\hat{g}^p - 1)a = (\hat{g} - 1)^p a$ (since $g^p = 1$ and $pa = 0$). There therefore exists a least positive m with $(\hat{g} - 1)^m a = 0$. Thus $gb = b \neq 0$ where $b = (\hat{g} - 1)^{m-1} a$, contradicting that G acts without fixed points. □

The remainder of this section is devoted to the proof of Theorem 4.1. First suppose the action of $C(m)$ on A is the restriction of an $R(m)$-module scalar multiplication. If $\zeta a = a$ for some $\zeta \in C(m)$ and $a \in A$ then $(1 - \zeta)a = 0$. Then by Lemma 4.2 either $\zeta = 1$ or $a = 0$. Hence the action of $C(m)$ on A is without fixed points.

Next assume the action of $C(m)$ on A is without fixed points. Let T_m denote the group ring of $C(m)$ over $\mathbb{Z}[1/m]$. By Lemma 4.3 multiplication by m is an automorphism of A, so we can regard A as a module over T_m. Let $\mathfrak{a} = \mathfrak{a}_m$ denote the ideal of T_m generated by all elements of the form $\sum_{d \in D} \hat{d}$ where D ranges over all finite nontrivial subgroups of $C(m)$ (as before, $\hat{d}$ denotes the image of d in the group ring).

Claim 1. $\mathfrak{a}$ *is contained in the annihilator of A.*

Proof. Suppose $1 \neq b \in D < C(m)$. Then $bD = D$ and hence for any $a \in A$,

$$\hat{b}\left(\sum_{d \in D} \hat{d}\right) a = \left(\sum_{d \in D} \hat{b}\hat{d}\right) a = \left(\sum_{d \in D} \hat{d}\right) a.$$

Thus by hypothesis $\left(\sum_{d\in D}\hat{d}\right)\ a = 0$. Hence $\mathfrak{a}$ annihilates A, and Claim 1 is proved. □

Because of Claim 1 we may assume A is naturally a $T_m/\mathfrak{a}_m$-module. Hence it suffices to prove our second claim.

Claim 2. *$\mathfrak{a}_m$ is exactly the kernel of the surjective homomorphism*

$$\theta_m : T_m \longrightarrow R(m)$$

canonically associated with the inclusion maps $C(m) \longrightarrow R(m)$ and $\mathbb{Z}[1/m] \longrightarrow R(m)$.

Proof. Clearly, $\mathfrak{a}_m \subset \ker\theta_m$ (any kth root of unity ζ satisfies $\sum_{i=0}^{k-1}\zeta^i = 0$). Thus it suffices to prove $\mathfrak{a}_m \supset \ker\theta_m$. First suppose $m = p^{t+1}$ is a nontrivial power of a prime p (so $t \geq 0$). Let $\alpha \in \ker\theta_m$. Then there exists a polynomial $f(x) \in \mathbb{Z}[1/m][x]$ with $\alpha = f(\hat{\zeta}_m)$, so $f(\zeta_m) = \theta_m(\alpha) = 0$. Hence there exists $g(x) \in \mathbb{Q}[x]$ with $f(x) = \Phi(x)g(x)$ where $\Phi(x)$ is the mth cyclotomic polynomial. Indeed $g(x) \in \mathbb{Z}[1/m][x]$ since in a Dedekind domain, content is multiplicative (e.g. see [6, Exercise 4, p. 610]). (Details. There exists a nonzero $s \in \mathbb{Z}$ with $sg(x) \in \mathbb{Z}[x]$. The $\mathbb{Z}[1/m]$-content of $sg(x)$ equals that of $sf(x)$ and hence is divisible by s, so $g(x) \in \mathbb{Z}[1/m][x]$.) Hence $\alpha = \Phi(\hat{\zeta}_m)g(\hat{\zeta}_m)$ is in the ideal generated by $\Phi(\hat{\zeta}_m) = \sum_{i=0}^{p-1}\hat{\zeta}_m^{ip^t}$, which is in $\mathfrak{a}_m$ since $\zeta_m^{p^t} \neq 1$ has order p. Thus $\alpha \in \mathfrak{a}_m$. Hence $\ker\theta_m \subset \mathfrak{a}_m$ in this case.

It remains to prove $\ker\theta_m \subset \mathfrak{a}_m$ when we can write $m = sk$ where s and k are relatively prime integers larger than 1. By induction on the number of prime factors of m we may assume $\ker\theta_s \subset \mathfrak{a}_s$ and $\ker\theta_k \subset \mathfrak{a}_k$. We may identify T_s and T_k with subrings of T_m and regard thereby $\mathfrak{a}_s$ and $\mathfrak{a}_k$ as additive subgroups of $\mathfrak{a}_m$. Indeed $\mathfrak{a}_s$ and $\mathfrak{a}_k$ together generate $\mathfrak{a}_m$ as an ideal since $\mathfrak{a}_m$ is in fact generated as an ideal by all elements of the form $\sum_{d\in D}\hat{d}$ where D ranges over all subgroups of $C(m)$ of prime order, and any such subgroup is a subgroup of either $C(s)$ or $C(k)$. Thus it suffices to show that $\ker\theta_m$ is generated as an ideal by $(\ker\theta_s) \cup (\ker\theta_k)$.

We have a commutative diagram with exact rows induced by θ_m, θ_k and θ_s:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \ker\theta_m & \longrightarrow & T_m & \longrightarrow & R(m) & \longrightarrow & 0 \\
 & & \uparrow{\scriptstyle \sigma_1} & & \uparrow{\scriptstyle \sigma_2} & & \uparrow{\scriptstyle \sigma_3} & & \\
0 & \longrightarrow & \ker(\theta_s\otimes\theta_k) & \longrightarrow & T_s\otimes T_k & \longrightarrow & R(s)\otimes R(k) & \longrightarrow & 0
\end{array}$$

where all tensor products are as $\mathbb{Z}$–modules, where σ_2 is induced by the multiplication on T_m and the natural maps $T_s \longrightarrow T_m$ and $T_k \longrightarrow T_m$, and where σ_3 is induced by the multiplication map on $R(m)$ and the inclusions $R(s) \longrightarrow R(m)$ and $R(k) \longrightarrow R(m)$. All the groups above can be considered as free $\mathbb{Z}[1/m]$–modules and as such we have

$$\operatorname{rank} T_s \otimes T_k = sk = m = \operatorname{rank} T_m$$

and

$$\operatorname{rank} R(s) \otimes R(k) = \varphi(s)\varphi(k) = \varphi(m) = \operatorname{rank} R(m)$$

(where φ above denotes the Euler φ-function). Thus σ_2 and σ_3, and hence also σ_1, are isomorphisms. Thus it suffices to show $\ker(\theta_s \otimes \theta_k)$ is generated by $T_s \otimes \ker \theta_k$ and $\ker \theta_s \otimes T_k$. In order to analyze $\theta_s \otimes \theta_k$ we consider the commutative diagram

$$\begin{array}{ccccccc}
 & & \ker \theta_s \otimes T_k & \longrightarrow & \ker \theta_s \otimes R(k) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \mu_2} & & \downarrow & & \\
T_s \otimes \ker \theta_k & \xrightarrow{\mu_4} & T_s \otimes T_k & \xrightarrow{\mu_5} & T_s \otimes R(k) & \longrightarrow & 0 \\
 & & & & \downarrow{\scriptstyle \mu_6} & & \\
 & & & & R(s) \otimes R(k) & &
\end{array}$$

which has exact rows and columns by the right exactness of the functors $-\otimes R(k)$, $T_s \otimes -$, and $\ker \theta_s \otimes -$. A diagram chase shows $\ker(\mu_6\mu_5)$ is generated as a group by the images of μ_2 and μ_4; that is, $\ker \theta_s \otimes \theta_k$ is generated by $\ker \theta_s \otimes T_k$ and $T_s \otimes \ker \theta_k$. This completes the proof of Claim 2 and hence of Theorem 4.1. □

5. Group actions and semiabelian groups

In the previous section we showed that the group actions without fixed points of finite cyclic groups on finite abelian groups are precisely those arising from finite cyclotomic modules. In this section we prove in Propositions 5.3 and 5.5 the analogous fact for semiabelian groups.

Proposition 5.1. *Suppose G is a semiabelian group. Then there exists a unique normal maximal abelian subgroup N of G. Moreover, G/N is cyclic, the order of N is relatively prime to $[G : N]$, and G has an element of order $[G : N]$.*

Proof. These assertions are trivial (take $N = G$) if G is abelian, so suppose it is not. Weisner [13] showed G must have a normal maximal abelian subgroup N and moreover that G/N is cyclic, any Sylow subgroup of N is a Sylow subgroup of G (so N has order relatively prime to $[G : N]$), and N is disjoint from any other such subgroup. It follows that N is unique, for if K were another such subgroup then NK would be a still larger abelian group. (This is clear if $N \cap K$ is nontrivial, but otherwise for all $n \in N$ and $k \in K$, $nkn^{-1}k^{-1} \in N \cap K$ so $nk = kn$.) The existence of an element of G of order $[G : N]$ is easy (consider a power of any $g \in G$ with gN generating G/N). □

Notation 5.2. We let N_G denote the subgroup N of Proposition 5.1 and let $m_G = [G : N_G]$.

Proposition 5.3. *Let G be a semiabelian group and let $g \in G$ have order $m = m_G$. There is a unique action of $C(m)$ on N_G with $\zeta_m n = gng^{-1}$ for all $n \in N_G$ and this action is without fixed points.*

We will call the above action of $C(m)$ on N_G the *g-action* (to emphasize its dependence on the choice of g).

Proof. Suppose $g^s n g^{-s} = n$ where $s \in \mathbb{Z}$, $1 \neq n \in N_G$. We will show $g^s = 1$, so that m divides s. This implies that conjugation by g is an automorphism of order m_G on N_G, proving the existence of the alleged group action of $C(m)$ on N_G. It also shows that this group action is without fixed points. Note n is in the center of the group generated by g^s and N_G, so this group is abelian (G is semiabelian) and hence equals N_G (a maximal abelian subgroup). Thus $g^s \in N_G$, so $g^s = 1$ and m divides s (recall m_G is relatively prime to the order of N_G). The uniqueness assertion is obvious since ζ_m generates $C(m)$. □

Remark 5.4. With notation as in Proposition 5.3, it is easy to check that there is an isomorphism

$$\delta_g : N_G \times C(m) \longrightarrow G$$

with $\delta_g(n, \zeta_m^i) = ng^i$ for all $n \in N_G$, $i \in \mathbb{Z}$. We will use this isomorphism in later sections.

In Proposition 5.3 we showed that semiabelian groups give rise to actions by $C(m)$ without fixed points. We next show that all such actions arise essentially in this way.

Proposition 5.5. *Suppose $1 < m \in \mathbb{Z}$ and $C(m)$ acts without fixed points on some nontrivial $C(m)$-module A. Let $G = A \times C(m)$. Then G is semiabelian, $N_G = A \times 1 = G'$ and $(0, \zeta_m)$ has order $m_G = m$. Moreover, if we identify A with $A \times 1$, then the given action of $C(m)$ on A is the $(0, \zeta_m)$-action of $C(m)$ on N_G.*

Corollary 5.6. *If G is a semiabelian group which is not abelian, then N_G is the commutator subgroup of G.*

Proof. By Remark 5.4 we may as well assume $G = A \times C(m)$ where $C(m)$ has an action on A without fixed points; then Proposition 5.5 tells us that $N_G = G'$. □

Proof of Proposition 5.5. Recall from Theorem 4.1 that A is naturally an $R(m)$-module. G is clearly solvable. Note for any $x = (b, r)$ and $y = (a, s)$ in G we have

$$xyx^{-1}y^{-1} = ((1 - s)b - (1 - r)a, 1). \tag{4}$$

Suppose x and y both commute with some $z = (e, t) \neq (0, 1)$ in G; in order to show G is semiabelian it suffices to prove $xyx^{-1}y^{-1} = (0, 1)$ and hence that

$$(1 - s)b = (1 - r)a. \tag{5}$$

Eq. (4) applied to the pair x and z and also to y and z yields

$$(1-r)e = (1-t)b \quad \text{and} \quad (1-s)e = (1-t)a. \tag{6}$$

Then

$$\begin{aligned}(1-t)a + s(1-t)b &= (1-s)e + s(1-r)e \\ &= (1-r)e + r(1-s)e = (1-t)b + r(1-t)a.\end{aligned}$$

Hence,

$$t((1-s)b - (1-r)a) = (1-s)b - (1-r)a.$$

If $t \neq 1$ then (5) follows from the fact that $C(m)$ acts without fixed points and if $t = 1$ then (6) implies $r = s = 1$ (Lemma 4.2), so again (5) is satisfied. Thus G is semiabelian. $A \times 1$ is easily checked to be the normal maximal abelian subgroup of G. That it equals G' follows directly from Eq. (4) and Lemma 4.2 which implies $(1-\zeta)A = A$ whenever $1 \neq \zeta \in C(m)$. Finally, $(0, \zeta_m)$ clearly has order m and for any $a \in A$,

$$(0,\zeta_m)(a,1)(0,\zeta_m)^{-1} = (\zeta_m a, 1).$$

That is, the $(0,\zeta_m)$-action of $C(m)$ on $A \times 1$ is just the given action of $C(m)$ on A (identifying A with $A \times 1$). □

6. Proof of Theorem 2.1

Let A_m and B_n be cyclotomic modules. As usual we also regard A as a $C(m)$-module and B as a $C(n)$-module.

