Inventiones math. 25, 299–325 (1974)

Rational Functions Invariant under a Finite Abelian Group

H.W. Lenstra, Jr. (Amsterdam)

Introduction

Let k be a field and A a permutation group on n symbols $x_1, \ldots, x_n$. Then A acts in a natural way as a group of k-automorphisms on the field of rational functions $k(x_1, \ldots, x_n)$. It is an old question, whether the field of invariants

$$k(x_1, \ldots, x_n)^A = \{f \in k(x_1, \ldots, x_n) \mid g(f) = f \text{ for all } g \in A\}$$

is purely transcendental over k or not, cf. Burnside, Theory of groups of finite order, second edition (1911), Ch. XVII. One usually calls this problem "Emmy Noether's conjecture" although Emmy Noether never stated that the answer would be affirmative [35–37].

Several positive results are known on this problem. Fischer [12] treated the case when A is abelian and k contains sufficiently many roots of unity. His result has been reproved [25, 7] and refined [32, 33] several times. If A is a p-group, where $p = \mathrm{char}(k) \neq 0$, then $k(x_1, \ldots, x_n)^A$ is purely transcendental over k, by [21, 20, 22, 16, 33]. Various groups of small order are treated in [35, 37, 41, 14, 3–5, 30, 31, 23, 46, 17].

Swan [44] and Voskresenskiĭ [46] proved that $\mathbf{Q}(x_1, \ldots, x_n)^A$ is not purely transcendental over $\mathbf{Q}$ if A is a cyclic group of order $n = 47$, permuting $x_1, \ldots, x_n$ transitively. An even smaller example is given by $n = 8$, cf. (7.2). Further results for abelian A were obtained by Endo and Miyata [10] and Voskresenskiĭ [47, 48].

Our main theorem [27, 19] gives a complete solution for the case when A is abelian and transitive. In this case we can index the x_i by the elements of A such that $g(x_h) = x_{gh}$ for all $g, h \in A$; we denote the field $k(\{x_g \mid g \in A\})^A$ by k_A. Before stating the main theorem, we introduce some terminology.

Let ρ be a finite cyclic group of order m with generator τ, and let $\Phi_m \in \mathbf{Z}[X]$ be the m-th cyclotomic polynomial. The ideal $\Phi_m(\tau)\mathbf{Z}[\rho] \subset \mathbf{Z}[\rho]$ (= group ring of ρ over $\mathbf{Z}$) does not depend on the choice of τ, and we define

$$\mathbf{Z}(\rho) = \mathbf{Z}[\rho]/\Phi_m(\tau)\,\mathbf{Z}[\rho].$$

Then $\mathbf{Z}(\rho) \cong \mathbf{Z}[\zeta_m]$, where ζ_m denotes a primitive m-th root of unity, so by [26, Ch. IV, Th. 4] the ring $\mathbf{Z}(\rho)$ is a Dedekind domain. The group of units of $\mathbf{Z}(\rho)$ contains ρ in a natural way.

Denote by k_{cycl} the maximal cyclotomic extension of the field k inside an algebraic closure. Consider a subfield $K \subset k_{\mathrm{cycl}}$ containing k for which

(0.1) $\quad \rho_K = \mathrm{Gal}(K/k)$ is finite cyclic, with generator τ_K,

and let p and s satisfy

(0.2) $\quad p$ is prime, $\quad 2 \neq p \neq \mathrm{char}(k)$, $\quad s \in \mathbf{Z}$, and $s \geqq 1$.

Then we define the $\mathbf{Z}(\rho_K)$-ideal $\mathfrak{a}_K(p^s)$ by

$$\mathfrak{a}_K(p^s) = \mathbf{Z}(\rho_K) \qquad \text{if } K \neq k(\zeta_{p^s}),$$

$$\mathfrak{a}_K(p^s) = (\tau_K - t, p) \subset \mathbf{Z}(\rho_K) \qquad \text{if } K = k(\zeta_{p^s}), \text{ where } t \in \mathbf{Z} \text{ is such that } \tau_K(\zeta_p) = \zeta_p^t.$$

This definition does not depend on the choice of τ_K.

For a finite abelian group A, put $m(A, p, s) = \dim_{\mathbf{Z}/p\mathbf{Z}}(p^{s-1}A/p^sA)$ (here A is written additively), and

$$\mathfrak{a}_K(A) = \prod_{p,s} \mathfrak{a}_K(p^s)^{m(A,p,s)} \subset \mathbf{Z}(\rho_K),$$

the ideal product ranging over all p and s satisfying (0.2).

Let $r(A)$ be the highest power of 2 dividing the exponent of A.

Main Theorem. *Let k be a field and let A be a finite abelian group. Then the field*

$$k_A = k(\{x_g \mid g \in A\})^A$$

is purely transcendental over k if and only if the following two conditions are satisfied:

(i) *for every intermediate field $k \subset K \subset k_{\mathrm{cycl}}$ for which* (0.1) *holds, the $\mathbf{Z}(\rho_K)$-ideal $\mathfrak{a}_K(A)$ is principal;*

(ii) *if $\mathrm{char}(k) \neq 2$, then $k(\zeta_{r(A)})$ is a cyclic field extension of k.*

Note that condition (ii) is satisfied if $\mathrm{char}(k) \neq 0$.

Sections 1–5 of the present paper are devoted to the proof of the main theorem. The idea is to use Fischer's result that l_A is purely transcendental over l if l is a suitable cyclotomic extension of k. The "Galois descent" problem which arises in going from l_A to k_A is discussed, in a more general setting, in Sections 1 and 2. Section 3 gives some useful technical information. The group A does not occur in these sections. In Section 4 we show that we may assume that $\mathrm{char}(k)$ does not divide

the order of A, and Section 5 contains the proof of the main theorem. Supplementary results are given in Section 6, and some corollaries are indicated in Section 7.

The methods of this paper hardly exceed Galois theory and elementary commutative algebra. From cohomology of groups we need some facts on H^1 and $\hat{H}^{-1}$; these results are easily proved from the explicit descriptions of H^1 and $\hat{H}^{-1}$ given in [42, Ch. VII, VIII; 6, Ch. IV]. In the proof of (2.6) we need that a projective module over an abelian group ring has a rank; but this will be clear for the modules to which (2.6) is applied. We shall use freely the theory of finitely generated torsion free modules over a Dedekind ring [18]. Finally, the proofs of some corollaries in Section 7 require some algebraic number theory.

In the rest of this paper we write "rational" instead of "purely transcendental". A field extension $k \subset L$ is called "stably rational" if there exists a field extension $L \subset L'$ of finite transcendence degree such that L' is rational over both L and k. It is unknown whether "stably rational" implies "rational" [40, 9, 34].

The notations Φ_m, ζ_m, $\mathbf{Z}(\rho)$ and k_A have been introduced above. The characteristic of a field k is denoted by $\mathrm{char}(k)$, the degree of a field extension $k \subset l$ by $[l:k]$ and the group of a Galois extension $k \subset l$ by $\mathrm{Gal}(l/k)$. For a prime p, a p-group is a group whose order is a power of p. The exponent of a group is the lowest common multiple of the orders of its elements. If a group π acts on a set S, then $S^\pi = \{s \in S \mid \forall \sigma \in \pi: \sigma(s) = s\}$. The action of π on S is called *trivial* if $S = S^\pi$ and *faithful* if for every $\sigma \in \pi$, $\sigma \neq 1$, there is an $s \in S$ with $\sigma(s) \neq s$. By a π-module we mean a left module over the group ring $\mathbf{Z}[\pi]$, and we write $\otimes_\pi$ and Hom_π instead of $\otimes_{\mathbf{Z}[\pi]}$ and $\mathrm{Hom}_{\mathbf{Z}[\pi]}$, respectively. The group of units of a ring R with 1 is denoted by R^*. If M is a module and t is a nonnegative integer, then M^t denotes the direct sum of t copies of M; the only exception is the definition of $\mathfrak{a}_K(A)$ above, where we mean ideal power. Set theoretic difference is denoted by $\smallsetminus$, and $|S|$ is the cardinality of a set S. The end or the absence of a proof is marked by $\square$.

1. Permutation Modules and Rationality of Field Extensions

Let π be a finite group. A π-module is called a *permutation module* if it is free as an abelian group and has a $\mathbf{Z}$-basis which is permuted by π. For example, free π-modules are permutation modules, and $\mathbf{Z}$, with trivial π-action, is a permutation module.

Every permutation module is a direct sum of modules $\mathbf{Z}[\pi/\pi']$; here $\pi' \subset \pi$ is a subgroup and

$$\mathbf{Z}[\pi/\pi'] = \mathbf{Z}[\pi] \otimes_{\pi'} \mathbf{Z} \quad \text{(as } \pi\text{-module)}$$

where π' acts trivially on $\mathbf{Z}$. We call a π-module N *permutation-projective* if $N \oplus N'$ is a permutation module for some π-module N'. One can take N' to be finitely generated if N is, cf. the proof of (1.2).

(1.1) **Proposition.** *Let N be a permutation-projective π-module. Then $\hat{H}^{-1}(\rho, N) = H^1(\rho, N) = 0$ for every subgroup $\rho \subset \pi$.*

Proof. Since any permutation module over π is a permutation module over every subgroup $\rho \subset \pi$, we may assume $\rho = \pi$. Also we may take $N = \mathbf{Z}[\pi/\pi']$, for a subgroup $\pi' \subset \pi$. Then by Shapiro's lemma [6, Ch. IV, Prop. 2] we have $H^1(\pi, N) = H^1(\pi', \mathbf{Z}) = 0$, and the proof for $\hat{H}^{-1}$ is analogous. □

(1.2) **Proposition.** *Let N be a π-module. The following statements about N are equivalent:*

(a) *N is permutation-projective;*

(b) *for every π-homomorphism $M_1 \to M_2$ which induces surjective maps $M_1^\rho \to M_2^\rho$ for all subgroups $\rho \subset \pi$, the induced map*

$$\mathrm{Hom}_\pi(N, M_1) \to \mathrm{Hom}_\pi(N, M_2)$$

is surjective;

(c) *if L is a π-module such that $H^1(\rho, L) = 0$ for all $\rho \subset \pi$, then every exact sequence of π-modules*

$$0 \to L \to M \to N \to 0$$

splits.