We first examine the behavior of S on cyclotomic modules. The action of $C(m)$ on A_m is without fixed points by Theorem 4.1, so $S(A_m) = A \times C(m)$ is semiabelian (Proposition 5.5). On the other hand, if G is a semiabelian group, say with $m = m_G$ (cf. Notation 5.2), then there is an action of $C(m)$ on N_G which is without fixed points (Proposition 5.3) and has $G \cong N_G \times C(m)$ (Remark 5.4). Then N_G is an $R(m)$-module (Theorem 4.1) with $S(N_G)_m) \cong G$.

We next consider the action of S on morphisms. The next lemma is the key to applying the results of Section 3, and uses the notation of that section.

Lemma 6.1. $\mathrm{Hom}(A \times C(m), B \times C(n)) = \mathrm{Hom}((A, C(m)), (B, C(n)))$.

Proof. We must show that if $m \neq 1$, then every homomorphism $A \times C(m) \longrightarrow B \times C(n)$ carries $A \times 1$ into $B \times 1$. If $n = 1$ this is obvious. If $n \neq 1$, then $A \times 1$ is the commutator subgroup of $A \times C(m)$ and similarly for B (when $A \neq 0$ we can use Theorem 4.1 to apply Proposition 5.5). The lemma follows therefore from the fact that homomorphisms carry commutators to commutators. □

Now suppose $\Phi : A_m \longrightarrow B_n$, $\Psi : B_n \longrightarrow D_s$, and $\Delta : D_s \longrightarrow E_t$ are morphisms of cyclotomic modules. We use the notation of Section 3 with $G = C(m)$, $I = C(n)$ and $J = C(s)$. Eq. (3) and Proposition 3.2 show $S(\Phi)$ is a homomorphism. Lemma 6.1 implies that the hypothesis on $H'(\Psi)H(\Phi)$ in Proposition 3.3 is satisfied, so $\Psi\Phi$ is in the image of M' and hence by Proposition 3.2 is a morphism. Applying the inverse of M' to both sides of the equation in Proposition 3.3 yields

$$S(\Psi)S(\Phi) = S(\Psi\Phi) \tag{7}$$

(using Eq. (3) and Proposition 3.2 to replace H, H', and the inverse of M' by S). Hence the associativity of composition of functions implies

$$S\big(\Delta(\Psi\Phi)\big) = S(\Delta)S(\Psi)S(\Phi) = S\big((\Delta\Psi)\Phi\big).$$

Since S is injective on $\mathrm{Morph}\big((A, C(m)), (E, C(t))\big)$ by Proposition 3.2, it follows that $\Delta(\Psi\Phi) = (\Delta\Psi)\Phi$, so composition of morphisms is associative.

The quadruple $(1_A, 1, 0, 1_{C(m)})$ is easily checked to be an identity for A_m (where 0 and 1 denote constant maps and $1_A : A \longrightarrow A$ and $1_{C(m)} : C(m) \longrightarrow C(m)$ are identity maps). Thus **Cyclo** is indeed a category. By Eq. (7), S is a functor from **Cyclo** to **Semi**. It is bijective on morphism sets by Proposition 3.2 and Lemma 6.1 and, as was shown above, every object of **Semi** is isomorphic to one in the image of S. Hence S is an equivalence of categories [6, Proposition 1.3, p. 27]. This completes the proof of Theorem 2.1. □

In the remainder of this section we sketch the construction of a functor C: **Semi** $\longrightarrow$ **Cyclo** such that the compositions CS and SC are naturally equivalent to the respective identity functors. As remarked in Section 2, such a construction must involve some choice; here we assume we have chosen for each semiabelian group G a particular element $g_G \in G$ of order m_G (cf. Proposition 5.1 and Notation 5.2). We may as well assume that we pick $g_G = (0, \zeta_m)$ whenever A_m is a cyclotomic module and G is the semidirect product $A \times C(m)$. We can then let C be the functor assigning to each object G of **Semi** the cyclotomic module $(N_G)_{m_G}$, where N_G has the $R(m_G)$-module structure associated with the g_G-action of $C(m_G)$ on N_G (cf. Proposition 5.3 and the paragraph immediately following and Theorem 4.1). C also assigns to any homomorphism $\psi : G \longrightarrow H$ of semiabelian groups the morphism $M(\delta_{g_H}^{-1}\psi\,\delta_{g_G})$, where

$$M : \mathrm{Hom}((N_G, C(m_G)), (N_H, C(m_H))) \longrightarrow \mathrm{Morph}((N_G, C(m_G)), (N_H, C(m_H)))$$

is defined just as in Section 3 but taking $(A, G) = (N_G, C(m_G))$ and $(B, I) = (N_H, C(m_H))$ (the action of $C(m_G)$ on N_G is of course the g_G-action, and similarly for H). Remark 5.4 and Proposition 5.5 (and the identification of $A \times 1$ with A) are the keys to constructing the promised natural equivalences of functors.

7. The category AK

Let G be a group.

Definition 7.1. A nontrivial normal subgroup N of G is an *abelian kernel* for G if G/N is locally finite; $C_G(n) = N$ for all $n \in N^{\#}$; and $mN = N$ whenever m is the order of an element of G/N.

In the above definition we used additive notation for N.

Example 7.2. (A) Any nontrivial abelian group is an abelian kernel for itself.

(B) Suppose G is locally finite. Then a nontrivial normal subgroup N of G is an abelian kernel for G if and only if $C_G(\alpha) = N$ for all $\alpha \in N^{\#}$ (cf. Lemma 4.3). In particular, for finite nonabelian groups the abelian kernels are just the Frobenius kernels which happen to be abelian [10, p. 348].

(C) Here is an example of an abelian kernel in a group having elements of infinite order. Let G be the semidirect product of the multiplicative group $\mathbb{Z}^{\bullet} = \{1, -1\}$ and the dyadic rationals $R(2) = \mathbb{Z}[1/2]$ (where $\mathbb{Z}^{\bullet}$ acts on $R(2)$ by multiplication). Then $R(2) \times 1$ is an abelian kernel for G. We will return to this example in Remark 9.10.

We now define a category of modules (analogous to the category **Cyclo***) which is equivalent to a full subcategory of groups whose objects include all groups having an abelian kernel.

Definition and Notation 7.3. We let $\mathbb{Z}_G$ denote the ring $\mathbb{Z}\,[\{1/n : G \text{ has an element of order } n\}]$. We let $\mathfrak{a}_G$ denote the ideal of the group ring $\mathbb{Z}_G G$ generated by elements of the form $\sum_{h \in H} \hat{h}$ where H ranges over the nontrivial finite subgroups of G and where for any $g \in G$, we denote by $\hat{g}$ the image of g under the natural map $G \longrightarrow \mathbb{Z}_G G$. We call the quotient ring $R_G = \mathbb{Z}_G G/\mathfrak{a}_G$ the *truncated group ring* of G. For $g \in G$ we also let $\bar{g} = \hat{g} + \mathfrak{a}_G \in R_G$.

Example 7.4. (A) The proof of Theorem 4.1 (cf. Claim 2) showed $R_{C(m)}$ is isomorphic to $R(m)$ by a map taking $\overline{\zeta}_m$ to ζ_m. Thus if $G = \langle g \rangle$ is any cyclic group of order m, then there is an isomorphism $R_G \longrightarrow R(m)$ taking $\bar{g}$ to ζ_m.

(B) If G is the Klein 4-group $\langle 1, \sigma, \tau, \sigma\tau \rangle$, then $R_G = 0$. After all, the unit $\hat{\sigma} = (1/2)(\hat{\sigma}(1+\hat{\tau}) + (1+\hat{\sigma}) - (1+\hat{\sigma}\hat{\tau}))$ is in $\mathfrak{a}_G$. This example is generalized in the proof of Corollary 8.5.

Definition and Notation 7.5. By a *truncated module* we mean a pair (M, G) where G is a locally finite group with $R_G \neq 0$ and M is a left R_G-module. Given such a pair (M, G) we can canonically regard M as a G-module and define morphisms between such pairs, and compositions of such morphisms, as in Definition 1.4. For any morphism $\Delta = (f, \varphi, j, \lambda) : (M, G) \longrightarrow (N, H)$ of truncated modules we define $S(M, G)$ and $S(\Delta) : S(M, G) \longrightarrow S(N, H)$ also as in Definition 1.4.

Theorem 7.6. *The truncated modules, with morphisms and composition as indicated above, form a category, and S is category equivalence from this category to the full subcategory of the category of groups whose objects are groups having an abelian kernel and subgroups of such groups which intersect that abelian kernel trivially.*

This theorem will be proved in Section 10. In Corollary 9.6 we will see that the subgroups of groups with an abelian kernel which intersect that abelian kernel trivially are precisely the "generalized Frobenius complements" in the sense of Definition 8.3.

8. Modules over truncated group rings

Throughout this section G will denote a locally finite group. We begin with an alternate description of the ideal $\mathfrak{a}_G$ of $\mathbb{Z}_G G$.

Lemma 8.1. *$\mathfrak{a}_G$ is generated as a left ideal of $\mathbb{Z}_G G$ by $\{\sum_{h\in H} \hat{h} : H$ is a subgroup of G of prime order$\}$.*

Proof. Let $\mathfrak{a}$ be the left ideal of R_G generated by the above set. If $g \in G$, and if $h \in G$ has prime order p, then

$$\hat{g}\left(\sum_{f\in H} \hat{f}\right) = \left(\sum_{f\in gHg^{-1}} \hat{f}\right)\hat{g};$$

this shows $\mathfrak{a}$ is an ideal contained in $\mathfrak{a}_G$. But then $\mathfrak{a} = \mathfrak{a}_G$ since any nontrivial finite subgroup H of G has an element h of prime order and $\sum_{g\in H} \hat{g} = \sum_{g\in T} \hat{g} \sum_{f\in\langle h\rangle} \hat{f}$ where T is a system of coset representatives for the cosets of $\langle h\rangle$ in H. □

If M is a left R_G-module then M is in a natural way a G-module. Our first main result describes when a G-module structure on an abelian group can be lifted to an R_G-module structure; it is related to Theorem 4.1.

Theorem 8.2. *Let M be a nontrivial G-module. The following are equivalent:*

(A) *M has a left R_G-module structure with $\overline{g}m = gm$ for all $g \in G$ and $m \in M$;*

(B) *the semidirect product $M \times G$ has abelian kernel $M \times 1$;*

(C) *G acts on M without fixed points and $mM = M$ whenever m is the order of an element of G.*

Proof. Suppose $\alpha \in M$ and suppose $g \in G$ has order $n > 1$. Note

$$(0, g)(\alpha, 1)(0, g)^{-1} = (g\alpha, 1).$$

From this identity the equivalence of (B) and (C) is easily verified.

Suppose condition (A) is true. Then $1/n \in \mathbb{Z}_G$ so clearly $nM = M$. If $g\alpha = \alpha$, then

$$\alpha = g\alpha = (1/n)(\alpha + g\alpha + g^2\alpha + \ldots + g^{n-1}\alpha)$$
$$= (1/n)\left(\sum_{h\in\langle g\rangle} \bar{h}\right)\alpha = 0\alpha = 0.$$

Thus G acts on M without fixed points, so (C) is true.

Finally, assume (C). By hypothesis and Lemma 4.3 M is a $\mathbb{Z}_G G$-module (with $\hat{g}\alpha = g\alpha$). It suffices to show $\mathfrak{a}_G M = 0$. Note

$$g\left(\sum_{h\in\langle g\rangle} h\alpha\right) = \sum_{h\in\langle g\rangle} h\alpha$$

so by hypothesis $\left(\sum_{h\in\langle g\rangle} \hat{h}\right)\alpha = 0$. Thus $\mathfrak{a}_G M = 0$. This completes the proof of Theorem 8.2. □

Definition 8.3. Suppose N is an abelian kernel for a group J. We call a subgroup H of J a *complement for* N in J if $HN = J$ and $H \cap N = 1$. We will call a group G a *generalized Frobenius complement* if it is a complement for an abelian kernel for some group.

We will remark in Proposition 8.6 that the usual Frobenius complements [6, Definition 5.4, p. 317] are just the finite nontrivial generalized Frobenius complements.

Theorem 8.4. *G is a generalized Frobenius complement if and only if $R_G \neq 0$.*

Proof. ($\Leftarrow$) This follows easily from the previous theorem (take M to be R_G, considered as a left R_G-module).