Proof. (a) $\Rightarrow$ (b). We may take $N = \mathbf{Z}[\pi/\rho]$ for some subgroup $\rho \subset \pi$. Then the functors $\mathrm{Hom}_\pi(N, -)$ and $(-)^\rho$ are equivalent, and (b) follows.

(b) $\Rightarrow$ (c). Let $0 \to L \to M \to N \to 0$ be a sequence as in (c). By the exact sequence of cohomology, the map $M^\rho \to N^\rho$ is surjective for every subgroup $\rho \subset \pi$. Applying (b) to $M_1 = M$ and $M_2 = N$ we find that the sequence splits.

(c) $\Rightarrow$ (a). One easily constructs a permutation module M over π and a π-homomorphism $M \to N$ such that $M^\rho \to N^\rho$ is surjective for every $\rho \subset \pi$. Let L be the kernel of $M \to N$. The exact sequence of cohomology of

$$0 \to L \to M \to N \to 0$$

and (1.1) show that $H^1(\rho, L) = 0$ for every $\rho \subset \pi$. By (c), the sequence splits, and (a) follows. □

Note the analogy with the well known characterization of projective modules as direct summands of free modules.

Let l be a field, M a free abelian group of finite $\mathbf{Z}$-rank r, and $l[M]$ the group ring of M over l. If M is written multiplicatively and $\{b_1, \ldots, b_r\}$

is a $\mathbf{Z}$-basis for M, then

$$l[M]=l[b_1,\ldots,b_r,b_1^{-1},\ldots,b_r^{-1}].$$

Thus we see that $l[M]$ is isomorphic to the ring of Laurent polynomials in r variables over l. It follows that $l[M]$ is a unique factorization domain with group of units $l[M]^*=l^*\cdot M$. We denote the field of fractions of $l[M]$ by $l(M)$. This field is rational over l of transcendence degree r.

Now suppose that π acts faithfully on l as a group of field automorphisms, and that M has a π-module structure. We make π act on $l[M]$ by

$$\sigma\Big(\sum_{m\in M}\lambda_m\cdot m\Big)=\sum_{m\in M}\sigma(\lambda_m)\cdot\sigma(m),\qquad \text{for } \sigma\in\pi,$$

if $\lambda_m\in l$, and $\lambda_m\neq 0$ for only finitely many $m\in M$. The action is extended to $l(M)$ by $\sigma(ab^{-1})=\sigma(a)\,\sigma(b)^{-1}$, for $a,\,b\in l[M]$, and $b\neq 0$.

In Theorem (1.7) we give a necessary and sufficient condition, in terms of M, that $l(M)^\pi$ be stably rational over l^π, cf. [45, 10]. Theorem (2.6) states that in a special situation this condition even implies that $l(M)^\pi$ is rational over l^π.

Remark that $l(M)^\pi$ is rational over l^π if and only if a certain torus, defined over l^π and splitting over l, is rational over l^π, cf. [38]. This will not be used in the sequel.

We usually write the group law in M additively, although M is a sub-π-module of the *multiplicative* group of $l(M)$.

(1.3) **Proposition** [43]. *Let W be an l-vector space on which π acts semilinearly, i.e. W is a π-module and $\sigma(\lambda w)=(\sigma\lambda)\cdot(\sigma w)$ for all $\sigma\in\pi$, $\lambda\in l$ and $w\in W$. Then W^π contains an l-basis for W.*

Proof. Put $S=\big(\sum_{\sigma\in\pi}\sigma\big)\in\mathbf{Z}[\pi]$. We show that $SW\subset W^\pi$ contains an l-basis by proving that any l-linear function $\phi\colon W\to l$ annihilating SW must be the zero function. Fix such a ϕ, and fix $w\in W$. Then for every $\lambda\in l$ we have

$$0=\phi(S\cdot\lambda w)=\sum_{\sigma\in\pi}\phi(\sigma w)\cdot\sigma(\lambda).$$

By the linear independence of field automorphisms [2, Ch. V, § 7.5] we conclude $\phi(\sigma w)=0$ for all $\sigma\in\pi$. In particular $\phi(w)=0$, and (1.3) follows. □

(1.4) **Proposition** [30]. *Let N be a finitely generated permutation module over π. Then $l(N)^\pi$ is rational over l^π.*

Proof. Let $\{x_1,\ldots,x_r\}\subset l(N)^*$ be a $\mathbf{Z}$-basis for N which is permuted by π. Applying (1.3) to $W=\Big(\sum_{i=1}^{r}l\cdot x_i\Big)\subset l(N)$ we find $y_1,\ldots,y_r\in l(N)^\pi$ such that $l(y_1,\ldots,y_r)=l(N)$. It follows that $l(N)^\pi=l^\pi(y_1,\ldots,y_r)$. □

(1.5) **Proposition.** *If N is a permutation-projective π-module, and $0 \to M_1 \to M_2 \to N \to 0$ is an exact sequence of finitely generated $\mathbf{Z}$-free π-modules, then the fields $l(M_2)^\pi$ and $l(M_1 \oplus N)^\pi$ are isomorphic over l^π.*

Proof. The field $l(M_1)$ is naturally contained in $l(M_2)$. Let $l(M_1)^* \cdot M_2 \subset l(M_2)^*$ be the subgroup generated by $l(M_1)^*$ and M_2. Consider the exact sequence of π-modules

$$0 \to l(M_1)^* \to l(M_1)^* \cdot M_2 \to N \to 0$$

where the map f: $l(M_1)^* \cdot M_2 \to N$ is defined by

$$f(\lambda \cdot m) = (m \bmod M_1) \in N, \quad \text{for } \lambda \in l(M_1)^* \text{ and } m \in M_2.$$

By Hilbert Theorem 90 and (1.2)(c) this exact sequence splits. The resulting π-homomorphism $N \to l(M_2)^*$ easily yields a field isomorphism $l(M_1 \oplus N) \cong l(M_2)$ which respects the action of π, and (1.5) follows. Compare [39, Prop. 1.2.2]. □

(1.6) **Proposition.** *If N is a permutation module over π, and*

$$0 \to M_1 \to M_2 \to N \to 0$$

is an exact sequence of finitely generated $\mathbf{Z}$-free π-modules, then $l(M_2)^\pi$ is rational over $l(M_1)^\pi$.

Proof. From (1.5) we get $l(M_2)^\pi \cong l(M_1 \oplus N)^\pi$, and (1.4), applied to the base field $l(M_1)$ instead of l, says that $l(M_1 \oplus N)^\pi$ is rational over $l(M_1)^\pi$. □

(1.7) **Theorem** [45, 10]. *Let M be a finitely generated $\mathbf{Z}$-free π-module. Then $l(M)^\pi$ is stably rational over l^π if and only if there is an exact sequence of π-modules*

$$0 \to M \to N_2 \to N_1 \to 0$$

in which N_1 and N_2 are finitely generated permutation modules.

Proof. If $0 \to M \to N_2 \to N_1 \to 0$ is an exact sequence as in the theorem, then $l(N_2)^\pi$ is rational over both l^π and $l(M)^\pi$, by (1.6). This proves the "if"-part.

Next suppose $l(M)^\pi$ is stably rational over l^π, so

$$l(M)^\pi(x_1, \ldots, x_s) = l^\pi(y_1, \ldots, y_{r+s})$$

where $\{x_1, \ldots, x_s\}$ is algebraically independent over $l(M)^\pi$ and $\{y_1, \ldots, y_{r+s}\}$ is algebraically independent over l^π. Let π act on

$$l(M)(x_1, \ldots, x_s) = l(M) \otimes_{l(M)^\pi} l(M)^\pi(x_1, \ldots, x_s)$$

via the first factor. Put

$$R_1 = l[M][x_1, \ldots, x_s] \quad \text{and} \quad R_2 = l[y_1, \ldots, y_{r+s}]$$

inside the field $l(M)(x_1, \ldots, x_s)$. By [44, Lemma 8] there are nonzero elements $a_1 \in R_1^\pi$ and $a_2 \in R_2^\pi$ such that $R_1[a_1^{-1}] = R_2[a_2^{-1}]$; call this last ring R. Lemma 7 of [44] tells us that there are exact sequences of π-modules

$$0 \to R_1^* \to R^* \to N_1 \to 0$$

$$0 \to R_2^* \to R^* \to N_2 \to 0$$

in which N_1 and N_2 are finitely generated permutation modules. Replacing R^*, R_1^* and R_2^* by R^*/l^*, R_1^*/l^* and R_2^*/l^* we get

$$0 \to M \to R^*/l^* \to N_1 \to 0$$

$$0 \to 0 \to R^*/l^* \to N_2 \to 0.$$

The theorem follows. □

(1.8) **Corollary.** *Let M be a finitely generated $\mathbf{Z}$-free π-module, and suppose $H^1(\rho, M) = 0$ for every subgroup $\rho \subset \pi$. Then $l(M)^\pi$ is stably rational over l^π if and only if $M \oplus N_1 \cong N_2$ for certain finitely generated permutation modules N_1 and N_2.*

Proof. (1.7) and (1.2)(c). □

2. A Special Case

In this section π is a finite *abelian* group, and l is a field on which π acts faithfully as a group of field automorphisms. If $\pi'' \subset \pi$ is a subgroup, then we call $\pi' = \pi/\pi''$ a *factor group* of π. The canonical map $\pi \to \pi'$ allows us to view every π'-module as a π-module in a natural way.

Let ρ be a *cyclic* factor group of π. Then there is a natural surjective ring homomorphism $\mathbf{Z}[\pi] \to \mathbf{Z}(\rho)$ (see the introduction for the definition of $\mathbf{Z}(\rho)$), which allows us to view every $\mathbf{Z}(\rho)$-module as a π-module. If M is a π-module, we put

$$F_{\pi,\rho}(M) = (M \otimes_\pi \mathbf{Z}(\rho))/\{\text{elements of finite additive order}\}.$$

Then $F_{\pi,\rho}$ is a functor from the category of π-modules to the category of torsion free $\mathbf{Z}(\rho)$-modules, left adjoint to an obvious functor the other way.