($\Rightarrow$) Let J be a group containing G with abelian kernel N and with $J = GN$ and $G \cap N = 1$. G acts on N by conjugation, so we can regard N as a $\mathbb{Z}G$-module. Indeed by Definition 7.1 and Lemma 4.3, we may regard N as a $\mathbb{Z}_G G$-module. (If $m\alpha = 0$ where m is the order of some $g \in G$, then $\langle g\rangle$ acts without fixed points on the torsion subgroup of N, so $\alpha = 0$.) Now suppose $R_G = 0$. Suppose that $\alpha \in N$ and that $g \in G$ has order $s > 1$. Let $\beta = (1 + \hat{g} + \cdots + \hat{g}^{s-1})\alpha$. Then $(1 - \hat{g})\beta = (1 - \hat{g}^s)\alpha = 0$, so $\beta = g\beta g^{-1}$ and so $g \in G \cap C_J(\beta)$. But $C_J(\beta) = N$ if $\beta \neq 0$, contradicting that $s > 1$ since $G \cap N = 1$. Thus $\beta = 0$. This shows $N = (\mathbb{Z}_G G)N = \mathfrak{a}_G N = 0$, a contradiction. Hence $R_G \neq 0$. □

The next result, which is standard for Frobenius complements [8, Theorem 18.1 (i), p. 193], will be used in Section 9.

Corollary 8.5. *Suppose G is a generalized Frobenius complement and p is a prime number. Then G has no subgroup of order p^2 and exponent p.*

Proof. Suppose $H = \langle \alpha, \beta \rangle$ were such a subgroup of G. For $\delta \in H$ let $\delta^* = \sum_{\rho \in \langle \delta \rangle} \hat{\rho}$. Then

$$p = \alpha^* - \alpha^* \beta^* + \sum_{\delta \in \langle \alpha \rangle} (\delta\beta)^*.$$

(The key facts here are that $\alpha^* \beta^* = \sum_{\delta \in H} \hat{\delta}$, and that the $p + 1$ groups $\langle \alpha \rangle$ and $\langle \delta\beta \rangle$, for $\delta \in \langle \alpha \rangle$, intersect trivially in pairs.) Thus $1 \in \mathfrak{a}_G$, contradicting that $R_G \neq 0$ (Theorem 8.4). □

Proposition 8.6. *Let H be a subgroup of G.*

(A) *If $R_H = 0$, then $R_G = 0$.*

(B) *If G is a generalized Frobenius complement, then so is H.*

(C) *If G is finite and nontrivial, then it is a generalized Frobenius complement if and only if it is a Frobenius complement.*

Proof. The inclusion map $H \longrightarrow G$ induces a unitary homomorphism $R_H \longrightarrow R_G$; (A) follows directly from this. (B) follows from the previous theorem, using (A). We now prove (C). Frobenius complements (of finite groups) are clearly generalized Frobenius complements in the sense of Definition 8.3 (note that if H is a Frobenius complement of a finite group J with kernel N, then the commutator subgroup N' of N is a normal subgroup of G and N/N' is an abelian kernel for G/N' with complement isomorphic to H). Now suppose G is a finite nontrivial generalized Frobenius complement. R_G cannot be divisible as an additive group, since it is finitely generated as a $\mathbb{Z}_G$-module. Hence there exists a prime integer t with $tR_G \neq R_G$. Let $M = R_G/tR_G$. M is finite since as a ring it is a homomorphic image of $(\mathbb{Z}/t\mathbb{Z})G$. Then $M \times 1$ is an abelian kernel for the semidirect product $M \times G$ with complement $0 \times G \cong G$ by Theorem 8.2. Hence G is a Frobenius complement. □

We now come to the last main result of this section.

Theorem 8.7. *If G is a generalized Frobenius complement, then it is finite or countable.*

Proof. We may suppose G is infinite. First suppose G has a finite nonsolvable subgroup. Let E denote the set of elements of G of order prime to 30.

Claim 1. *E is a normal subgroup of G of index at most* 240.

Subproof. E is closed under conjugation by elements of G, so it suffices to show it is a subgroup of index at most 240. Let $a, b \in E$. Since G is locally finite, there is a finite nonsolvable subgroup F of G with $a, b \in F$. Then F is a nonsolvable Frobenius complement (Proposition 8.6). Hence by a theorem of Zassenhaus [8, Theorem 18.6, p. 204] F has a subgroup of index at most 2 which itself is an internal direct product of a subgroup M which is a $\mathbb{Z}$-group of order prime to 30 and a subgroup L isomorphic to

$SL(2,5)$. The image of a in G/ML has order dividing 2 and prime to 2, so $a \in ML$ and hence $a \in M$. (Recall the order of a is relatively prime to that of $SL(2,5)$.) Similarly, $b \in M$ and hence $ab \in M \subset E$. Hence E is a normal subgroup of the locally finite group G.

Let us now suppose $[G : E] > 240$. Let $a_1, \ldots, a_{241} \in G$ represent distinct cosets of E. We may suppose the group F of the previous paragraph has been chosen to contain all the a_i, $i \leq 241$. By the above paragraph $M = F \cap E$, so we have a natural injection $F/M \longrightarrow G/E$, so the cosets $a_i M$, $1 \leq i \leq 241$, are all distinct. This contradicts the fact that

$$[F : M] = [F : ML][ML : M] \leq 2[SL(2,5) : 1] = 240.$$

The claim is proved. □

Because of the above claim, it suffices to show that E is countable. Now every finite subgroup of E is solvable, since all the elements of E have order prime to 30 [8, Theorem 18.6, p. 204]. Hence for the remainder of the proof we may assume, without loss of generality, that all the members of the set $\mathscr{F}$ of all finite subgroups of G are solvable.

Let $A \in \mathscr{F}$. Then by [8, Theorem 18.2, p. 196] A admits a normal subgroup of index at most 24 which is a $\mathbb{Z}$–group, and hence A has a subnormal series of the form

$$A_0 = A \supset A_1 \supset \cdots \supset A_5 \supset A_6 = 1, \tag{8}$$

where $[A_i : A_{i+1}] \leq 3$ for $i \leq 3$ and where A_4/A_5 and A_5 are cyclic (A_4 is the normal subgroup which is a $\mathbb{Z}$–group). Then an easy induction shows that for all $i \leq 6$, $A_i \supset A^{(i)}$ (the ith higher commutator group) [9, Lemma 5.7, p. 83]. Thus the derived series of A has length at most 6. Since G is locally finite, the derived series of G has length at most 6. In order to show G is countable, it suffices to show $B_i := G^{(i)}/G^{(i+1)}$ is finite or countable whenever $0 \leq i \leq 5$. Suppose $0 \leq i \leq 5$ and $0 < t \in \mathbb{Z}$. In order to show B_i is finite or countable, it suffices to show it contains at most t^6 elements of order t. Let $A \in \mathscr{F}$. Then it suffices to show that $C := A \cap G^{(i)}/A \cap G^{(i+1)}$ has at most t^6 elements of order t. This follows from the next claim.

Claim 2. *C is a direct product of at most 6 cyclic groups.*

Subproof. The derived series of G yields a normal series for A:

$$A = G^{(0)} \cap A \supset G^{(1)} \cap A \supset \cdots \supset G^{(6)} \cap A = 1$$

(where it is possible that $G^{(s)} \cap A$ or even $G^{(s)}$ is trivial for $s < 6$). Combining this with the subnormal series (8) we have a subnormal series for any $i < 6$:

$$\begin{aligned} G^{(i)} \cap A = (G^{(i+1)} \cap A)(G^{(i)} \cap A_0) \supset (G^{(i+1)} \cap A)(G^{(i)} \cap A_1) \\ \supset (G^{(i+1)} \cap A)(G^{(i)} \cap A_2) \supset \cdots \supset (G^{(i+1)} \cap A)(G^{(i)} \cap A_6) = G^{(i+1)} \cap A \end{aligned}$$

(cf. the construction of a common refinement to two series [9, pp. 77–78]). For each $j \leq 6$, the jth factor group of this series is

$$(G^{(i+1)} \cap A)(G^{(i)} \cap A_{j-1})/(G^{(i+1)} \cap A)(G^{(i)} \cap A_j)$$

which is a homomorphic image of $G^{(i)} \cap A_{j-1}/G^{(i)} \cap A_j$, which in turn injects into the cyclic group A_{j-1}/A_j. Thus C has a subnormal series of length at most 6 with cyclic factor groups. The claim follows from this and the fundamental theorem of finite abelian groups. □

9. Groups with an abelian kernel

Throughout this section N will denote an abelian kernel of a group G. We develop here the properties of such groups which will be needed in the proof of Theorem 7.6. These include analogues of many of the fundamental properties of Frobenius groups; in Remark 9.10 below we note that not all such properties generalize to groups with abelian kernel.

Theorem 9.1. *There exists a complement for N in G.*

Our proof of Theorem 9.1 will require some preliminary lemmas. As usual N is regarded as a G/N-module; the action takes any pair (gN, α) to $g\alpha g^{-1}$ (for $g \in G$, $\alpha \in N$).

Lemma 9.2. *N is a $\mathbb{Z}_{G/N}$-module.*

Proof. Say $g \in G$ and gN has order n, so $1/n$ is one of the generators of $\mathbb{Z}_{G/N}$. By hypothesis multiplication by n is a surjection $N \longrightarrow N$. It suffices to show it is in fact a bijection. Just suppose $n\alpha = 0$ for some $\alpha \in N$. Now $\langle gN \rangle$ surely acts on N_t, the torsion subgroup of N, and $\alpha \in N_t$. Since N is an abelian kernel, this action has no fixed points. Then n is relatively prime to the order of α (Lemma 4.3), so $\alpha = 0$. Thus multiplication by n is injective on N. □

Lemma 9.3. *Suppose $1 \neq \beta \in G/N$. Then $1 - \overline{\beta}$ is a multiplicative unit in $R_{G/N}$.*

Proof. β has finite order, say m. By Lemma 4.2 and Example 7.4(A), $1 - \gamma$ is a unit in $R_{\langle\beta\rangle}$, where γ denotes the image of β in $R_{\langle\beta\rangle}$. The canonical unitary homomorphism $R_{\langle\beta\rangle} \longrightarrow R_{G/N}$ carries $1 - \gamma$ to $1 - \overline{\beta}$, so $1 - \overline{\beta}$ is a unit in $R_{G/N}$. □

Lemma 9.4. *If $g \in G \backslash N$, then $N = \{gag^{-1}a^{-1} : a \in N\}$.*

Proof. Since N is an abelian kernel for G, Theorem 8.2 implies that N has the natural $R_{G/N}$-module structure. Hence $(\overline{g} - 1)N = N$ by Lemma 9.3. That is, $N = \{gag^{-1}a^{-1} :$

$a \in N\}$. (We have written N additively when thinking of it as an $R_{G/N}$-module and multiplicatively when thinking of it as a subgroup of G.) □

Lemma 9.5. *Suppose that H is a complement for N in G and that K is a nontrivial subgroup of G with $K \cap N = 1$. Then there exists a unique $b \in N$ with $K \subset bHb^{-1}$.*

Proof. Suppose that $1 \neq a \in K$.

Claim 1. *There exists a unique $b \in N$ with $a \in bHb^{-1}$.*

Subproof. By hypothesis there exists $c \in N$, $d \in H$ with $a = dc$. Note $d \neq 1$ since $N \cap K = 1$. By Lemma 9.4 there exists $e \in N$ with $c = d^{-1}ede^{-1}$. Then $a = d(d^{-1}ede^{-1}) \in eHe^{-1}$. Now suppose $b \in N$ and $a \in bHb^{-1}$; we will prove that $b = e$. Write $a = bhb^{-1}$ for $h \in H$. Then $(e^{-1}b)h(e^{-1}b)^{-1}h^{-1} = e^{-1}aeh^{-1} \in H \cap N = 1$. Thus $h \in C_G(e^{-1}b) \cap H$. Hence $e = b$ (since otherwise $1 \neq h \in N \cap H = 1$), as required. □

Claim 2. *Say $xyx^{-1} \in \langle y \rangle$ for some $x, y \in K^{\#}$. Suppose $x = sgs^{-1}$ and $y = tkt^{-1}$ where $s, t \in N$ and $g, k \in H$. Then $s = t$.*

Subproof. By hypothesis $1 \neq xyx^{-1} \in tHt^{-1}$ and also $xyx^{-1} = \alpha gkg^{-1}\alpha^{-1} \in \alpha H\alpha^{-1}$ where $\alpha = sgs^{-1}tg^{-1} \in N$. Thus by Claim 1, $sgs^{-1}tg^{-1} = t$, so $sgs^{-1} = tgt^{-1}$. Again by Claim 1, $s = t$. Claim 2 is proved. □

We may suppose, without loss of generality, that K is finite. After all, K is isomorphic to a subgroup of the locally finite group G/N.