(2.1) **Proposition.** *Let $S(\pi)$ denote the set of cyclic factor groups of π, and let π' be a factor group of π. Then there is a natural inclusion $S(\pi') \subset S(\pi)$, and for every π'-module M we have:*

(i) *if $\rho \in S(\pi')$, then $F_{\pi,\rho}(M) \cong F_{\pi',\rho}(M)$ over $\mathbf{Z}(\rho)$;*

(ii) *if $\rho \in S(\pi)$ but $\rho \notin S(\pi')$, then $F_{\pi,\rho}(M) = 0$.*

Proof. The inclusion $S(\pi') \subset S(\pi)$ is induced by the surjection $\pi \to \pi'$. Assertion (i) is clear from $M \otimes_\pi \mathbf{Z}[\pi'] \cong M$. We prove (ii). Since $\rho \notin S(\pi')$,

we can choose an element $\sigma \in \pi$, which has image 1 in π' while its image σ^* in ρ is $\neq 1$. Then σ acts trivially on M, so

$$(\sigma^* - 1) \cdot (M \otimes_\pi \mathbf{Z}(\rho)) = 0,$$

where $\sigma^* - 1$ is a nonzero element of $\mathbf{Z}(\rho)$. Since $\sigma^* - 1$ divides some positive integer in $\mathbf{Z}(\rho)$, it follows that $M \otimes_\pi \mathbf{Z}(\rho)$ is torsion, so $F_{\pi,\rho}(M) = 0$. □

This proposition says that $F_{\pi,\rho}$ does not depend on π, in a certain sense. From now on we will write F_ρ instead of $F_{\pi,\rho}$.

(2.2) **Proposition.** *Let N be a π-module, and $M \subset N$ a sub-π-module such that N/M is a torsion group. Then $F_\rho(M)$ is isomorphic to the image of M under the natural map $N \to F_\rho(N)$, for every cyclic factor group ρ of π.*

Proof. Let J be the kernel of $\mathbf{Z}[\pi] \to \mathbf{Z}(\rho)$. Then for every π-module P there is a natural surjection $P \to F_\rho(P)$ with kernel

$$\{p \in P \mid \exists k \in \mathbf{Z},\ k \neq 0:\ k \cdot p \in J \cdot P\}.$$

Since N/M is torsion, we have

$$\{m \in M \mid \exists k \in \mathbf{Z},\ k \neq 0:\ k \cdot m \in J \cdot M\} = M \cap \{n \in N \mid \exists k \in \mathbf{Z},\ k \neq 0:\ k \cdot n \in J \cdot N\},$$

and (2.2) follows. □

(2.3) **Proposition.** *If N is a permutation module over π, then $F_\rho(N)$ is $\mathbf{Z}(\rho)$-free for every cyclic factor group ρ of π.*

Proof. It suffices to treat the case $N = \mathbf{Z}[\pi']$, where π' is a factor group of π. Then $F_\rho(N) \cong \mathbf{Z}(\rho)$ or $F_\rho(N) = 0$, by (2.1). □

(2.4) **Theorem.** *Let π be a finite cyclic group, and M a finitely generated projective π-module. Then the fields $l(M)^\pi$ and $l(\bigoplus_\rho F_\rho(M))^\pi$ are isomorphic over l^π; here ρ ranges over the set of cyclic factor groups of π.*

The proof of this theorem is given at the end of this section. An analogous result is given in [10]. Compare also [11].

(2.5) **Corollary.** *Let π be a finite abelian group, and let M be a finitely generated π-module of the form*

$$M = \bigoplus_{\pi'} M_{\pi'},$$

where each $M_{\pi'}$ is a projective π'-module, and where π' ranges over the set of cyclic factor groups of π. Then

$$l(M)^\pi \cong l\Big(\bigoplus_\rho F_\rho(M)\Big)^\pi \qquad \text{over } l^\pi,$$

with ρ ranging over the set of cyclic factor groups of π.

Proof. Let $\pi' = \pi/\pi''$ be a cyclic factor group of π. Applying (2.4) to the cyclic group π', the module $M_{\pi'}$ and the field $l^{\pi''}$, we find, using (2.1):

$$l(M_{\pi'})^{\pi} \cong l\Big(\bigoplus_{\rho} F_{\rho}(M_{\pi'})\Big)^{\pi} \qquad \text{over } l^{\pi}.$$

Tensoring with l over l^{π} gives an l-isomorphism

$$l(M_{\pi'}) \cong l\Big(\bigoplus_{\rho} F_{\rho}(M_{\pi'})\Big)$$

which respects the action of π. Combination yields an l-isomorphism

$$l(M) \cong l\Big(\bigoplus_{\rho} F_{\rho}(M)\Big)$$

which respects the action of π, and (2.5) follows. □

(2.6) **Theorem.** *Let π be a finite abelian group, and let M be a finitely generated π-module of the form*

$$M = \bigoplus_{\pi'} M_{\pi'},$$

where each $M_{\pi'}$ is a projective π'-module, and where π' ranges over the set of cyclic factor groups of π. Then the following three statements are equivalent:

(a) *the field $l(M)^{\pi}$ is rational over l^{π};*

(b) *the field $l(M)^{\pi}$ is stably rational over l^{π};*

(c) *for every cyclic factor group ρ of π, the $\mathbf{Z}(\rho)$-module $F_{\rho}(M)$ is free.*

Proof. The implication (a) ⇒ (b) is obvious.

(b) ⇒ (c). Since M is permutation-projective over π, we can apply (1.8). Using (2.3) we find that for every cyclic factor group ρ of π there exist finitely generated free $\mathbf{Z}(\rho)$-modules P_1 and P_2 such that $F_{\rho}(M) \oplus P_1 \cong P_2$ over $\mathbf{Z}(\rho)$. Since $\mathbf{Z}(\rho)$ is a Dedekind domain, this implies that $F_{\rho}(M)$ is $\mathbf{Z}(\rho)$-free, as required.

(c) ⇒ (a). Let $r(\pi')$ be the rank of $M_{\pi'}$ over $\mathbf{Z}[\pi']$, and put

$$N = \bigoplus_{\pi'} \mathbf{Z}[\pi']^{r(\pi')}.$$

Let ρ be a cyclic factor group of π. Then the $\mathbf{Z}(\rho)$-modules $F_{\rho}(M)$ and $F_{\rho}(N)$ are isomorphic; in fact, by assumption and by (2.3), they are both $\mathbf{Z}(\rho)$-free of rank $\sum_{\pi'} r(\pi')$, the sum ranging over those cyclic factor groups π' of π for which ρ is a factor group of π'. Therefore

$$\bigoplus_{\rho} F_{\rho}(M) \cong \bigoplus_{\rho} F_{\rho}(N),$$

so $l(M)^\pi \cong l(N)^\pi$ by a twofold application of (2.5). But $l(N)^\pi$ is rational over l^π, by (1.4), and (a) follows. □

The remainder of this section is devoted to the proof of Theorem (2.4). We assume that π is a cyclic group of order m with generator τ. The set of positive divisors of m is denoted by $E(m)$. For $d \in E(m)$, the unique factor group of π of order d is denoted by π_d. If $C \subset E(m)$ is a subset, then we write $\Phi_C = \prod_{d \in C} \Phi_d$; for example, $\Phi_{E(m)} = X^m - 1$. If M is a π-module and $C \subset E(m)$, we write $M_C = M/\Phi_C(\tau)\, M$.

(2.7) **Lemma.** *If M is π-projective, and $d \in E(m)$, then $M_{E(d)}$ is permutation-projective over π.*

Proof. The module $M_{E(d)} \cong M \otimes_\pi \mathbf{Z}[\pi_d]$ is π_d-projective, hence a direct summand of $\mathbf{Z}[\pi_d]^t$ for some $t \in \mathbf{Z}$, $t \geqq 0$. □

(2.8) **Lemma.** *Let M be π-projective, and $C, C' \subset E(m)$ disjoint subsets. Then there is an exact sequence of π-modules*

$$0 \to M_C \to M_{C \cup C'} \to M_{C'} \to 0.$$

Proof. The map $M_{C \cup C'} \to M_{C'}$ is the natural one, and the map $M_C \to M_{C \cup C'}$ is induced by multiplication with $\Phi_{C'}(\tau)$. For $M = \mathbf{Z}[\pi]$, exactness of the resulting sequence is easily checked. The general case follows since everything preserves direct sums. □

Let $G(m)$ denote the set of all equivalence relations on $E(m)$. For $u \in G(m)$, we denote by $[u]$ the set of non-empty equivalence classes of u. Let $S(m) \subset G(m) \times G(m)$ be the set of $(u, v) \in G(m) \times G(m)$ for which

(2.9) there exist $d \in E(m)$ and $D \in [u]$, such that $E(d) \subset D$, $E(d) \neq D$ and $[v] = \{E(d), D \smallsetminus E(d), C \mid C \in [u], C \neq D\}$.

(2.10) **Lemma.** *The graph $(G(m), S(m))$ is connected.*

Proof. The statement means that for all $u, v \in G(m)$ there is a finite sequence $(u_j)_{j=0}^a$ of elements of $G(m)$ such that $u_0 = u$ and $u_a = v$, and such that for every j with $0 \leqq j < a$, either $(u_j, u_{j+1}) \in S(m)$ or $(u_{j+1}, u_j) \in S(m)$. We call such a sequence a "path from u to v".

Let the two "trivial" equivalence relations $i(m), w(m) \in G(m)$ be defined by

$$[i(m)] = \{\{d\} \mid d \in E(m)\} \quad \text{and} \quad [w(m)] = \{E(m)\}.$$

Clearly, it is sufficient to show that for each $u \in G(m)$ there is a path from u to $i(m)$. This is done by induction on m. For fixed m, we use induction on $n(u) = |E(m)| - |[u]|$.