We now consider two special cases. First suppose K is a finite group of odd order. Since K is isomorphic to a subgroup of G/N, it is a finite Frobenius complement (cf. Proposition 8.6) and hence we can write $K = \langle x, y \rangle$ where $x \neq 1$, $y \neq 1$ and $xyx^{-1} \in \langle y \rangle$ [8, Theorem 18.1 (p. 194) and Proposition 12.11 (p. 106)]. Applying Claims 1 and 2 to x and y we see there exists a unique $b \in N$ with $K = \langle x, y \rangle \subset bHb^{-1}$. Next suppose K is a finite group of even order. Then K has a unique element, say y, of order 2 [8, Theorem 18.1iii, p. 194]. There exists a unique $b \in N$ with $y \in bHb^{-1}$. For any $x \in K^{\#}$, $xyx^{-1} \in \langle y \rangle$. Hence (again applying Claims 1 and 2 to x and y), $x \in bHb^{-1}$. Thus $K \subset bHb^{-1}$.

We can now prove our main result for this section.

Proof of Theorem 9.1. Since G/N is countable (Theorem 8.7), G is the union of a chain of subgroups $L_1 \subset L_2 \subset L_3 \ldots$ such that for all $i \geq 1$, N is a normal subgroup of L_i of finite index.

Let $L = L_i$ for some $i \geq 1$. Clearly, N is an abelian kernel for L; we now show it has a complement Δ_i in L. Since multiplication by $[L : N]^{-1}$ is an isomorphism $N \longrightarrow N$ (Lemma 9.2), N is weakly projective as a (left) L/N–module [3, Proposition 8.6, p. 200], so $\hat{H}(L/N, N) = 0$ [3, Proposition 2.2, p. 236]. In particular, $H^2(L/N, N) = 0$,

so the exact sequence $0 \longrightarrow N \longrightarrow L \longrightarrow L/N \longrightarrow 0$ splits [3, Remark, p. 303], proving the existence of the complement Δ_i.

By Lemma 9.5 there exist $b_1, b_2, \ldots \in N$ with $\Delta_i \subset b_i \Delta_{i+1} b_i^{-1}$ for all $i \geq 1$. Let Δ be the union of the chain

$$\Delta_1 \subset b_1 \Delta_2 b_1^{-1} = b_1 b_2 \Delta_3 (b_1 b_2)^{-1} \subset b_1 b_2 b_3 \Delta_4 (b_1 b_2 b_3)^{-1} \subset \cdots.$$

We claim Δ is a complement for N in G. Clearly, $\Delta \cap N = 1$. Now let $g \in G$. Then $g \in \Gamma_s$ for some $s \geq 1$, so $g = \alpha\beta$ for some $\alpha \in N$, $\beta \in \Delta_s$. But then

$$g = \left(\alpha b^{-1}\right)\left(\left(b\beta b^{-1}\right) b \left(b\beta b^{-1}\right)^{-1}\right)\left(b\beta b^{-1}\right) \in N\Delta,$$

where $b = b_1 \ldots b_{s-1}$. This proves Δ is a complement for N in G, and completes the proof of Theorem 9.1. □

We next show the objects in the subcategory of the category of groups in Theorem 7.6 are precisely the groups with abelian kernel and the generalized Frobenius complements.

Corollary 9.6. *Suppose L is a subgroup of G with $L \cap N = 1$. Then L is a generalized Frobenius complement.*

Proof. By Lemma 9.5 (and Theorem 9.1), we may suppose, without loss of generality, that L is contained in a complement H of N. But then L is a generalized Frobenius complement by Proposition 8.6(B). □

Lemma 9.7. *Suppose M is a normal subgroup of G not contained in N. Then N is a subgroup of M.*

Proof. By hypothesis there exists $g \in M \backslash N$. For any $\alpha \in N$ there exists $\beta \in N$ with $\alpha = g\beta g^{-1}\beta^{-1}$ (Lemma 9.4), which is in M. Thus $N \subset M$. □

Lemma 9.8. *Suppose $N \neq G$. If A is a normal subgroup of G such that G/A is a generalized Frobenius complement, then $A \supset N$.*

Proof. This proof will make frequent implicit use of Theorem 8.2 and Proposition 8.6. By Theorem 9.1 there is a complement J for N in G; J is naturally isomorphic to G/N.

Just suppose A does not contain N. By Lemma 9.7, A is then a proper subset of N.

N is an $R_{G/N}$-module by Theorem 8.2; suppose first that A is not an $R_{G/N}$-submodule of N. Now $J \cong G/N$ acts on A without fixed points, so there exists $h \in J$ with $pA \neq A$ where p is the order of h. We may choose such h with p prime. Since $N = pN$, the group M of elements of N/A of exponent p is nontrivial. M is clearly an $\langle h \rangle$-module. By Lemma 4.3, the action of $\langle h \rangle$ on M has fixed points; thus $h\alpha h^{-1} A = \alpha A$ for some $\alpha \in N \backslash A$ with $p\alpha \in A$. Then $\langle \alpha A, hA \rangle$ is a finite Frobenius complement

(Proposition 8.6(B)) of exponent p and order p^2. This contradicts Corollary 8.5, so we may henceforth assume A is an $R_{G/N}$-submodule of N, and hence that N/A is an $R_{G/N}$-module.

Let $H = \langle h \rangle$ be a subgroup of J of prime order p. There exists $\alpha \in N \backslash A$. Since N/A is an $R_{G/N}$-module, it is also an R_H-module (the action is induced by conjugation as usual). Let $L = R_H(\alpha A)$ be the R_H-submodule of N/A generated by αA. L is additively torsion (recall G/A is a generalized Frobenius complement) and is a cyclic module over $R_H \cong \mathbb{Z}[\zeta_p, 1/p]$ (cf. Example 7.4(A)). Thus L is finite. Hence the semidirect product $L \times H$ is a finite Frobenius group and a finite Frobenius complement (it is naturally isomorphic to a subgroup of G/A). This contradiction of the Theorem 12.6.11 of [10, p. 353] completes the proof of Lemma 9.8. □

Corollary 9.9. *A group has at most one abelian kernel. Indeed, N is the unique maximal abelian subgroup of G which is normal.*

Proof. Maximality follows from the fact that if A is any abelian subgroup of G containing N then by definition $A \subset C_G(\alpha) = N$ for any nontrivial $\alpha \in N$. Uniqueness follows from maximality and Lemma 9.7. □

Remark 9.10. Theorem 9.1 and Lemma 9.5 can be combined to extend the "decomposition theorem" for Frobenius groups to groups with an abelian kernel: if H is a complement for N in G and $\alpha \in G \backslash N$, then there exists a unique $b \in N$ with $\alpha \in bHb^{-1}$. Not all familiar properties of Frobenius groups generalize directly to groups with abelian kernel. For example, if A is a normal subgroup of G properly contained in N, then G/A does not necessarily have an abelian kernel (compare with [10, 12.6.6 (ii), p. 351]). For example let G be the semidirect product $R(2) \times \mathbb{Z}^\bullet$ (where $\mathbb{Z}^\bullet = \{\pm 1\}$ acts on $R(2) = \mathbb{Z}[1/2]$ by multiplication). Then $A = \mathbb{Z} \times 1$ is a normal subgroup of G contained in the abelian kernel $R(2) \times 1$, but G/A has no abelian kernel. (Note G/A is nonabelian and every element has order a power of 2; Proposition 4.3 says it can therefore have no abelian kernel.)

10. Proof of Theorem 7.6

The argument will parallel that of Section 6. Let **AK** (for "abelian kernel") denote the full subcategory of the category of groups whose objects are all groups with an abelian kernel and all generalized Frobenius complements. Corollary 9.6 says **AK** is precisely the category in Theorem 7.6. Also let **TM** (for "truncated modules") be the structure which in Theorem 7.6 is asserted to be a category of truncated modules.

As in Section 6 we first look at the action of S on objects. Let (A, G) be a truncated module. If $A = 0$, then $S(A, G) \cong G$, which is a generalized Frobenius complement by Proposition 8.4. If $A \neq 0$, then $S(A, G)$ has an abelian kernel by Theorem 8.2. Thus in all cases, $S(A, G)$ is an object of **AK**. We next show that for any object K

of **AK**, there exists a truncated module (A, G) with $A \times G \cong K$. If K is a generalized Frobenius complement, then it suffices to set $(A, G) = (0, K)$ (Theorem 8.4), so suppose otherwise. Then K has an abelian kernel N; by Theorem 9.1 there is a complement H in K for N. By Theorem 8.4, $R_H \neq 0$. H acts on N by conjugation and there is a natural isomorphism from the semidirect product $N \times H$ to K taking each $(a, h) \in N \times H$ to ah. Thus $N \times 1$ is an abelian kernel of $N \times H$, so N is an R_H-module (Theorem 8.2). Therefore (N, H) is a truncated module and $S(N, H) \cong K$.

We next examine the action of S on morphisms. Suppose (A, G) and (B, I) are truncated modules. We claim that

$$\mathrm{Hom}\big((A, G), (B, I)\big) = \mathrm{Hom}(A \times G, B \times I), \tag{9}$$

that is, if $G \neq 1$ then any group homomorphism $\varphi : A \times G \longrightarrow B \times I$ has $\varphi(A \times 1) \subset B \times 1$ (cf. Section 3). This is trivial if $A = 0$, so suppose $A \neq 0$. Then by Theorem 8.2, $A \times 1$ is an abelian kernel of $A \times G$. Let $T = \varphi^{-1}(B \times 1)$. Then φ induces an isomorphism from $A \times G/T$ onto a subgroup of I, so $A \times G/T$ is a generalized Frobenius complement (Proposition 8.6). Hence by Lemma 9.8, $A \times 1 \subset T$, so $\varphi(A \times 1) \subset B \times 1$, as claimed.

The remainder of the proof of Theorem 7.6 is a precise analogue of the part of the proof of Theorem 2.1 in Section 6 following Lemma 6.1, with Eq. (9) above playing here the role that Lemma 6.1 plays in Section 6. Proposition 3.2 says S carries morphisms to homomorphisms. Eq. (9) then allows us to apply Propositions 3.2 and 3.3 to conclude that a composition of morphisms is a morphism, that this composition is associative (so **TM** is a category), and that S is a functor bijective on morphism sets, so it is a category equivalence. □

11. Isomorphism classes of metabelian Frobenius groups

In this section we examine the set of isomorphism classes of metabelian Frobenius groups and, more generally, sets of isomorphism classes of objects of **Semi**, **Cyclo**, and **Cyclo***.

Throughout this section m and n will denote relatively prime positive integers with $n > 1$. Let $G = G(m) = \mathrm{Aut}(\mathbb{Q}[\zeta_m])$. For each $\sigma \in G$ and each $R(m)$-module A let σA denote the $R(m)$-module with the same addition as A and with scalar multiplication $\#_\sigma : R(m) \times A \longrightarrow A$ taking each pair (r, a) to $r\#_\sigma a = \sigma^{-1}(r)a$. Let $R(m)$-**Mod** denote the category of left $R(m)$-modules. The next lemma relates the concepts of isomorphism in **Cyclo**, **Cyclo***, and $R(m)$-**Mod**.

Lemma 11.1. *Let A_m and B_r be nonzero cyclotomic modules. The following are equivalent*:

(A) *A_m and B_r are isomorphic in* **Cyclo**;

(B) *A_m and B_r are isomorphic in* **Cyclo***;

(C) *$m = r$ and for some $\sigma \in G$, σA_m and B_r are isomorphic in $R(m)$-***Mod**.

Proof. (C) $\Rightarrow$ (B): Suppose $f : \sigma A \longrightarrow B$ is an isomorphism in $R(m)$-**Mod** for some $\sigma \in G$. Then

$$f(ra) = f(\sigma(r)\#_\sigma a) = \sigma(r)f(a)$$

for any $r \in R(m)$ and $a \in A$, so $(f, \sigma|R(m))$ is an isomorphism $A_m \longrightarrow B_r$ in **Cyclo***.

(B) $\Rightarrow$ (A): If $(f, \sigma) : A_m \longrightarrow B_r$ is an isomorphism in **Cyclo***, then $(f, 1, 0, \sigma|C(m))$ is easily verified to be an isomorphism in **Cyclo**. (σ maps $C(m)$ into $C(r)$ since it is an isomorphism and $C(m)$ is exactly the set of roots of unity of odd order in $R(m)$ if $\frac{1}{2} \notin R(m)$ and the set of all roots of unity in $R(m)$ otherwise.)

(A) $\Rightarrow$ (C) Suppose that $(f, \varphi, j, \lambda) : A_m \longrightarrow B_r$ is an isomorphism. Then $S(A_m)$ and $S(B_r)$ are isomorphic by Theorem 2.1, so $m = r$. (Since $A \neq 0$, $m = 1$ if and only if $S(A_m)$ is abelian and hence if and only if $r = 1$. If $m \neq 1$ then $S(A_m)$ is a Frobenius group with complement of order m, so again $m = r$.) If $m = 1$, then $f : A_m \longrightarrow B_r$ is an isomorphism in $R(m)$-**Mod**. If $m > 1$ then $\varphi \equiv 0$, so f is additive and bijective (g is an inverse for f if (g, ψ, k, μ) is an inverse for (f, φ, j, λ)). Moreover for any $r \in R(m)$ and $a \in A$, $f(r\#_\sigma a) = f(\sigma^{-1}(r)a) = rf(a)$, so f is an isomorphism $\sigma A \longrightarrow B$ in $R(m)$-**Mod**. □

Remark 11.2. With the above lemma it is clear that **Cyclo** and **Cyclo*** have exactly the same sets of isomorphism classes of objects; note that for each $m > 1$ the zero $R(m)$-module 0_m, which is an object of **Cyclo** but not of **Cyclo***, lies in the isomorphism class of the $R(1)$-module $(\mathbb{Z}/m\mathbb{Z})_1$. (See Remark 12.4 for more on isomorphism in **Cyclo**.)