If $n(u) = 0$ then $u = i(m)$ and obviously the required path exists. Suppose that $n(u) > 0$, and let e be the smallest element of $E(m)$ for which there exists a class $D \in [u]$ with $e \in D$ and $|D| > 1$. Clearly $e < m$. Therefore,

the induction hypothesis on m may be applied, yielding a path $(v_j)_{j=0}^{b}$ from $i(e)$ to $w(e)$ in the graph $(G(e), S(e))$. For $0 \leqq j \leqq b$, let $D_j \in [v_j]$ be such that $e \in D_j$. Define $u_j \in G(m)$, for $0 \leqq j \leqq 2b+1$, by

$$[u_j] = \{C \in [u] \mid C \cap E(e) = \emptyset\} \cup \{D \cup D_j\} \cup ([v_j] \setminus \{D_j\})$$

if $0 \leqq j \leqq b$, and

$$[u_j] = \{C \in [u] \mid C \cap E(e) = \emptyset\} \cup \{D \setminus \{e\}\} \cup [v_{2b+1-j}]$$

if $b+1 \leqq j \leqq 2b+1$. We leave it to the reader to check that $(u_j)_{j=0}^{2b+1}$ is a well defined path from $u = u_0$ to u_{2b+1}, and that

$$[u_{2b+1}] = \{D \setminus \{e\}, \{e\}\} \cup ([u] \setminus \{D\}).$$

It follows that $n(u_{2b+1}) = n(u) - 1$, and the induction hypothesis on $n(u)$ yields a path from u_{2b+1} to $i(m)$. Combination yields a path from u to $i(m)$. This proves the lemma. □

Let l and M be as in (2.4). For $u \in G(m)$ we put $M(u) = \bigoplus_{C \in [u]} M_C$.

(2.11) **Lemma.** *Let $u, v \in G(m)$. Then $l(M(u))^\pi \cong l(M(v))^\pi$ over l^π.*

Proof. By Lemma (2.10) we may assume that (2.9) holds. Then by (2.8) there is an exact sequence of π-modules

$$0 \to M_{D \setminus E(d)} \to M_D \to M_{E(d)} \to 0.$$

Adding a summand

$$N = \bigoplus_{C \in [u],\, C \neq D} M_C$$

yields an exact sequence

$$0 \to N \oplus M_{D \setminus E(d)} \to N \oplus M_D \to M_{E(d)} \to 0.$$

These modules are $\mathbf{Z}$-free, since M is projective. Using (2.7) and (1.5) we get an isomorphism of fields

$$l(N \oplus M_{D \setminus E(d)} \oplus M_{E(d)})^\pi \cong l(N \oplus M_D)^\pi$$

over l^π. Because of (2.9) this is exactly the same as $l(M(u))^\pi \cong l(M(v))^\pi$ over l^π. □

Proof of (2.4). Let $i(m), w(m) \in G(m)$ be as in the proof of (2.10). Then

$$M(i(m)) = \bigoplus_{d \mid m} M/\Phi_d(\tau)\, M \cong \bigoplus_{\rho} F_\rho(M),$$

$$M(w(m)) = M/(\tau^m - 1)\, M = M.$$

So (2.4) follows from (2.11) if we put $u = i(m)$ and $v = w(m)$. □

Remark. Theorem (2.4) can be generalized to the case M is permutation-projective over π. The only modification in the proof is that for $C \subset E(m)$ the module M_C has to be redefined as follows:

$$M_C = M/\{x \in M \mid \exists k \in \mathbf{Z},\ k \neq 0:\ k \cdot x \in \Phi_C(\tau) \cdot M\},$$

and that C' in (2.8) must be equal to $E(d)$, for some $d \in E(m)$.

3. The Modules I_q and J_q

Let p be a prime number, and let $q = p^s$ be a power of p, with $s \geqq 1$. In this section l denotes a field of characteristic $\neq p$ which contains a primitive q-th root of unity ζ_q, and π is a finite abelian group of automorphisms of l. We put $k = l^\pi$ and $\pi(q) = \{\sigma \in \pi \mid \sigma(\zeta_q) = \zeta_q\} = \mathrm{Gal}(l/k(\zeta_q))$. Let $\rho(q) = \mathrm{Gal}(k(\zeta_q)/k) = \pi/\pi(q)$. The map $\pi \to (\mathbf{Z}/q\mathbf{Z})^*$, which sends τ to $(t \bmod q)$ if $\tau(\zeta_q) = \zeta_q^t$, gives rise to an injective group homomorphism $\phi_q\colon \rho(q) \to (\mathbf{Z}/q\mathbf{Z})^*$. This map makes $\mathbf{Z}/q\mathbf{Z}$ into a $\rho(q)$-module and hence into a π-module.

We consider first the case when $\rho(q)$ is non-cyclic, and afterwards the case when $\rho(q)$ is cyclic.

So assume that $\rho(q)$ is non-cyclic. Then q is divisible by 8. Put $C(q) = (\mathbf{Z}/q\mathbf{Z}) \smallsetminus \{0\}$, and let $\mathbf{Z}^{C(q)}$ be a free abelian group of rank $q-1$ with $\mathbf{Z}$-basis $\{e_c \mid c \in C(q)\}$. We make $\mathbf{Z}^{C(q)}$ into a $\rho(q)$-module by $\sigma(e_c) = e_{\sigma c}$, for $\sigma \in \rho(q)$ and $c \in C(q)$. Then the group homomorphism $\mathbf{Z}^{C(q)} \to \mathbf{Z}/q\mathbf{Z}$, mapping e_c to c for $c \in C(q)$, is $\rho(q)$-linear, and we call its kernel I_q. So there is an exact sequence of $\rho(q)$-modules

$$0 \to I_q \to \mathbf{Z}^{C(q)} \to \mathbf{Z}/q\mathbf{Z} \to 0.$$

(3.1) **Proposition.** *For every subgroup $\pi' \subset \pi$ we have $H^1(\pi', I_q) = 0$.*

Proof. Obvious from the exact sequence of cohomology. □

(3.2) **Proposition.** *For some subgroup $\pi' \subset \pi$ we have $\hat{H}^{-1}(\pi', I_q) \neq 0$.*

Proof (sketch). Since I_q is torsion free, we may assume $\pi = \rho(q)$. We assumed that π is non-cyclic, so there is a subgroup π' with $\phi_q[\pi'] = \{1, u-1, u+1, -1\} \subset \mathbf{Z}/q\mathbf{Z}$, where $u = \frac{1}{2}q$. We are going to prove $\hat{H}^{-1}(\pi', I_q) \cong \mathbf{Z}/2\mathbf{Z}$.

Put $C = \{1, u-1, u, u+1, -1\} \subset C(q) \subset \mathbf{Z}/q\mathbf{Z}$. Then $\mathbf{Z}^C$ is a sub-π'-module of $\mathbf{Z}^{C(q)}$ in an obvious way, and restricting the map $\mathbf{Z}^{C(q)} \to \mathbf{Z}/q\mathbf{Z}$ to $\mathbf{Z}^C$ we get an exact sequence of π'-modules

$$0 \to M \to \mathbf{Z}^C \to \mathbf{Z}/q\mathbf{Z} \to 0$$

where $M = \mathbf{Z}^C \cap I_q$. The exact sequence of cohomology easily yields $H^1(\pi'', M) = 0$ for all five subgroups $\pi'' \subset \pi'$, and an explicit computation

inside M shows $\hat{H}^{-1}(\pi', M) \cong \mathbf{Z}/2\mathbf{Z}$. By diagram chasing one gets an exact sequence

$$0 \to M \to I_q \to \mathbf{Z}^{C(q)\setminus C} \to 0,$$

which splits by (1.2). Using (1.1) we find $\hat{H}^{-1}(\pi', I_q) \cong \mathbf{Z}/2\mathbf{Z}$, as required. □

For the remainder of this section we assume $\rho(q)$ is cyclic. The ring homomorphism $\mathbf{Z}[\rho(q)] \to \mathbf{Z}/q\mathbf{Z}$ induced by ϕ_q is $\rho(q)$-linear, and we call its kernel J_q. So there is an exact sequence of $\rho(q)$-modules

$$0 \to J_q \to \mathbf{Z}[\rho(q)] \to \mathbf{Z}/q\mathbf{Z} \to 0.$$

(3.3) **Proposition** [10]. *Let $\rho(q)$ be cyclic. Then J_q is a projective $\rho(q)$-module except if* (3.4) *holds:*

$$q \equiv 0 \bmod 4 \quad \textit{and} \quad \phi_q[\rho(q)] = \{+1, -1\} \subset (\mathbf{Z}/q\mathbf{Z})^*. \tag{3.4}$$

Proof. Suppose (3.4) does not hold. Let $\rho = \phi_q[\rho(q)] \subset (\mathbf{Z}/q\mathbf{Z})^*$ and $n = |\rho| = |\rho(q)|$. Let $\rho_1 \subset (\mathbf{Z}/pq\mathbf{Z})^*$ be the inverse image of ρ under the canonical map $(\mathbf{Z}/pq\mathbf{Z})^* \to (\mathbf{Z}/q\mathbf{Z})^*$. Then ρ_1 has order np, and we claim that ρ_1 is cyclic.

Suppose, in fact, that ρ_1 is non-cyclic. Then $(\mathbf{Z}/pq\mathbf{Z})^*$ is non-cyclic, so $p=2$ and $q \equiv 0 \bmod 4$. Moreover, $(-1 \bmod pq) \in \rho_1$, so $-1 \in \rho$. But the only cyclic subgroup of $(\mathbf{Z}/q\mathbf{Z})^*$ containing -1 is $\{+1, -1\}$, so $\rho = \{+1, -1\}$. Hence (3.4) holds, contradicting our assumption. We conclude that ρ_1 is cyclic.

Choose $t \in \mathbf{Z}$ such that $(t \bmod pq)$ generates ρ_1. Since $|\rho_1| > n$, we have $t^n \not\equiv 1 \bmod pq$. Clearly, $(t \bmod q)$ generates ρ, so $t^n \equiv 1 \bmod q$. Hence $t^n - 1 = a \cdot q$, where a and q are relatively prime.