Let $P = P(m)$ denote the set of nonzero primary ideals of $R(m)$ and let $\mathscr{S} = \mathscr{S}(m)$ denote the free abelian semigroup on the set P. Formally, elements of $\mathscr{S}$ are functions from P to the set of nonnegative integers with finite nonempty support; we often will write any $s \in \mathscr{S}$ as a formal sum

$$s = \sum_{\mathfrak{p} \in P} s(\mathfrak{p})\mathfrak{p}.$$

For each such s let $M(s)$ denote the $R(m)$-module $\bigoplus_{\mathfrak{p} \in P}(R(m)/\mathfrak{p})^{s(\mathfrak{p})}$. G acts on P and hence on $\mathscr{S}$ ($\sigma \in G$ assigns to any $s \in S$ the composition $s\sigma^{-1}$); let $\mathscr{S}/G = \mathscr{S}(m)/G(m)$ denote the set of orbits of this group action.

Lemma 11.3. *If $\sigma \in G$ and $s \in \mathscr{S}$, then $\sigma M(s)$ and $M(\sigma s)$ are isomorphic in $R(m)$–**Mod**.*

Proof. For each $\mathfrak{p} \in P$, σ induces an isomorphism $\sigma(R(m)/\mathfrak{p}) \longrightarrow R(m)/\sigma\mathfrak{p}$ in $R(m)$-**Mod**. The lemma now follows from the fact that the action of σ on $R(m)$-modules preserves direct sums. □

Let Iso(1) denote the set of isomorphism classes of nontrivial finite abelian groups and for $m > 1$ let Iso(m) denote the set of isomorphism classes of metabelian Frobenius groups with Frobenius complement of order m.

Theorem 11.4. *The map $\mathscr{S} \longrightarrow$ Iso(m) assigning to each $s \in \mathscr{S}$ the isomorphism class of $S(M(s))$ induces a bijection $\mathscr{S}/G \longrightarrow$ Iso(m).*

The S appearing in Theorem 11.4 is the functor of Theorem 2.1.

Proof. When $m = 1$ the theorem reduces to the fundamental theorem of finite abelian groups, so suppose $m > 1$. Let $\psi : \mathscr{S} \longrightarrow$ Iso(m) be the map of the theorem. Suppose $\delta \in$ Iso(m). By Theorem 2.1 there exists a cyclotomic module D_m with δ the isomorphism class of $S(D_m)$. Since $R(m)$ is a Dedekind domain, D_m is isomorphic in $R(m)$-**Mod** to $M(s)$ for some $s \in \mathscr{S}$ [2, Proposition 23, p. 79]. Hence ψ is surjective. Now suppose $t \in \mathscr{S}$. Then $\psi(s) = \psi(t)$ if and only if $M(t)_m$ and $M(s)_m$ are isomorphic in **Cyclo** (Theorem 2.1) and hence if and only if $M(\sigma s)_m$ and $M(t)_m$ are isomorphic in $R(m)$-**Mod** for some $\sigma \in G$ (Lemmas 11.1 and 11.3). But then $\psi(s) = \psi(t)$ if and only if $\sigma s = t$ for some $\sigma \in G$ [2, Proposition 23, p. 79], i.e., s and t lie in the same orbit of $\mathscr{S}/G$. This says ψ induces a well-defined bijection $\mathscr{S}/G \longrightarrow$ Iso(m). □

Let Iso(m,n) denote the subset of Iso(m) whose elements are the isomorphism classes of groups of order mn, and let $\mathscr{S}(m,n)$ denote the set of elements $s \in \mathscr{S}$ with $|M(s)| = n$. By Lemma 11.3 the action of G on $\mathscr{S}$ restricts to an action of G on $\mathscr{S}(m,n)$; let $\mathscr{S}(m,n)/G$ denote the set of orbits.

Remark 11.5. Here are two corollaries of Theorem 11.4.

(A) There is a natural bijection $\mathscr{S}(m,n)/G \longrightarrow$ Iso(m,n).

(B) The set of all isomorphism classes of nontrivial semiabelian groups is naturally bijective with the disjoint union $\bigcup_{k>0} \mathscr{S}(k)/G(k)$.

Example 11.6. If $m = 2$ then G is trivial, so Iso(2) is bijective with $\mathscr{S}(2)$, and hence with the set of isomorphism classes of finite abelian groups of odd order. If N is such an abelian group, the corresponding Frobenius group with complement of order two is the semidirect product $N \times \{1, \sigma\}$ where $\sigma : N \longrightarrow N$ assigns to each element of N its inverse. (Note that all Frobenius groups with abelian complement of even order have abelian kernel [10, 12.6.19, p. 358].)

Now suppose $m = 4$. For small n it is easy to list the elements of $\mathscr{S}(4,n)/G(4)$. A hand count shows 59 such orbits with $n \leq 250$ and hence 59 isomorphism classes of Frobenius groups of order at most 1000 and complement of order 4.

We give two concrete examples that we will return to later. The orbits of $\mathscr{S}(4,225)$ are $\{(2+i)+(2-i)+(3)\}$, $\{2(2+i)+(3), 2(2-i)+(3)\}$ and $\{(2+i)^2+(3), (2-i)^2+(3)\}$, where the above sums of ideals are the formal sums in the free abelian semigroup $\mathscr{S}(4)$ and for each $\alpha \in R(4) = \mathbb{Z}[i, 1/2]$, (α) denotes the principal ideal generated by α. Thus every Frobenius group of order 900 with complement of order 4 is isomorphic to

exactly one of the semidirect products $\mathbb{Z}[i]/(15) \times \langle i \rangle$, $[\mathbb{Z}[i]/(2+i) \oplus \mathbb{Z}[i]/(2+i) \oplus \mathbb{Z}[i]/(3)] \times \langle i \rangle$, $\mathbb{Z}[i]/(9+12i) \times \langle i \rangle$, where i acts by multiplication. Also, $\mathscr{S}(4,85) = \{\{(2+i)+(4+i),(2-i)+(4-i)\}, \{(2+i)+(4-i),(2-i)+(4+i)\}\}$. The Frobenius groups of order 340 with complement of order 4 are therefore each isomorphic to one of the two semidirect products: $Z[i]/(7+6i) \times \langle i \rangle$ or $Z[i]/(9+2i) \times \langle i \rangle$.

We next use Theorem 11.4 to compute the number of elements of $\mathrm{Iso}(m,n)$ in terms of the group of units $(\mathbb{Z}/m\mathbb{Z})^\bullet$ and the prime factorization $n = p_1^{a_1} \dots p_r^{a_r}$, where the p_i are assumed to be distinct primes. Let $\mathscr{E} = \{i \in \mathbb{Z} : 0 \le i \le m \text{ and } GCD(m,i) = 1\}$ and for integers a and b relatively prime to m let $d(a,b)$ denote the order of the subgroup of $(\mathbb{Z}/m\mathbb{Z})^\bullet$ generated by $a+m\mathbb{Z}$ and $b+m\mathbb{Z}$. Also, if $0 < v \in \mathbb{Z}$, let $P(u,v) = 0$ if u is not a nonnegative integer and let $P(u,v)$ denote the coefficient of x^u in the power series expansion of $\prod_{i=1}^{\infty}(1-x^i)^{-v}$ otherwise. (For more on $P(u,v)$ see Lemma 11.12 and Remark 11.14.)

Theorem 11.7.

$$|\mathrm{Iso}(m,n)| = \frac{1}{\varphi(m)} \sum_{e \in \mathscr{E}} \prod_{i=1}^{r} P\left(\frac{a_i}{d(e,p_i)}, \frac{\varphi(m)}{d(e,p_i)}\right).$$

Before proving Theorem 11.7 we look at some corollaries and examples. The first well-known corollary puts strong restrictions on the order of the kernel of a Frobenius group.

Corollary 11.8. *The following are equivalent:*

(A) *there is a metabelian Frobenius group with kernel of order n and complement of order m;*

(B) *there is a Frobenius group with kernel of order n and complement of order m;*

(C) $p_i^{a_i} \equiv 1 \pmod{m}$ *for all* $i \le r$.

Proof. (A) $\Rightarrow$ (B): Trivial.

(B) $\Rightarrow$ (C): Say G, with Frobenius kernel N and complement H, is such a group. Let N_i be a p_i-Sylow subgroup. Then H acts by conjugation on the nontrivial elements of N_i and each orbit has m elements. Thus m divides $|N_i| - 1$, proving (C).

(C) $\Rightarrow$ (A): This is immediate from Theorem 11.7 since then for all $i \le r$, $a_i/d(1,p_i) \in \mathbb{Z}$, so $P(a_i/d(1,p_i), \varphi(m)/d(1,p_i)) \neq 0$. □

Corollary 11.9. *Suppose* $(\mathbb{Z}/m\mathbb{Z})^\bullet$ *is cyclic. For each* $i \le r$ *let* f_i *denote the order of* $p_i + m\mathbb{Z}$ *in* $(\mathbb{Z}/m\mathbb{Z})^\bullet$. *Then*

$$|\mathrm{Iso}(m,n)| = \sum_{d \mid \varphi(m)} \frac{\varphi(d)}{\varphi(m)} \prod_{i=1}^{r} P\left(\frac{a_i}{\mathrm{LCM}[d,f_i]}, \frac{\varphi(m)}{\mathrm{LCM}[d,f_i]}\right).$$

The summation above is over all positive divisors of $\varphi(m)$. $(\mathbb{Z}/m\mathbb{Z})^\bullet$ is cyclic if and only if m has one of the forms 1, 2, 4, p^α, or $2p^\alpha$ for p an odd prime [7, Theorem 2.25, p. 62].

Proof. For any positive divisor d of $\varphi(m)$, there are $\varphi(d)$ elements of $(\mathbb{Z}/m\mathbb{Z})^\bullet$ of order d; for each $i \leq r$ the least common multiple of d and f_i is exactly the order of the subgroup of $(\mathbb{Z}/m\mathbb{Z})^\bullet$ generated by an element of order d and $p_i + m\mathbb{Z}$. □

Example 11.10. Assume the primes p_i are indexed so that $p_i \equiv 1 \pmod 4$ if and only if $i \leq t$ (where $0 \leq t \leq r$). Corollary 11.9 then implies

$$|\operatorname{Iso}(4,n)| = \frac{1}{2}\left(\prod_{i\leq t} P(a_i,2)\prod_{i>t} P(a_i/2,1) + \prod_i P(a_i/2,1)\right).$$

For example, $|\operatorname{Iso}(4,225)| = \frac{1}{2}(P(2,2)P(1,1) + P(1,1)^2) = (5+1)/2 = 3$. The three isomorphism classes were described in Example 11.6 above.

Corollary 11.11. *Suppose n is square-free. Then* $\operatorname{Iso}(m,n)$ *is nonempty if and only if $p_i \equiv 1 \pmod m$ for all $i \leq r$, in which case it has $\varphi(m)^{r-1}$ elements. Indeed, let $\mathfrak{p}_1$ be any maximal ideal of $\mathbb{Z}[\zeta_m]$ containing p_1. If F is any metabelian Frobenius group with Frobenius complement and kernel of orders m and n respectively, then there exist unique maximal ideals $\mathfrak{p}_2,\ldots,\mathfrak{p}_r$ of $\mathbb{Z}[\zeta_m]$ with $p_i \in \mathfrak{p}_i$ for all $i \leq r$ such that F is isomorphic to the semidirect product $(\mathbb{Z}[\zeta_m]/(\mathfrak{p}_1\ldots\mathfrak{p}_r)) \times \langle\zeta_m\rangle$. Moreover, every such semidirect product is a metabelian Frobenius group with isomorphism class in* $\operatorname{Iso}(m,n)$.

For example, the number of isomorphism classes of Frobenius groups of order 340 with complement of order 4 is

$$|\operatorname{Iso}(4,5\cdot 17)| = \varphi(4)^{2-1} = 2.$$

The two isomorphism classes were described in Example 11.6.

Proof. Let $\mathfrak{p}_1$ be a prime ideal of $R(m)$ containing p_1 (note this is not the meaning of $\mathfrak{p}_1$ in the statement of the Corollary). By Corollary 11.8 we may suppose, without loss of generality, that $p_i \equiv 1 \pmod m$ for all $i \leq r$. Note $P(1/d(e,p_i), \varphi(m)/d(e,p_i))$ will be zero unless $e = 1$. Thus Theorem 11.7 implies

$$|\operatorname{Iso}(m,n)| = \frac{1}{\varphi(m)}\prod_{i=1}^{r} P(1,\varphi(m)) = \varphi(m)^{r-1}.$$

Each p_i has $\varphi(m)$ extensions to a maximal ideal of $R(m)$. Hence there are $\varphi(m)^{r-1}$ elements of the form $s = \sum_{i=1}^r \mathfrak{p}_i$ of $\mathscr{S}(m,n)$ (where $\mathfrak{p}_1$ is fixed) and these lie in distinct orbits of $\mathscr{S}(m,n)/G$. By the Chinese remainder theorem, $R(m)/(\mathfrak{p}_1\ldots\mathfrak{p}_r)$ is isomorphic to $M(s)$ and hence $(R(m)/\mathfrak{p}_1\ldots\mathfrak{p}_r) \times \langle i\rangle$ is isomorphic to $S(M(s))$. The corollary now follows from the bijective correspondence between maximal ideals of $R(m)$ and maximal ideals of $\mathbb{Z}[\zeta_m]$ which do not contain m, and the natural isomorphism $R(m)/\mathfrak{p}_1\ldots\mathfrak{p}_r \cong \mathbb{Z}[\zeta_m]/\prod_{i=1}^r \mathfrak{p}_i \cap \mathbb{Z}[\zeta_m]$. □

One might hope the situation of the previous corollary is common; after all over 60% of integers are square-free [7, Corollary 11.4, p. 293]. Indeed about 64% of the isomorphism classes of metabelian Frobenius groups of order at most 1 000 000 have commutator subgroup of square-free order (specifically, 361 610 out of 568 220). For more numerical results see Remark 11.13.

The proof of Theorem 11.7 will use the following characterization of the numbers $P(u,v)$ when $0 < u \in \mathbb{Z}$.

For any integer $k \geq 0$ let $q(k)$ denote the set of all partitions of k into a sum of positive integers, i.e., all solutions of the equation $k = x_1 + 2x_2 + 3x_3 + \cdots$ in nonnegative integers $x_1, x_2, \cdots$. (Thus $|q(0)| = 1$.)

Lemma 11.12. *Let u and v be positive integers.*

(A) $P(u,1) = |q(u)|$.

(B) *If $1 \leq w < v$ then $P(u,v) = \sum_{i=0}^{u} P(i,w)P(u-i, v-w)$.*

(C) *$P(u,v)$ is the number of sequences $(r_1,A_1),\ldots,(r_v,A_v)$ where the r_i are nonnegative integers with $\sum_{i=1}^{v} r_i = u$ and for each $i \leq v$, $A_i \in q(r_i)$.*

Proof. Let $\mathscr{D}(u,v)$ be the set of sequences described in condition (C) and set $D(u,v) = |\mathscr{D}(u,v)|$. If $1 \leq w < v$, then $\mathscr{D}(u,v)$ can be partitioned into subsets $\mathscr{D}_0,\ldots,\mathscr{D}_u$ where each $\mathscr{D}_k$ is the set of sequences $(r_1,A_1),\ldots,(r_v,A_v)$ in $\mathscr{D}(u,v)$ with $\sum_{i=1}^{w} r_i = k$. Then

$$D(u,v) = \sum_{i=0}^{u} |\mathscr{D}_i| = \sum_{i=0}^{u} D(i,w)D(u-i, v-w). \tag{10}$$

Also, by definition $D(u,1) = |q(u)|$. It remains to show $P(u,v) = D(u,v)$ for all u, v. This is well known for $v = 1$ [7, p. 273]. For $v > 1$ we can deduce by induction on v that

$$\begin{aligned}
\sum_{u=0}^{\infty} P(u,v)x^u &= \prod_{i=1}^{\infty}(1-x^i)^{-v} \\
&= \prod_{i=1}^{\infty}(1-x^i)^{-(v-1)} \prod_{i=1}^{\infty}(1-x^i)^{-1} \\
&= \sum_{u=0}^{\infty} D(u, v-1)x^u \sum_{u=0}^{\infty} D(u,1)\,x^u \\
&= \sum_{u=0}^{\infty} \left(\sum_{i=0}^{u} D(i,1)D(u-i, v-1) \right) x^u \\
&= \sum_{u=0}^{\infty} D(u,v)x^u
\end{aligned}$$

by Eq. (10). Thus $P(u,v) = D(u,v)$ for all u, v. □

Remark 11.13. (A) Using Theorem 11.7 one can compute that the number of isomorphism classes of metabelian Frobenius groups of order:

≤ 1000 is 569;
$\leq 10\,000$ is 5730;
$\leq 100\,000$ is 56 991;
$\leq 1\,000\,000$ is 568 220.

Perhaps these figures suggest some asymptotic behavior.

(B) The computations reported above were facilitated by the observation (an easy corollary of Theorem 11.7) that if $(m+1)^2 > n$, then $|\mathrm{Iso}(m,n)| \leq 1$, with equality precisely when n has the form p^a where p is a prime such that the order of $p + m\mathbb{Z}$ in $(\mathbb{Z}/m\mathbb{Z})^\bullet$ is a.

(C) The computations in (A) required that $P(a,b)$ be evaluated only when a and b were relatively small; specifically the values of $P(a,b)$ used all had $a = 1$, or $a = 2$ and $b \leq 52$, or $a \geq 3$ and $b \leq 121/a^2$. For small a one easily obtains formulas for $P(a,b)$ (Lemma 11.12 gives a difference equation to be solved):

$$P(0,b) = 1 \quad \text{and} \quad P(1,b) = b,$$
$$P(2,b) = b(b+3)/2,$$
$$P(3,b) = b(b+1)(b+8)/6,$$
$$P(4,b) = b(b+1)(b+3)(b+14)/24,$$
$$P(5,b) = b(b+3)(b^3+27b^2+134b+48)/120.$$

For the general case Euler's identity [7, Theorem 10.5, p. 274] and Lemma 11.12 give an inductive procedure for evaluating $P(a,b)$. Given values of $P(a,1)$, one can evaluate $P(a,b)$ with roughly $2a \log_2 b$ applications of Lemma 11.12(B) by first considering the case when b is a 2-power and then combining these cases to obtain the general case.

We now construct a $\varphi(m) : 1$ cover of $\mathscr{S}/G$ by a disjoint union of sets indexed by G. For each $\sigma \in G$ let R_σ denote the set of elements of $R(m)$ fixed by σ; $R(m)$ is the integral closure of R_σ in $\mathbb{Q}[\zeta_m]$ and R_σ is the integral closure of $\mathbb{Z}[1/m]$ in the fixed field $\mathbb{Q}[\zeta_m]^\sigma$. Thus R_σ is a Dedekind domain [6, Theorem 10.7, p. 613]. Let $\mathscr{S}_\sigma$ denote the free abelian semigroup on the set P_σ of nonzero primary ideals of R_σ. For any $\mathfrak{q} \in P_\sigma$ let $P(\mathfrak{q}) = \{\mathfrak{p} \in P : \mathfrak{p} \cap R_\sigma = \mathfrak{q}\}$ and for any $s \in \mathscr{S}_\sigma$ let $s \otimes R(m)$ denote the element $\sum_{\mathfrak{p} \in P} s(\mathfrak{p} \cap R_\sigma)\mathfrak{p}$ of $\mathscr{S}$. (This notation is chosen since for any $\sigma \in G$ and $s \in \mathscr{S}_\sigma$, $M(s \otimes R(m))$ is isomorphic in $R(m)$-**Mod** to $M(s) \otimes_{R_\sigma} R(m)$.)

Lemma 11.14. *For any $\sigma \in G$ and $\mathfrak{p} \in P$,*

$$P(\mathfrak{p} \cap R_\sigma) = \{\tau\mathfrak{p} : \tau \in \langle\sigma\rangle\}.$$

Proof. Suppose $\mathfrak{a}$ and $\mathfrak{b}$ are maximal ideals of $R(m)$, and s and t are positive integers. No maximal ideals of $\mathbb{Z}[1/m]$ ramify in $R(m)$ [1, Lemma 6, p. 88] and hence all maximal ideals of R_σ are unramified in $R(m)$. Thus $\mathfrak{a}^s \cap R_\sigma = (\mathfrak{a} \cap R_\sigma)^s$, and similarly for $\mathfrak{b}^t$. Now suppose $\mathfrak{a}^s \cap R_\sigma = \mathfrak{b}^t \cap R_\sigma$. Then $(\mathfrak{b} \cap R_\sigma)^t = (\mathfrak{a} \cap R_\sigma)^s$, so $s = t$ and $\mathfrak{b} = \rho\mathfrak{a}$ for some $\rho \in \langle\sigma\rangle$ [5, Proposition 2, p. 40]. Thus $\mathfrak{b}^t \in \{\tau\mathfrak{a}^s : \tau \in \langle\sigma\rangle\}$. This shows $P(\mathfrak{p} \cap R_\sigma) \subset \{\tau\mathfrak{p} : \tau \in \langle\sigma\rangle\}$. The reverse inclusion is trivial. □

Let $\mathscr{U} = \bigcup_{\sigma \in G} \{\sigma\} \times \mathscr{S}_\sigma$.

Theorem 11.15. *There is a $\varphi(m) : 1$ covering of $\mathscr{S}/G$ by $\mathscr{U}$ mapping each $(\sigma, s) \in \mathscr{U}$ to the orbit of $s \otimes R(m)$.*

Proof. Suppose $s \in \mathscr{S}$ and $\sigma \in G$. Let H denote the stabilizer of s with respect to the action of G on $\mathscr{S}$. If $s = t \otimes R(m)$ for some $t \in \mathscr{S}_\sigma$, then by Lemma 11.14

$$\begin{aligned} \sigma s &= \sum_{\mathfrak{p} \in P} t(R_\sigma \cap \sigma^{-1}(\mathfrak{p}))\mathfrak{p} \\ &= \sum_{\mathfrak{p} \in P} t(R_\sigma \cap \mathfrak{p})\mathfrak{p} = s, \end{aligned}$$

so $\sigma \in H$. Suppose, conversely, that $\sigma \in H$. Then $s(\mathfrak{p}) = s(\sigma\mathfrak{p})$ for all $\mathfrak{p} \in P$ so by Lemma 11.14 s is constant on $P(\mathfrak{p} \cap R_\sigma)$. Thus, we can unambiguously define $t \in \mathscr{S}_\sigma$ with $t(R_\sigma \cap \mathfrak{p}) = s(\mathfrak{p})$ for all $\mathfrak{p} \in P$. By construction, $s = t \otimes R(m)$. Hence $s = t \otimes R(m)$ for some $t \in R_\sigma$ if and only if $\sigma \in H$, in which case there is clearly only one such $t \in R_\sigma$. This shows that if s' is any of the [G:H] elements of the orbit of s, then there are exactly $|H|$ elements t of $\mathscr{U}$ with $t \otimes R(m) = s'$. (Note that since G is abelian, H is the stabilizer of any element of the orbit of s.) Hence the number of elements of $\mathscr{U}$ mapping to the orbit of s is $|H|[G : H] = |G| = \varphi(m)$. □

We now give the proof of Theorem 11.7. It will require the following two lemmas, which for each $\sigma \in G$ will serve to identify, and then count, the subset of $\mathscr{S}_\sigma$ corresponding to elements of $\mathrm{Iso}(m, n)$.

Lemma 11.16. *Suppose $\sigma \in G$ and $t \in \mathscr{S}_\sigma$. Then $|M(t \otimes R(m))| = |M(t)|^{|\sigma|}$.*

Proof. Let $\mathfrak{q} \in P_\sigma$ and $\mathfrak{p} \in P(\mathfrak{q})$. Write $\mathfrak{p} = \mathfrak{a}^i$ where $\mathfrak{a} \in P$ is a maximal ideal. Let $f = [R(m)/\mathfrak{a} : R_\sigma/R_\sigma \cap \mathfrak{q}]$ and $g = |P(R_\sigma \cap \mathfrak{a})|$. As was noted in the proof of Lemma 11.14, all maximal ideals of R_σ are unramified in $R(m)$ and thus $fg = |\sigma|$ [5, Corollary, p. 40] and $R_\sigma \cap \mathfrak{a}^i = (R_\sigma \cap \mathfrak{a})^i$. Hence,

$$\begin{aligned} |R(m)/\mathfrak{p}| &= |R(m)/\mathfrak{a}|^i = |R_\sigma/R_\sigma \cap \mathfrak{a}|^{fi} \\ &= |R_\sigma/R_\sigma \cap \mathfrak{a}^i|^f = |R_\sigma/\mathfrak{q}|^f. \end{aligned}$$

Therefore,

$$\begin{aligned}|M(t \otimes R(m))| &= \prod_{\mathfrak{q} \in P_\sigma} \prod_{\mathfrak{p} \in P(\mathfrak{q})} |R(m)/\mathfrak{p}|^{t(\mathfrak{q})} \\ &= \prod_{\mathfrak{q} \in P_\sigma} \prod_{\mathfrak{p} \in P(\mathfrak{q})} |R_\sigma/\mathfrak{q}|^{ft(\mathfrak{q})} \\ &= \prod_{\mathfrak{q} \in P_\sigma} |R_\sigma/\mathfrak{q}|^{fgt(q)} = |M(t)|^{|\sigma|}. \qquad \square\end{aligned}$$

For each $e \in \mathscr{E}$ let σ_e denote the unique $\sigma \in G$ with $\sigma(\zeta_m) = \zeta_m^e$; the map $e \mapsto \sigma_e$ is a bijection from $\mathscr{E}$ to G.