Let $\tau \in \rho(q)$ be such that $\phi_q(\tau) = (t \bmod q)$. Then τ generates $\rho(q)$, and the $\mathbf{Z}[\rho(q)]$-ideal J_q is generated by $\tau - t$ and q. Denote by M the $\mathbf{Z}[\rho(q)]$-ideal generated by $\tau - t$ and a. Then $J_q + M = \mathbf{Z}[\rho(q)]$, so $J_q \cap M = J_q \cdot M$. Hence we have an exact sequence of $\mathbf{Z}[\rho(q)]$-modules

$$0 \to J_q \cdot M \to J_q \oplus M \to \mathbf{Z}[\rho(q)] \to 0$$

where the map $J_q \oplus M \to \mathbf{Z}[\rho(q)]$ is defined by $(j, m) \mapsto j - m$. The ideal $J_q \cdot M$ is generated by the four elements $\{(\tau - t)^2, a(\tau - t), q(\tau - t), aq\}$ where $aq = t^n - \tau^n$. It follows that $J_q \cdot M = \mathbf{Z}[\rho(q)] \cdot (\tau - t)$ is a free $\mathbf{Z}[\rho(q)]$-module, and since the above sequence splits we find that J_q is $\rho(q)$-projective. □

Remark. If (3.4) holds, then J_q is not projective. In fact, suppose $q \equiv 0 \bmod 4$ and $\rho(q) = \{1, \tau\}$, where $\phi_q(\tau) = -1$. Then J_q has a $\mathbf{Z}$-basis $\{1 + \tau, \frac{1}{2}q - \frac{1}{2}q \cdot \tau\}$, so $J_q \cong \mathbf{Z} \oplus \mathbf{Z}'$; here $\rho(q)$ acts trivially on $\mathbf{Z}$, while the $\rho(q)$-module $\mathbf{Z}'$ has underlying abelian group $\mathbf{Z}$ and $\rho(q)$-action $\tau \cdot m = -m$, for $m \in \mathbf{Z}$.

(3.5) **Proposition.** *Suppose q is a power of 2 and $\rho(q)$ is cyclic. Then $l(J_q)^\pi$ is rational over l^π.*

Proof. Replacing l by $l^{\pi(q)}$ we may assume $\pi=\rho(q)$. Suppose first that (3.4) holds. Then by the above remark $l(J_q)=l(x, y)$, where $\tau(x)=x$ and $\tau(y)=y^{-1}$; here τ denotes the non-trivial element of π. Choose $\alpha\in l$ with $\tau(\alpha)\neq\alpha$. Then $l(x, y)^\pi=l^\pi(x, z)$, where $z=(\alpha y+\tau(\alpha))/(y+1)$. So in this case $l(J_q)^\pi$ is rational over l^π.

Suppose now that (3.4) does not hold. By (3.3), the π-module J_q is projective, so we are in a position to apply (2.6). Hence we need only check that $F_\rho(J_q)$ is $\mathbf{Z}(\rho)$-free for every factor group ρ of π.

So let $\rho\neq\{1\}$ be a factor group of π of order 2^r. Since J_q has index q in $\mathbf{Z}[\pi]$, it follows from (2.2) that $F_\rho(J_q)$ may be considered as a submodule of 2-power index in $F_\rho(\mathbf{Z}[\pi])\cong\mathbf{Z}(\rho)$. But $\mathbf{Z}(\rho)\cong\mathbf{Z}[\zeta_{2^r}]$, and every ideal of 2-power index in $\mathbf{Z}[\zeta_{2^r}]$ is generated by the corresponding power of $1-\zeta_{2^r}$, and is therefore free. It follows that $F_\rho(J_q)$ is $\mathbf{Z}(\rho)$-free, as required. □

If K is a subfield of l which is a cyclic extension of k, then $\mathrm{Gal}(K/k)$ is a cyclic factor group of π, and we will write F_K instead of $F_{\mathrm{Gal}(K/k)}$.

(3.6) **Proposition.** *Suppose q is odd. Let K be an intermediate field $k\subset K\subset l$ such that $\rho_K=\mathrm{Gal}(K/k)$ is cyclic. Let $\mathfrak{a}_K(-)$ be as in the introduction. Then*

$$F_K(J_q)\cong\mathfrak{a}_K(\mathbf{Z}/q\mathbf{Z}) \quad \text{as } \mathbf{Z}(\rho_K)\text{-modules if } K\subset k(\zeta_q),$$
$$F_K(J_q)=0 \quad \text{if } K\not\subset k(\zeta_q).$$

This is proved after the proof of (3.7).

(3.7) **Lemma.** *Let $q=p^s$ be odd, let τ be a generator of $\rho(q)=\pi/\pi(q)=\mathrm{Gal}(k(\zeta_q)/k)$, and choose $t\in\mathbf{Z}$ such that $\tau(\zeta_q)=\zeta_q^t$. We denote the order of $(t \bmod p)\in(\mathbf{Z}/p\mathbf{Z})^*$ by f, and we put $p^r=\mathrm{g.c.d.}(q, t^f-1)$; here $r\in\mathbf{Z}$ and $1\leqq r\leqq s$.*

In this situation, any intermediate field $k\subset K\subset k(\zeta_q)$ is uniquely determined by its degree $[K:k]$ over k. Moreover, if K is such a field, then $\rho_K=\mathrm{Gal}(K/k)$ is a cyclic group, generated by the image τ_K of τ in ρ_K. We have:

(i) *if $K=k(\zeta_p)$, then $K=k(\zeta_{p^i})$ for all $1\leqq i\leqq r$, the degree $[K:k]$ equals f, and $F_K(J_q)$ is, as a $\mathbf{Z}(\rho_K)$-module, isomorphic to the r-th ideal power of the $\mathbf{Z}(\rho_K)$-ideal generated by p and $\tau_K-t\in\mathbf{Z}(\rho_K)$;*

(ii) *if $K=k(\zeta_{p^i})$ with $r<i\leqq s$, then $[K:k]=f\cdot p^{i-r}$, and $F_K(J_q)$ is, as a $\mathbf{Z}(\rho_K)$-module, isomorphic to the $\mathbf{Z}(\rho_K)$-ideal generated by p and τ_K-t;*

(iii) *for all other $K\subset k(\zeta_q)$, we have $F_K(J_q)\cong\mathbf{Z}(\rho_K)$ as $\mathbf{Z}(\rho_K)$-modules.*

(3.8) **Lemma.** *For $m \in \mathbf{Z}$, let* $\operatorname{ord}(m)$ *denote the number of factors p in m. Let t and f be as in* (3.7). *Then:*

(i) $\operatorname{ord}(\Phi_f(t)) = \operatorname{ord}(t^f - 1) > 0$,
$\operatorname{ord}(\Phi_{fp^i}(t)) = 1$ *for all* $i \in \mathbf{Z}$, $i > 0$,
$\operatorname{ord}(\Phi_d(t)) = 0$ *for all other* $d \in \mathbf{Z}$, $d > 0$.

(ii) $\operatorname{ord}(t^m - 1) = 0$ *if* $m \in \mathbf{Z}$, $m > 0$ *and* $m \not\equiv 0 \bmod f$,
$\operatorname{ord}(t^m - 1) = \operatorname{ord}(t^f - 1) + \operatorname{ord}(m)$ *if* $m \in \mathbf{Z}$, $m > 0$ *and* $m \equiv 0 \bmod f$.

Proof of (3.8). See [1, Lemma 1]. □

Proof of (3.7). Since $k(\zeta_q)$ is a cyclic extension of k, it is clear that an intermediate field K is determined by its degree over k, and that ρ_K is generated by the image of τ.

Let $1 \leqq i \leqq s$. By Galois theory, $[k(\zeta_{p^i}):k]$ is the smallest positive integer m for which $\tau^m(\zeta_{p^i}) = \zeta_{p^i}$, i.e., for which $t^m - 1 \equiv 0 \bmod p^i$. From (3.8)(ii) it follows then that $[k(\zeta_{p^i}):k] = f$ if $1 \leqq i \leqq r$, and $[k(\zeta_{p^i}):k] = f \cdot p^{i-r}$ if $r < i \leqq s$. This proves the statements concerning the degrees $[k(\zeta_{p^i}):k]$. In particular, $[k(\zeta_q):k] = f \cdot p^{s-r}$.

Now let $k \subset K \subset k(\zeta_q)$ be such that $[K:k] = d$, where $d \mid f \cdot p^{s-r}$. Tensoring the exact sequence defining J_q with $\mathbf{Z}(\rho_K)$ over $\mathbf{Z}[\rho(q)]$, we find an exact sequence of $\mathbf{Z}(\rho_K)$-modules

$$J_q \otimes_{\rho(q)} \mathbf{Z}(\rho_K) \to \mathbf{Z}[\rho(q)] \otimes_{\rho(q)} \mathbf{Z}(\rho_K) \to (\mathbf{Z}/q\mathbf{Z}) \otimes_{\rho(q)} \mathbf{Z}(\rho_K) \to 0.$$

Since J_q is projective, the first two modules in this sequence are $F_K(J_q)$ and $F_K(\mathbf{Z}[\rho(q)]) \cong \mathbf{Z}(\rho_K)$, and the first arrow is injective by (2.2). Using $\mathbf{Z}(\rho_K) = \mathbf{Z}[\rho(q)]/\Phi_d(\tau)\,\mathbf{Z}[\rho(q)]$ we find for the cokernel:

$$\begin{aligned}(\mathbf{Z}/q\mathbf{Z}) \otimes_{\rho(q)} \mathbf{Z}(\rho_K) &\cong (\mathbf{Z}/q\mathbf{Z})/\Phi_d(\tau) \cdot (\mathbf{Z}/q\mathbf{Z}) \\ &= \mathbf{Z}/(q \cdot \mathbf{Z} + \Phi_d(t) \cdot \mathbf{Z})\end{aligned}$$

since τ acts on $\mathbf{Z}/q\mathbf{Z}$ as multiplication by t.

Summarizing, we have an exact sequence of $\mathbf{Z}(\rho_K)$-modules

$$0 \to F_K(J_q) \to \mathbf{Z}(\rho_K) \to \mathbf{Z}/(q \cdot \mathbf{Z} + \Phi_d(t) \cdot \mathbf{Z}) \to 0$$

where the map $\mathbf{Z}(\rho_K) \to \mathbf{Z}/(q \cdot \mathbf{Z} + \Phi_d(t) \cdot \mathbf{Z})$ sends τ_K to the residue class of t.