Lemma 11.17. *Let $e \in \mathscr{E}$ and $\sigma = \sigma_e$. Then $\prod_{i=1}^r P(a_1/d(e, p_i), \varphi(m)/d(e, p_i))$ is the number of elements of $\{t \in \mathscr{S}_\sigma : |M(t)|^{|\sigma|} = n\}$.*

Proof. Let E denote the subgroup of $(\mathbb{Z}/m\mathbb{Z})^\bullet$ generated by $e + m\mathbb{Z}$. For each rational prime p not dividing m let $\Delta(p)$ denote the set of maximal ideals of R_σ containing p and let $f_E(p)$ denote the order of $(p + m\mathbb{Z})E$ in the factor group $(\mathbb{Z}/m\mathbb{Z})^\bullet/E$. Then $f_E(p)$ is the ramification degree of p for the extension $R_\sigma/\mathbb{Z}[1/m]$ [12, Proposition 2.3, p.165] (observe that $p + m\mathbb{Z}$ corresponds to the Frobenius automorphism for p under the canonical identification of G with $(\mathbb{Z}/m\mathbb{Z})^\bullet$). Thus $|\sigma| f_E(p) = d(e, p)$ and hence $|\Delta(p)| = \varphi(m)/d(e, p)$ by [5, Corollary, p. 40] (note that p is unramified in the field extension $\mathbb{Q}[\zeta_m]^\sigma/\mathbb{Q}$, which has degree $\varphi(m)/|\sigma|$). Consider $t \in \mathscr{S}_\sigma$. Then

$$\begin{aligned}|M(t)| &= \prod_{p \nmid m} \prod_{\mathfrak{p} \in \Delta(p)} \prod_{i=1}^{\infty} |R_\sigma/\mathfrak{p}^i|^{t(\mathfrak{p}^i)} \\ &= \prod_{p \nmid m} \prod_{\mathfrak{p} \in \Delta(p)} \prod_{i=1}^{\infty} p^{f_E(p) i t(\mathfrak{p}^i)}.\end{aligned}$$

Therefore, $|M(t)|^{|\sigma|} = n$ if and only if $t(\mathfrak{p}^i) = 0$ for all $\mathfrak{p}$ containing a rational prime not dividing n and for all $k \leq r$, if $p = p_k$ then

$$a_k = |\sigma| \sum_{\mathfrak{p} \in \Delta(p)} \sum_{i=1}^{\infty} f_E(p) i t(\mathfrak{p}^i),$$

or, equivalently,

$$a_k/d(e, p) = \sum_{\mathfrak{p} \in \Delta(p)} \sum_{i=1}^{\infty} i t(\mathfrak{p}^i).$$

By Lemma 11.12(C), the number of solutions of $\sum_{\mathfrak{p} \in \Delta(p)} \sum_{i=1}^{\infty} i x_{i,\mathfrak{p}} = a_k/d(e, p)$ in nonnegative integers $x_{i,\mathfrak{p}}$ is $P(a_k/d(e, p), \varphi(m)/d(e, p))$. Hence the number of $t \in \mathscr{S}_\sigma$ with $|M(t)|^{|\sigma|} = n$ is $\prod_{k=1}^r P(a_k/d(e, p_k), \varphi(m)/d(e, p_k))$. $\square$

Proof of Theorem 11.7. Theorems 11.4 and 11.16 together give us a $\varphi(m) : 1$ cover of $\mathrm{Iso}(m)$ by $\mathscr{U}$. Hence, $\varphi(m)|\mathrm{Iso}(m,n)| = \sum_{\sigma\in G} |\{t \in \mathscr{S}_\sigma : |M(t \otimes R(m))| = n\}|$ which by Lemma 11.16 equals

$$\sum_{\sigma\in G} |\{t \in \mathscr{S}_\sigma : |M(t)|^{|\sigma|} = n\}|.$$

Finally, Lemma 11.17 then implies

$$\varphi(m)|\mathrm{Iso}(m,n)| = \sum_{e\in\mathscr{E}} \prod_{i=1}^{r} P\left(\frac{a_i}{d(e,p_i)}, \frac{\varphi(m)}{d(e,p_i)}\right). \qquad \square$$

12. Homomorphisms of metabelian Frobenius groups

Let m and n denote positive integers; let $s \in \mathscr{S}(m)$ and $t \in \mathscr{S}(n)$. Then up to isomorphism $A_m := M(s)_m$ and $B_n := M(t)_n$ form an arbitrary pair of nontrivial cyclotomic modules, and $\Gamma := S(A)$ and $\Delta := S(B)$ form an arbitrary pair of nontrivial semiabelian groups (Remark 11.3(B)). We describe here the set of homomorphisms from Γ to Δ, ultimately in terms of the numerical invariants s and t. This is equivalent, of course, to computing the set of morphisms in **Cyclo** from A_m to B_n.

We start with the homomorphisms $\Gamma \longrightarrow \Delta$ which have nonabelian image. The homomorphisms with abelian image are fairly transparent and are discussed in Remark 12.3. For any $b \in B$ and $\sigma \in G(m)$ let $j = j_{\sigma,b} : C(m) \longrightarrow B$ map any $\zeta \in C(m)$ to $(1 - \sigma(\zeta))b$. (As in Section 11, $G(m) = \mathrm{Aut}(\mathbb{Q}[\zeta_m])$.)

Proposition 12.1. *Suppose $m > 1$ and $n > 1$. The set of group homomorphisms from Γ to Δ with nonabelian image is empty if $m \nmid n$ and otherwise is naturally bijective with the set of triples (f,σ,b) where $\sigma \in G(m)$, $b \in B$, and f is a nontrivial $R(m)$-module homomorphism $(\sigma A)_m \longrightarrow B_m$. The bijection associates with any such triple (f,σ,b) the homomorphism $S(f,1,j_{\sigma,b},\sigma|C(m))$.*

The hypotheses of Proposition 12.1 are precisely those that guarantee that Γ and Δ are nonabelian, and hence are metabelian Frobenius groups. Note that if m divides n, then $R(m) \subset R(n)$ so that the $R(n)$-module B_n induces by restriction of scalar multiplication an $R(m)$-module B_m, and the restriction $\sigma|C(m)$ can be identified with a homomorphism $C(m) \longrightarrow C(n)$. We are implicitly asserting in Proposition 12.1 that the quadruples $(f,1,j_{\sigma,b},\sigma|C(m))$ are always morphisms in **Cyclo**.

Proof. First suppose $m|n$ and (f,σ,b) is a triple of the above sort. One easily verifies that $\Upsilon := (f,1,j_{\sigma,b},\sigma|C(m))$ is a morphism in **Cyclo**. $S(\Upsilon)$ has nonabelian image since if $f(a) \neq 0$ then by Lemma 4.2 $\sigma(\zeta_m)f(a) \neq f(a)$ and hence $S(\Upsilon)(a,1)$ and $S(\Upsilon)(0,\zeta_m)$ do not commute. Next suppose $\psi : \Gamma \longrightarrow \Delta$ is a homomorphism with nonabelian image. We will prove that m divides n and there is a unique triple (f,σ,b) with $\sigma \in G(m)$, f a nontrivial $R(m)$-module homomorphism $\sigma A_m \longrightarrow B_m$, and $b \in B$

such that $(f, 1, j_{\sigma,b}, \sigma|C(m))$ is a morphism in **Cyclo** with image ψ under S. By Theorem 2.1, $\psi = S(\Upsilon)$ for some morphism $\Upsilon = (f, \varphi, j, \lambda)$ of **Cyclo**. Since $m \neq 1$, $\varphi \equiv 1$. Hence f is nontrivial, since otherwise by Eq. (1), $\psi(\Gamma) \subset \psi(1 \times G)$ would be abelian. Now assume $1 \neq \zeta \in \ker \lambda$. Then for all $a \in A$, $f((1-\zeta)a) = f(a) - \lambda(\zeta)f(a) = 0$ so by Lemma 4.2, $f \equiv 0$, a contradiction. Hence $\ker \lambda$ is trivial and $\lambda : C(m) \longrightarrow C(n)$ is injective. It follows that m divides n and $\lambda = \sigma|C(m)$ for some $\sigma \in G(m)$. Then for all $\zeta \in C(m)$ and $a \in A$,

$$f(\zeta \#_\sigma a) = f(\sigma^{-1}(\zeta)a) = \zeta f(a),$$

so f is an $R(m)$-module homomorphism from σA_m to B_m. By Lemma 4.2 there exists $b \in B$ with $(1 - \sigma(\zeta_m))b = j(\zeta_m)$. An easy induction then shows $j = j_{\sigma,b}$. Hence,

$$\psi = S(f, 1, j_{\sigma,b}, \sigma|C(m)).$$

Now suppose (h, ρ, c) is another triple with $\psi = S(h, 1, j_{\rho,c}, \rho|C(m))$. Then by Theorem 2.1, $h = f$, $j_{\sigma,b} = j_{\rho,c}$, and $\rho|C(m) = \sigma|C(m)$. It follows that $\rho = \sigma$ and hence that $c = b$ since $1 - \sigma(\zeta_m)$ is a unit of $R(m)$ and

$$(1 - \sigma(\zeta_m))b = j_{\sigma,b}(\zeta_m) = j_{\rho,c}(\zeta_m) = (1 - \sigma(\zeta_m))c.$$

This completes the proof of Proposition 12.1. □

Remark 12.2. Suppose m divides n. Proposition 12.1 shows the set of homomorphisms $\Gamma \longrightarrow \Delta$ with nonabelian image is bijective with

$$\bigcup_{\sigma \in G(m)} \{\sigma\} \times \mathrm{Hom}_{R(m)}(\sigma A_m, B_m)^{\#} \times B.$$

Since $\mathrm{Hom}_{R(m)}$ is additive in both variables,

$$\mathrm{Hom}_{R(m)}(\sigma A_m, B_m) \cong \prod_{\mathfrak{p} \in P(m)} \prod_{\mathfrak{q} \in P(n)} \mathrm{Hom}_{R(m)}(\sigma(R(m)/\mathfrak{p}), R(n)/\mathfrak{q})^{s(\mathfrak{p})t(\mathfrak{q})}.$$

For each $\mathfrak{p} \in P(m)$ and $\mathfrak{q} \in P(n)$, say $\mathfrak{p} = \mathfrak{a}^i$ and $\mathfrak{q} = \mathfrak{b}^j$ where $\mathfrak{a}$ and $\mathfrak{b}$ are maximal ideals of $R(m)$ and $R(n)$ respectively, we have $\mathrm{Hom}_{R(m)}(R(m)/\mathfrak{p}, R(n)/\mathfrak{q})$ trivial if $\mathfrak{b} \cap R(m) \neq \mathfrak{a}$ and isomorphic to $R(n)/\mathfrak{b}^{\min(i,j)}$ otherwise. After all, any homomorphism $(R(m)/\mathfrak{p})_m \longrightarrow (R(n)/\mathfrak{q})_m$ is determined by the image of $1 + \mathfrak{p}$ and this must be an element of $R(n)/\mathfrak{q}$ annihilated by $\mathfrak{p}$. There are no such nontrivial elements of $R(n)/\mathfrak{q}$ if $\mathfrak{b} \cap R(m) \neq \mathfrak{a}$ since then $\mathfrak{p} + R(m) \cap \mathfrak{q} = R(m)$. On the other hand, if $\mathfrak{b} \cap R(m) = \mathfrak{a}$, then the set of such elements is exactly $\mathfrak{b}^{j-\min(i,j)}/\mathfrak{b}^j$, which is naturally isomorphic to $R(n)/\mathfrak{b}^{\min(i,j)}$. Thus the set of homomorphisms with nonabelian image is naturally bijective with

$$\bigcup_{\sigma \in G(m)} \{\sigma\} \times \prod_{\mathfrak{p} \in P(n)} (R(n)/\mathfrak{p})^{t(\mathfrak{p})} \times \left[\prod_{\mathfrak{a}} \prod_{\mathfrak{b}} \prod_{i,j} (R(n)/\mathfrak{b}^{\min(i,j)})^{s(\mathfrak{a}^i)t(\mathfrak{b}^j)} \right]^{\#},$$

where the triple product above is over all maximal ideals $\mathfrak{a}$ of $R(m)$, all $\mathfrak{b} \in P(n)$ with $\mathfrak{b} \cap R(m) = \sigma(\mathfrak{a})$, and all positive integers i and j. We leave to the interested reader (if there are any left at this point) the task of writing a formula for the number of homomorphisms in terms of s, t, $(\mathbb{Z}(m\mathbb{Z})^\bullet$, and the ramification degrees of maximal ideals of $R(m)$ and $R(n)$.