In case (iii) we have g.c.d.$(q, \Phi_d(t)) = 1$, by (3.8)(i), so $F_K(J_q)$ is isomorphic to $\mathbf{Z}(\rho_K)$. In case (ii), we have g.c.d.$(q, \Phi_d(t)) = p$, by (3.8)(i), so $F_K(J_q)$ is isomorphic to $(p, \tau_K - t) \subset \mathbf{Z}(\rho_K)$. Finally, in case (i) we have g.c.d.$(q, \Phi_d(t)) = p^r$, so $\mathbf{Z}(\rho_K)/F_K(J_q) \cong \mathbf{Z}/p^r\mathbf{Z}$ is a local ring. Therefore $F_K(J_q)$ is an ideal power of $(p, \tau_K - t)$, and computing norms we find that the exponent has to be r. □

Proof of (3.6). For $K \not\subset k(\zeta_q)$ we have $F_K(J_q)=0$ by (2.1). Therefore it suffices to consider subfields $K \subset k(\zeta_q)$. These fields are described in (3.7), and for each of them $F_K(J_q)$ is computed. Comparing the outcome with the definition of $\mathfrak{a}_K(\mathbf{Z}/q\mathbf{Z})$ (see introduction) one finds that $F_K(J_q) \cong \mathfrak{a}_K(\mathbf{Z}/q\mathbf{Z})$, as required. □

4. A Reduction

Let k be a field, and A a finite abelian group. The field k_A has been defined in the introduction. We write $A \cong P \oplus B$, such that $|B| \not\equiv 0 \bmod \mathrm{char}(k)$ while $|P|$ is a power of $\mathrm{char}(k)$.

(4.1) **Proposition.** *The field k_A is k-isomorphic to a rational field extension of k_B.*

Before proving (4.1) we state two lemmas.

(4.2) **Lemma.** *Let $K_0 \subset K_1 \subset \cdots \subset K_d$ be a chain of fields of characteristic $p \neq 0$, such that for each i with $1 \leqq i \leqq d$ there is an element $u_i \in K_i$ such that $K_i = K_{i-1}(u_i)$. Let P be a finite p-group of field automorphisms of K_d such that*

(i) *the action of P on K_0 is trivial;*

(ii) *$\sigma(u_i) - u_i \in K_{i-1}$ for all $\sigma \in P$ and $1 \leqq i \leqq d$.*

Then $K_d^P = K_0(z_1, \ldots, z_d)$ for some $z_1, \ldots, z_d \in K_d$.

Proof of (4.2). This lemma is Satz 2 of [16]. For a short proof, see [33]. □

(4.3) **Lemma.** *Let K be a field of characteristic $p \neq 0$, and let P be a finite p-group. Let M be a nonzero $K[P]$-module. Then $M^P \neq 0$.*

Proof. See [42, Ch. IX, Th. 2; 6, Ch. IV, § 9; 33]. □

Proof of (4.1). Put $p = \mathrm{char}(k)$. Clearly we may assume $p \neq 0$.

We denote by V the k-vector space inside $k(\{x_g | g \in A\})$ generated by $\{x_g | g \in A\}$. Clearly, V is a $k[A]$-module isomorphic to the left module $k[A]$. Let $W \subset V$ be the subspace $W = V^P$. This is a $k[B]$-module isomorphic to $k[B]$. Therefore, to prove (4.1) it suffices to show that $k(V)^A$ is rational over $k(W)^B$; here $k(W)$ denotes the field generated by k and W inside $k(V) = k(\{x_g | g \in A\})$. The codimension of W in V is denoted by d; we have $d = |A| - |B|$.

By U we denote the $k(W)$-vector space spanned by V inside $k(V)$. It is easy to see that U has dimension $d+1$ over $k(W)$, that $1 \in U$, and that B acts semilinearly on U. Put $T = U^B$. Then from (1.3) it follows that T is a $(d+1)$-dimensional vector space over $k(W)^B$ with $1 \in T$.

The definition of T implies $\sigma T = T$ for $\sigma \in P$, so T is a $k(W)^B[P]$-module. We choose a sequence of $k(W)^B[P]$-submodules Y_i of T, for

$0 \leqq i \leqq d$, such that $Y_0 = k(W)^B \cdot 1$ and such that for each i with $1 \leqq i \leqq d$ we have:

$$Y_{i-1} \subset Y_i, \quad \text{and} \quad Y_i/Y_{i-1} \text{ is a one-dimensional vector space over } k(W)^B \text{ on which } P \text{ acts trivially.}$$

Such a sequence $(Y_i)_{i=0}^d$ is easily constructed by induction on i: just apply (4.3) to $M = T/Y_{i-1}$ to find Y_i. Of course, $Y_d = T$.

Let $u_i \in Y_i$ be such that Y_i as a $k(W)^B$-vector space is generated by Y_{i-1} and u_i, for $1 \leqq i \leqq d$. Let K_i be the field generated by $k(W)^B$ and Y_i, for $0 \leqq i \leqq d$. Then $K_0 = k(W)^B$ and we claim

$$K_d = k(V)^B. \tag{4.4}$$

Assume (4.4) for a moment. The conditions of (4.2) are satisfied, by construction, so

$$K_d^P = K_0(z_1, \ldots, z_d)$$

for some $z_1, \ldots, z_d \in K_d$, or, what is the same,

$$k(V)^A = (k(V)^B)^P = k(W)^B(z_1, \ldots, z_d).$$

Counting transcendence degrees we conclude that $k(V)^A$ is rational over $k(W)^B$, as required.

It remains to prove (4.4). By definition,

$$K_d = k(W)^B(T) = k(W)^B(U^B),$$

so the inclusion $K_d \subset k(V)^B$ is obvious. We prove equality by a degree calculation.

Using (1.3) we choose a B-invariant $k(W)$-basis $\{b_0, \ldots, b_d\}$ for U. Then $\{b_0, \ldots, b_d\}$ is a $k(W)^B$-basis for U^B so

$$K_d = k(W)^B(b_0, \ldots, b_d)$$

while

$$k(V) = k(W)(U) = k(W)(b_0, \ldots, b_d).$$

Therefore

$$[k(V):K_d] \leqq [k(W):k(W)^B] = |B|,$$

and since

$$[k(V):k(V)^B] = |B|$$

it follows that $K_d = k(V)^B$. This completes the proof of (4.1). □

5. Proof of the Main Theorem

Let k be a field and A a finite abelian group. We write $A \cong P \oplus B$ as in the preceding section. By e we denote the exponent of B, and we put $l = k(\zeta_e)$. The Galois group of l over k is called π. As is well known,

the character group $D=\mathrm{Hom}(B, l^*)$ is, as an abelian group, isomorphic to B (non-canonically). We make D into a π-module by $(\sigma d)(g)=\sigma(d(g))$ for $\sigma\in\pi$, $d\in D$ and $g\in B$. Let $\mathbf{Z}^D$ be a free abelian group with $\{e_d \mid d\in D\}$ as a $\mathbf{Z}$-basis, and make $\mathbf{Z}^D$ into a permutation module over π by $\sigma e_d = e_{\sigma d}$, for $\sigma\in\pi$ and $d\in D$. The group homomorphism $\mathbf{Z}^D\to D$ sending e_d to d, for $d\in D$, is π-linear, and we call its kernel J. So we have an exact sequence of π-modules

$$0\to J\to \mathbf{Z}^D\to D\to 0.$$

(5.1) **Proposition** [12, 31]. *The fields k_B and $l(J)^\pi$ are isomorphic over $k=l^\pi$.*

Proof. Let $l(x)=l(\{x_g \mid g\in B\})$ and $k(x)=k(\{x_g \mid g\in B\})$. First we describe $l_B=l(x)^B$.

For $d\in D$, let

$$y_d=\Big(\sum_{g\in B} d(g)^{-1}\cdot x_g\Big)\in l(x).$$

Then $l(x)=l(\{y_d \mid d\in D\})$, and the action of B on $l(\{y_d \mid d\in D\})$ is given by

$$g(y_d)=d(g)\cdot y_d, \quad \text{for } g\in B \text{ and } d\in D.$$

Let $F\subset l(x)^*$ be the multiplicative subgroup generated by $\{y_d \mid d\in D\}$. Clearly, F is $\mathbf{Z}$-free of rank $|D|=|B|$. Define the homomorphism $\phi\colon F\to D$ by sending y_d to d, for $d\in D$. Then

$$g(y)=\phi(y)(g)\cdot y \quad \text{for } y\in F \text{ and } g\in B.$$

So if $y\in\ker(\phi)$ then $g(y)=y$ for all $y\in B$, i.e. $y\in l_B$. This means

$$l(\ker(\phi))\subset l_B\subset l(x)=l(F).$$

The index of $\ker(\phi)$ in F equals $|D|$. Therefore we find, by extracting roots successively:

$$[l(F):l(\ker(\phi))]\leqq|D|.$$

But $[l(F):l_B]=|D|$ by Galois theory, so we conclude $l(\ker(\phi))=l_B$. Since a $\mathbf{Z}$-basis for $\ker(\phi)$ is algebraically independent over l, the field $l(\ker(\phi))$ is isomorphic to the field of fractions of the group ring of $\ker(\phi)$ over l. This removes a slight ambiguity in our notations, cf. Section 1.

Next we let come in k. We let π act on $l(x)\cong l\otimes_k k(x)$ via the first factor. Then the actions of π and B on $l(x)$ commute, so

$$k_B=(l(x)^\pi)^B=(l(x)^B)^\pi=(l_B)^\pi.$$

One easily checks

$$\sigma(y_d)=y_{\sigma d} \quad \text{for } \sigma\in\pi \text{ and } d\in D,$$

so F is a sub-π-module of $l(x)^*$, and $F \cong \mathbf{Z}^D$. The map $\phi: F \to D$ is π-linear, so $\ker(\phi)$ is a sub-π-module of F, and clearly $\ker(\phi) \cong J$. It follows that there is an l-isomorphism of fields $l_B = l(\ker(\phi)) \cong l(J)$ which respects the action of π. Hence there is an isomorphism

$$k_B = (l_B)^\pi \cong l(J)^\pi$$

over $k = l^\pi$, as required. □

We write

$$B \cong \bigoplus_q (\mathbf{Z}/q\mathbf{Z})^{n(q)} \quad \text{(as abelian groups)}$$

with non-negative integers $n(q)$, where q ranges over the set of prime powers >1. We define the π-modules I_1, I_2 and I_3 by

$$I_1 = \bigoplus_{q,\ q \text{ is odd}} J_q^{n(q)},$$

$$I_2 = \bigoplus_{q,\ \rho(q) \text{ is non-cyclic}} I_q^{n(q)},$$

$$I_3 = \bigoplus_{q,\ q \text{ is even, } \rho(q) \text{ is cyclic}} J_q^{n(q)}.$$

(See Section 3 for the definitions of I_q, J_q and $\rho(q)$.) Finally, we put

$$I = I_1 \oplus I_2.$$

(5.2) **Proposition.** *The field $l(J)^\pi$ is l^π-isomorphic to a rational extension of $l(I)^\pi$.*

Proof. By a π-set we mean a set E on which π acts as a group of permutations (the action need not be faithful). The corresponding permutation module is denoted by $\mathbf{Z}^E$. A subset E' of a π-set is called a π-subset if $\sigma(e') \in E'$ for all $\sigma \in \pi$ and $e' \in E'$.

The decomposition

$$B \cong \bigoplus_q (\mathbf{Z}/q\mathbf{Z})^{n(q)}$$

gives rise to a decomposition of π-modules

$$D \cong \bigoplus_q (\mathbf{Z}/q\mathbf{Z})^{n(q)},$$

each direct summand $\mathbf{Z}/q\mathbf{Z}$ being a π-module as described in Section 3.

We first consider a direct summand $\mathbf{Z}/q\mathbf{Z}$ for which $\rho(q)$ is non-cyclic. If $\mathbf{Z}/q\mathbf{Z} \to D$ is an injective π-homomorphism identifying $\mathbf{Z}/q\mathbf{Z}$ with one of the direct summands, then the resulting injection of π-sets $C(q) \subset \mathbf{Z}/q\mathbf{Z} \to D$ (see Section 3 for the definition of $C(q)$) gives rise to a π-linear map $\mathbf{Z}^{C(q)} \to \mathbf{Z}^D$. It is easily checked that the following diagram

with exact rows is then commutative:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & I_q & \longrightarrow & \mathbf{Z}^{C(q)} & \longrightarrow & \mathbf{Z}/q\mathbf{Z} & \longrightarrow & 0 \\ & & & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & J & \longrightarrow & \mathbf{Z}^{D} & \longrightarrow & D & \longrightarrow & 0. \end{array}$$

Analogously, if $\rho(q)$ is cyclic, and we have a π-homomorphism $\mathbf{Z}/q\mathbf{Z} \to D$ which identifies $\mathbf{Z}/q\mathbf{Z}$ with one of the direct summands, then an injective map of π-sets $\rho(q) \to (\mathbf{Z}/q\mathbf{Z})^* \subset \mathbf{Z}/q\mathbf{Z} \to D$ is induced (here the map $\rho(q) \to (\mathbf{Z}/q\mathbf{Z})^*$ is the map ϕ_q defined in Section 3). The resulting π-homomorphism $\mathbf{Z}[\rho(q)] \cong \mathbf{Z}^{\rho(q)} \to \mathbf{Z}^D$ then makes the following diagram with exact rows commutative:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & J_q & \longrightarrow & \mathbf{Z}[\rho(q)] & \longrightarrow & \mathbf{Z}/q\mathbf{Z} & \longrightarrow & 0 \\ & & & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & J & \longrightarrow & \mathbf{Z}^{D} & \longrightarrow & D & \longrightarrow & 0. \end{array}$$

So with each direct summand $\mathbf{Z}/q\mathbf{Z}$ of D we have associated a diagram, and all these diagrams have the same second row. Taking the direct sum of all first rows we find the commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & I_1 \oplus I_2 \oplus I_3 & \longrightarrow & \mathbf{Z}^{E} & \longrightarrow & \bigoplus_q (\mathbf{Z}/q\mathbf{Z})^{n(q)} & \longrightarrow & 0 \\ & & & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & J & \longrightarrow & \mathbf{Z}^{D} & \longrightarrow & D & \longrightarrow & 0 \end{array}$$

where E is some π-set which is a disjoint union of π-sets of the form $C(q)$ and $\rho(q)$, with certain multiplicities. Since $0 \notin C(q) \subset \mathbf{Z}/q\mathbf{Z}$ and $0 \notin \phi_q[\rho(q)] \subset \mathbf{Z}/q\mathbf{Z}$, the images of these π-sets in D do not overlap. This means that E may be considered as a π-subset of D, and that the map $\mathbf{Z}^E \to \mathbf{Z}^D$ is injective and has a cokernel N which is itself a permutation module over π. Since the second vertical arrow in the above diagram is an isomorphism, we get an exact sequence of π-modules

$$0 \to I \oplus I_3 \to J \to N \to 0$$

in which N is a permutation module. From (1.6) it follows that $l(J)^\pi$ is l^π-isomorphic to a rational field extension of $l(I \oplus I_3)^\pi$. Applying (3.5) we find that $l(I \oplus I_3)^\pi$ is rational over $l(I)^\pi$. This proves (5.2). □

(5.3) **Proposition.** *The field k_A is k-isomorphic to a rational field extension of $l(I)^\pi$.*

Proof. Combine (4.1), (5.1) and (5.2). □

(5.4) **Proposition.** *For every subgroup $\pi' \subset \pi$ we have $H^1(\pi', I) = 0$.*

Proof. This follows from (3.1), (3.3) and the definition of I. □

(5.5) **Proposition.** *Let $k \subset K \subset l$ be an intermediate field such that $\rho_K = \mathrm{Gal}(K/k)$ is cyclic. Then $F_K(I_1)$ is $\mathbf{Z}(\rho_K)$-free if and only if the $\mathbf{Z}(\rho_K)$-ideal $\mathfrak{a}_K(A)$ is principal.*

Proof. This is immediate from (3.6), the definitions of I_1 and $\mathfrak{a}_K(A)$, and the following fact on modules over a Dedekind domain: if $\mathfrak{a}_1, \ldots, \mathfrak{a}_t$ are nonzero ideals in a Dedekind domain R, then the direct sum $\mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_t$ is R-free if and only if the ideal product $\mathfrak{a}_1 \ldots \mathfrak{a}_t \subset R$ is a principal ideal [18]. □

(5.6) **Proposition.** *The following three assertions are equivalent:*

(a) *the field $l(I_1)^\pi$ is rational over l^π;*

(b) *the field $l(I_1)^\pi$ is stably rational over l^π;*

(c) *condition* (i) *of the main theorem is satisfied.*

Proof. From the definitions of I_1 and (3.3) it is clear that (2.6) may be applied to $M = I_1$. Therefore it suffices to prove that condition (c) of (2.6), with $M = I_1$, is equivalent to condition (i) of the main theorem. But this is precisely (5.5). □

Proof of the Main Theorem. First suppose k_A is rational over k. Then $l(I)^\pi$ is stably rational over k, by (5.3). Using (5.4) and (1.8) we find $I \oplus N_1 \cong N_2$ for some permutation modules N_1 and N_2 over π. From (1.1) and (3.2) we conclude that $n(q) = 0$ if $\rho(q)$ is non-cyclic, that is, we have proved (ii) of the main theorem. It follows that $I = I_1$, and applying (5.6) we find that (i) is also satisfied.

Secondly, assume that (i) and (ii) of the main theorem hold. Then $I = I_1$ and (5.6) tells us that $l(I)^\pi$ is rational over $l^\pi = k$. Application of (5.3) concludes the proof. □

(5.7) *Remark.* Note that the proof implies: if k_A is stably rational over k, then k_A is rational over k, for abelian A.

6. Supplementary Results

Two extension fields K and L of a field k are called *stably isomorphic* over k if there exist rational field extensions $K \subset K'$ and $L \subset L'$ of finite transcendence degree, such that K' and L' are k-isomorphic.

Let k be a field, and A and A' finite abelian groups. Write

$$A' \cong P' \oplus B', \qquad B' \cong \bigoplus_q (\mathbf{Z}/q\mathbf{Z})^{n'(q)}$$

just as we did for A in Sections 4 and 5.

(6.1) **Theorem.** *Let k be a field, and A and A' finite abelian groups. Then k_A and $k_{A'}$ are stably isomorphic over k if and only if the following two conditions are satisfied:*

(i) *for every intermediate field $k \subset K \subset k_{\mathrm{cycl}}$ for which* (0.1) *holds, the $\mathbf{Z}(\rho_K)$-ideals $\mathfrak{a}_K(A)$ and $\mathfrak{a}_K(A')$ are in the same ideal class;*

(ii) *if $\mathrm{char}(k) \neq 2$, then $n(q) = n'(q)$ for every power of two $q = 2^s$ for which the Galois group of $k(\zeta_q)$ over k is non-cyclic.*

Proof. Analogous to the proof of the main theorem. □

Following Burnside, we consider a generalization of the problem posed in the introduction. Let k be a field, A a finite group, and V a finitely generated faithful $k[A]$-module. The symmetric algebra of V over k is denoted by $S_k(V)$. The field of fractions $k(V)$ of $S_k(V)$ is rational over k of transcendence degree $\dim_k(V)$, and the A-action on V induces an action of A on $k(V)$ as a group of field automorphisms over k. We ask under which conditions $k(V)^A$ is rational over k. If V has a k-basis which is permuted by A, this is the question of the introduction. For A abelian and $V = k[A]$, as $k[A]$-module, the answer is given by the main theorem. Theorem (6.4) below gives a partial solution for abelian A.

(6.2) **Proposition.** *Let V be a finitely generated faithful $k[A]$-module, and $W \subset V$ a faithful $k[A]$-submodule. Then $k(V)^A$ is rational over $k(W)^A$.*

Proof. This follows easily from (1.3). Compare [33]. □

(6.3) **Proposition.** *Suppose $A \cong P \oplus B$, where $|P|$ is a power of $\mathrm{char}(k)$ and $|B| \not\equiv 0 \bmod \mathrm{char}(k)$. Let V be a finitely generated faithful $k[A]$-module. Then V^P is a faithful $k[B]$-module, and $k(V)^A$ is rational over $k(V^P)^B$.*

Proof. We show that V^P is a faithful $k[B]$-module. Let $b \in B$, with $b \neq 1$. Then $(b-1)V$ is a nonzero P-module, so by (4.3) there is a nonzero element $w \in (b-1)V \cap V^P$, say $w = (b-1)v$. Let m be the order of b. Then $b \cdot w = w$ would imply $m \cdot w = (b^{m-1} + \cdots + b + 1)w = (b^m - 1)v = 0$, but $m \cdot 1 \neq 0$ in k, so $w = 0$, contradiction. Hence $b \cdot w \neq w$, and V^P is faithful over $k[B]$. The proof that $k(V)^A$ is rational over $k(V^P)^B$ follows exactly the same lines as the proof of (4.1). □

(6.4) **Theorem.** *Let k be a field, A a finite abelian group, and V a finitely generated faithful $k[A]$-module. Then $k(V)^A$ is stably rational over k if and only if k_A is rational over k. Moreover, if $\dim_k(V) \geqq |A|$, then $k(V)^A$ is rational over k if and only if $k(V)^A$ is stably rational over k.*

Proof. Write $A = P \oplus B$ as in (6.3). Combination of (6.3) and (6.2) (with $W = V^P$) shows that $k(V)^A$ and $k(V)^B$ are k-isomorphic, so it suffices to do the case $A = B$, i.e. $|A| \not\equiv 0 \bmod \mathrm{char}(k)$.