Remark 12.3. We now consider homomorphisms with abelian image.

(A) If $\Upsilon = (f, \varphi, j, \lambda) : A_m \longrightarrow B_n$ is a morphism in **Cyclo**, then $S(f, \varphi, j, \lambda)$ has abelian image if and only if $f \equiv 0$ or $\lambda \equiv 1$.

(B) Let D denote A_m if $m = 1$ and $C(m)$ if $m \neq 1$. (In all cases D is isomorphic to the commutator factor group of $A \times C(m)$.) The set of nontrivial homomorphisms $\Gamma \longrightarrow \Delta$ with abelian image is naturally bijective with

$$\mathrm{Hom}(D, B)^\# \cup (\mathrm{Hom}(D, C(n))^\# \times B). \tag{11}$$

Here $\mathrm{Hom} = \mathrm{Hom}_{\mathbb{Z}}$. The bijection assigns to each nontrivial $g \in \mathrm{Hom}(D, B)$ the homomorphism $S(g, 1, 0, 1)$ if $m = 1$ and $S(0, 1, g, 1)$ if $m \neq 1$ and assigns to each $(h, b) \in \mathrm{Hom}(D, C(n))^\# \times B$ the homomorphism $S(j_{I,b}h, h, 0, 1)$ if $m = 1$ and $S(0, 1, j_{I,b}h, h)$ if $m \neq 1$ where $I \in G(n)$ is the identity map.

The homomorphisms $\Gamma \longrightarrow \Delta$ with abelian image can be calculated in terms of s and t using the techniques of the previous remark. For example in the case $m \neq 1$ (which includes the metabelian Frobenius groups) the set (11) is naturally bijective with

$$\left(\prod_{p^i} \prod_{\mathfrak{b}} \prod_{j>1} \left(R(n)/\mathfrak{b}^{\min(i,j)}\right)^{t(\mathfrak{b}^j)} \right)^\# \bigcup \left(C\big(GCD(m,n)\big)^\# \times \prod_{\mathfrak{p} \in P(n)} (R(n)/\mathfrak{p})^{t(\mathfrak{p})} \right).$$

The first product is over all maximal prime powers p^i dividing m; the second is over all $\mathfrak{b} \in P(n)$ containing p. Details are left to the interested reader.

The proof of Remark 12.3(A) is an easy exercise using Lemmas 3.1 and 4.2. A proof of Remark 12.3(B) is possible with no reference to semiabelian groups (the condition that $S(f, \varphi, j, \lambda)$ has abelian image can be replaced by the equivalent requirement that $f = 0$ or $\lambda = 1$). The analysis breaks naturally into four cases corresponding to the four types of morphisms listed: those with $m = 1$ and $\varphi = 1$; $m = 1$ and $\varphi \neq 1$; $m \neq 1$ and $\lambda = 1$; and $m \neq 1$ and $\lambda \neq 1$. Details are left to the reader. One can also approach Remark 12.3B through the group theory. Homomorphisms of semiabelian groups with abelian image are rather transparent because of the very special nature of abelian subgroups and quotient groups of semiabelian groups (cf. Lemma 9.7).

Remark 12.4 (*Isomorphisms*). In the setting of Proposition 12.1, a triple (f, σ, b) will correspond to an isomorphism if and only if $m = n$ and f is bijective. Any other isomorphism of cyclotomic modules must be between objects of **Cyclo** of the form 0_r or D_1. Isomorphisms between such objects are precisely the quadruples of one of the forms $(0, 1, 0, \lambda) : 0_r \longrightarrow 0_r$ where $\lambda \in \mathrm{Aut}(C(r))$; $(f, 1, 0, 1) : D_1 \longrightarrow E_1$ where

$f : D \longrightarrow E$ is an isomorphism of abelian groups; $(0, 1, j, 1) : 0_r \longrightarrow D_1$ where $j : C(r) \longrightarrow D$ is a group isomorphism; or $(0, \varphi, 0, 1) : D_1 \longrightarrow 0_r$ where $\varphi : D \longrightarrow C(r)$ is a group isomorphism.

13. A category equivalence for Cyclo*

Suppose $\alpha : G \longrightarrow H$ is a homomorphism in **Semi**. We say it is *restricted* if $\alpha^{-1}(N_H) = N_G$ (cf. Notation 5.2). We say α is *equivalent* to a homomorphism $\beta : G \longrightarrow H$ in **Semi** if there exists $b \in N_H$ with $\alpha(g) = b\beta(g)b^{-1}$ for all $g \in G$.

Let **Semi*** denote the category whose objects are semiabelian groups and whose morphisms, say from G to H, are equivalence classes of restricted homomorphisms from G to H. The composition in **Semi*** of the equivalence class of a restricted homomorphism $\alpha : G \longrightarrow H$ with the equivalence class of a restricted homomorphism $\gamma : H \longrightarrow I$ is defined to be the equivalence class of $\gamma\alpha$. That this composition is well-defined and gives **Semi*** a category structure follows easily from the next lemma, whose routine proof is left to the reader.

Lemma 13.1. *Let α, $\beta \in \mathrm{Hom}(G,H)$ and γ, $\delta \in \mathrm{Hom}(H,I)$ be equivalent pairs of homomorphisms in* **Semi**.

(A) *If α and γ are restricted, then so is $\gamma\alpha$.*

(B) *If δ is restricted, then $\gamma\alpha$ and $\delta\beta$ are equivalent.*

Here is the main result for this section.

Theorem 13.2. *There is a natural equivalence S^* : **Cyclo*** $\longrightarrow$ **Semi*** which agrees with S on objects and assigns to each morphism $(f, \lambda) : A_m \longrightarrow B_n$ in* **Cyclo*** *the equivalence class of the homomorphism $S(f, 1, 0, \lambda | C(m))$.*

Proof. For any (f, λ) as above, $S(f, 1, 0, \lambda | C(m))$ is easily checked to be a restricted homomorphism of **Semi**, so S^* is clearly a functor. Let G be any semiabelian group. Then by Theorem 2.1 G is isomorphic to $S(A_m)$ for some cyclotomic module A_m in **Cyclo*** (note that any cyclotomic module of the form 0_m is isomorphic in **Cyclo** to $(C(m))_1$, i.e., to $C(m)$ considered in the natural way as a module over $R(1) = \mathbb{Z}$). Now any isomorphism $S(A_m) \longrightarrow G$ is restricted and hence induces an isomorphism in **Semi***. Thus every object in **Semi*** is isomorphic in **Semi*** to one in the image of S^*.

Now suppose A_m and B_n are objects of **Cyclo***. To prove the theorem it suffices to show the map

$$s : \mathbf{Cyclo^*}(A_m, B_n) \longrightarrow \mathbf{Semi^*}(A \times C(m), B \times C(n))$$

induced by S^* is a bijection [6, Proposition 1.3, p. 27]. (We are letting $\mathscr{C}(E,F)$ denote the set of morphisms from E to F for any objects E and F of a category $\mathscr{C}$.) So

consider any restricted homomorphism

$$\delta : A \times C(m) \longrightarrow B \times C(n).$$

Since S is an equivalence, there exists a morphism $\Delta = (f, \varphi, j, \lambda) \in \mathbf{Cyclo}(A_m, B_n)$ with $S(\Delta) = \delta$.

Just suppose λ is not injective. Then $m \neq 1$, so $\varphi = 1$. There exists $\zeta \in \ker \lambda$, $\zeta \neq 1$. Then $\delta(0, \zeta) = (j(\zeta), 1) \in B \times 1$ so

$$(0, \zeta) \in \delta^{-1}(B \times 1) = \delta^{-1}(N_{B \times C(n)}) = N_{A \times C(m)} = A \times 1$$

by Proposition 5.5. This contradiction shows λ is injective and hence is the restriction of a unitary ring homomorphism $\mu : R(m) \longrightarrow R(n)$.

Next suppose $\varphi \neq 1$. Then $m = 1$ and $n \neq 1$, so $B \neq 0$. Again using Proposition 5.5 we see

$$A \times C(m) = N_{A \times C(m)} = \delta^{-1}(N_{B \times C(n)}) = \delta^{-1}(B \times 1)$$

so $\delta(A \times C(m)) \subset B \times 1$. But $\varphi(a) \neq 1$ for some $a \in A$, so $\delta(a, 1) = (f(a), \varphi(a)) \notin B \times 1$. Thus $\varphi = 1$. Hence $f \in \mathrm{Hom}(A, B)$. Therefore $(f, \mu) \in \mathbf{Cyclo}^*(A_m, B_n)$.

We now show $S^*(f, \mu)$ is the equivalence class of δ (so the map s above is surjective). This is obvious if $m = 1$ since then $j = 0$, so δ equals $S(f, 1, 0, \mu | C(m))$. Suppose $m \neq 1$, so $n \neq 1$ and $B \neq 0$. Let $b = \big(1 - \lambda(\zeta_m)\big)^{-1} j(\zeta_m)$ (cf. Lemma 4.2). We claim $j(\zeta) = \big(1 - \lambda(\zeta)\big)b$ for all ζ in $C(m)$. This is obvious if $\zeta = \zeta_m$ and is easily proved for arbitrary powers $\zeta = \zeta_m^k$ by induction on k. Now $(b, 1) \in N_{B \times C(n)}$ and for any $(a, \zeta) \in A \times C(m)$ we have

$$\begin{aligned}
&(b, 1)\big(S(f, 1, 0, \mu | C(m))(a, \zeta)\big)(b, 1)^{-1} \\
&\quad = (b, 1)\big(f(a), \lambda(\zeta)\big)(-b, 1) = \big(f(a) + j(\zeta), \lambda(\zeta)\big) \\
&\quad = S(f, \varphi, j, \lambda)(a, \zeta) = \delta(a, \zeta).
\end{aligned}$$

Thus $S(f, 1, 0, \mu \mid C(m))$ is equivalent to δ, so $S^*(f, \mu)$ is the equivalence class of δ.

Now suppose $S^*(g, \rho) = S^*(f, \mu)$ for some $(g, \rho) \in \mathbf{Cyclo}^*(A_m, B_n)$. We prove $(g, \rho) = (f, \mu)$, which will show the map s is injective. By hypothesis there exists $b \in B$ such that for all $(a, \zeta) \in A \times C(m)$ we have

$$\big[S(f, 1, 0, \mu \mid C(m))(a, \zeta)\big](b, 1) = (b, 1)\big[S(g, 1, 0, \rho \mid C(m))(a, \zeta)\big],$$

i.e., $f(a) + \mu(\zeta)b = b + g(a)$ and $\mu(\zeta) = \rho(\zeta)$. Thus $\mu = \rho$ (a unitary homomorphism $R(m) \longrightarrow R(n)$ is determined by its action on $C(m)$). Taking $\zeta = 1$ in the above equation gives $f(a) = g(a)$, so $f = g$. This completes the proof that s is a bijection, and hence the proof of Theorem 13.2. □

References

[1] B.J. Birch, Cyclotomic fields and Kummer extensions, in: J.W.S. Cassels and A. Fröhlich, Eds., Algebraic Number Theory (Thompson, Washington, 1967) 85–93.

[2] N. Bourbaki, Algèbre Commutative, Ch. 7: Diviseurs (Hermann, Paris, 1964).
[3] H. Cartan and S. Eilenberg, Homological Algebra (Princeton Univ. Press, Princeton, 1956).
[4] M.J. Collins, Some infinite Frobenius groups, J. Algebra 131 (1990) 161–165.
[5] A. Fröhlich, Local fields, in: J.W.S. Cassels and A. Fröhlich, Eds., Algebraic Number Theory (Thompson, Washington, 1967) 1–41.
[6] N. Jacobson, Basic Algebra II (Freeman, San Francisco, 1980).
[7] I. Niven and H.S. Zuckerman, An Introduction to the Theory of Numbers (Wiley, New York, 4th edn., 1980).
[8] D. Passman, Permutation Groups (Benjamin, New York, 1968).
[9] J.J. Rotman, An Introduction to the Theory of Groups (Allyn and Bacon, Boston, 3rd edn., 1984).
[10] W.R. Scott, Group Theory (Prentice-Hall, Englewood Cliffs, NJ, 1964).
[11] A.I. Starostin, On Frobenius Groups, Ukrain. Mat. Ž. 23 (1971) 629–639. (Translated in Ukranian Math. J. 23 (1971) 518–526 (1972).)
[12] J.T. Tate, Global class field theory, in: J.W.S. Cassels and A. Fröhlich, Eds., Algebraic Number Theory (Thompson, Washington, 1967) 162–203.
[13] L. Weisner, Groups in which the normalizer of every element except the identity is abelian, Bull. Amer. Math. Soc. 31 (1925) 413–416.