By (6.2), the field $k(V \oplus k[A])^A$ is rational over both $k(V)^A$ and k_A, so $k(V)^A$ and k_A are stably isomorphic over k. Also, by (5.7), the field k_A is rational over k if and only if it is stably rational over k. We conclude that $k(V)^A$ is stably rational over k if and only if k_A is rational over k.

Finally, assume $\dim_k(V) \geqq |A|$. We may write $V \cong \bigoplus_{i=1}^{t} V_i^{n(i)}$ over $k[A]$, where each V_i is an irreducible $k[A]$-module, $n(i)$ is a positive integer, and V_i and V_j are non-isomorphic for $i \neq j$. Put $W = \bigoplus_{i=1}^{t} V_i$. Then W is a faithful $k[A]$-module, and there are injective $k[A]$-homomorphisms $W \to V$ and $W \to k[A]$. Therefore k_A and $k(V)^A$ are both rational over $k(W)^A$. Since $\dim_k(V) \geqq |A|$, it follows that $k(V)^A$ is k-isomorphic to a rational extension of k_A. Application of (5.7) completes the proof. □

The argument in our solution of the case $V = k[A]$ which does not carry over to the general case is the proof of (5.2). But by exercising a little more care one can show that the bound $|A|$ in (6.4) may be replaced by $|A| - |\Phi(A)|$, where $\Phi(A)$ denotes the Frattini subgroup of A (i.e., the intersection of the maximal subgroups of A).

7. Corollaries

We note some consequences of our main theorem. Some of them appeared already in [10, 48].

(7.1) **Corollary.** *Let k be a field and p a prime number. The splitting field of $X^p - 1$ over k is denoted by l, and $d = [l:k]$. Then $k_{\mathbf{Z}/p\mathbf{Z}}$ is rational over k if and only if the ring $\mathbf{Z}[\zeta_d]$ contains a principal ideal of index p.*

Proof. We may assume $2 \neq p \neq \mathrm{char}(k)$. By the main theorem, $k_{\mathbf{Z}/p\mathbf{Z}}$ is rational over k if and only if $\mathfrak{a}_l(\mathbf{Z}/p\mathbf{Z})$ is a principal ideal of $\mathbf{Z}(\rho_l)$. This implies (7.1), since $\mathfrak{a}_l(\mathbf{Z}/p\mathbf{Z})$ has index p in $\mathbf{Z}(\rho_l) \cong \mathbf{Z}[\zeta_d]$ and since any two ideals of index p in $\mathbf{Z}[\zeta_d]$ are conjugate over $\mathbf{Z}$. □

(7.2) **Corollary.** *Let $n \geqq 1$ be an integer. Then $\mathbf{Q}_{\mathbf{Z}/n\mathbf{Z}}$ is rational over $\mathbf{Q}$ if and only if the following two conditions are satisfied:*

(i) *the integer n is not divisible by 8;*

(ii) *for every divisor q of n of the form $q = p^s$, with p an odd prime and s a positive integer, the ring $\mathbf{Z}[\zeta_{\phi(q)}]$ contains a principal ideal of index p; here $\phi(q) = p^{s-1} \cdot (p-1)$.*

Proof. This is just a translation of the main theorem for this case. □

(7.3) **Corollary.** *Let k be a field and A a finite abelian group such that the exponent of A divides*

$$2^2 \cdot 3^m \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 61 \cdot 67 \cdot 71$$

for some non-negative integer m. Then k_A is rational over k.

Proof. It suffices to show that for each odd prime power $q=p^s$ dividing the exponent of A the ring $\mathbf{Z}[\zeta_{\phi(q)}]$ contains an element of norm p. This has been done in [10]. □

(7.4) **Corollary.** *Let k be a field and A a finite abelian group such that:*

(i) *for every odd prime p which divides the exponent of A, the splitting field of X^p-1 over k has degree 1 or 2 over k;*

(ii) *if r is the highest power of 2 dividing the exponent of A, then the splitting field of X^r-1 over k is a cyclic extension of k.*

Then k_A is rational over k.

Proof. This follows from the main theorem and the remark that $1-\zeta_{p^t}$ is an element of norm p in the ring $\mathbf{Z}[\zeta_{p^t}]=\mathbf{Z}[\zeta_{2p^t}]$, for every odd prime power p^t. □

Corollary (7.4) confirms a conjecture of Kuniyoshi [32] for $p\neq 2$; for $p=2$ the conjecture is false.

(7.5) **Corollary.** *Let k be a field and A a finite abelian group. Assume that condition* (ii) *of the main theorem is satisfied. Then there exists a rational field extension $k\subset L$ of finite transcendence degree, and a Galois extension $L\subset L'$, such that* $\mathrm{Gal}(L'/L)\cong A$.

Proof. Let e be the exponent of A, and let l be the splitting field of X^e-1 over k. Denote by h the lowest common multiple of the class numbers of the rings $\mathbf{Z}(\rho_K)$, where K runs over the fields $k\subset K\subset l$ which are cyclic over k. Put $G=A^h$. Then the main theorem implies that k_G is rational over k. Hence we can take $L=k_G$ and L' equal to a suitable intermediate field $k_G\subset L'\subset k(\{x_g\mid g\in G\})$. □

(7.6) **Corollary.** *Let k be a field, which, as a field, is finitely generated over its prime field. Let P_k denote the set of prime numbers p for which $k_{\mathbf{Z}/p\mathbf{Z}}$ is rational over k. Then P_k has Dirichlet density 0 inside the set of all prime numbers.*

Proof (sketch). We need some algebraic number theory [26].

First we consider the case $\mathrm{char}(k)=0$. Then $[k(\zeta_p):k]=p-1$ for all but finitely many prime numbers p, so by (7.1) it suffices to do the case $k=\mathbf{Q}$.

For a prime number m, let $K_m=\mathbf{Q}(\zeta_m)$, let L_m be the Hilbert class field of K_m, and let $h(m)=[L_m:K_m]$ be the class number of K_m. We put

$$S_m=\{p\mid p \text{ is a prime number, which either splits completely in } L_m, \text{ or does not split completely in } K_m\}\cup\{m\}.$$

We claim $P_{\mathbf{Q}}\subset S_m$, for every prime number m. In fact, if $p\in P_{\mathbf{Q}}$ is a prime number unequal to m which splits completely in K_m, then $m\mid p-1$; but

by (7.1) the ring $\mathbf{Z}[\zeta_{p-1}]$ contains a principal ideal of norm p, and therefore also $\mathbf{Z}[\zeta_m]$ contains a principal ideal of norm p. This means that p splits completely in L_m, as required.

Using Tchebotarev's theorem and an easily proved linear disjointness statement, we find that for any finite set M of prime numbers the set $\bigcap_{m\in M} S_m$ has Dirichlet density

$$\prod_{m\in M}(1-(h(m)-1)/h(m)\cdot(m-1)).$$

Since $h(m)\geqq 2$ for all prime numbers $m\geqq 23$, cf. [29], it follows that $\bigcap_{m \text{ prime}} S_m$ has Dirichlet density 0. Therefore also the subset $P_{\mathbf{Q}}$ of $\bigcap_{m \text{ prime}} S_m$ has Dirichlet density 0.

The case of nonzero characteristic is slightly more complicated. We may assume that k is a finite field, say $k=\mathbf{F}_q$, where $q=r^n$ and $r=\mathrm{char}(k)$.

For a prime number m, let K_m, L_m and $h(m)$ be as above, and put $E_m=K_m(q^{1/m})$. We define:

$$\begin{aligned} T_m=\{p \mid & p \text{ is a prime number, which splits completely in } L_m,\\ & \text{or splits completely in } E_m,\\ & \text{or does not split completely in } K_m\}\cup\{m,r\}. \end{aligned}$$

We show $P_k\subset T_m$ for every prime number m. Namely, assume that $p\in P_k$ does not divide mr and splits completely in K_m. We distinguish two cases. If the order of $(q \bmod p)\in\mathbf{F}_p^*$ is divisible by m, then $[k(\zeta_p):k]$ is divisible by m. Using (7.1), we then conclude in the same way as for $k=\mathbf{Q}$ that p splits completely in L_m, so $p\in T_m$. On the other hand, if the order of $(q \bmod p)$ in $\mathbf{F}_p^*$ is not divisible by m, then it is relatively prime to m, so $(q \bmod p)$ is an m-th power in $\mathbf{F}_p$. Since we assumed that p splits completely in K_m, this implies that p splits completely in E_m, so $p\in T_m$, as required.

If M is any finite set of prime numbers m not dividing $n\cdot r$, the Dirichlet density of $\bigcap_{m\in M} T_m$ is

$$\prod_{m\in M}(1-(h(m)-1)/h(m)\cdot m).$$

Hence

$$\bigcap_{m \text{ prime}, m \text{ does not divide } nr} T_m$$

has Dirichlet density 0, so the same is true for P_k. □

Finally, we remark that for $k=\mathbf{F}_2$ the set P_k contains all Mersenne and Fermat prime numbers.

Acknowledgements. The author is greatly indebted to Prof. F. Oort and Prof. W. Kuyk, without whose stimulating help this paper never would have been written.

References

1. Artin, E.: The Orders of the Linear Groups. Comm. Pure Appl. Math. **8**, 355–366 (1955)
2. Bourbaki, N.: Algèbre, Ch. IV et V. Paris: Hermann 1967
3. Breuer, S.: Zyklische Gleichungen 6. Grades und Minimalbasis. Math. Ann. **86**, 108–113 (1922)
4. Breuer, S.: Zur Bestimmung der metazyklischen Minimalbasis von Primzahlgrad. Math. Ann. **92**, 126–144 (1924)
5. Breuer, S.: Metazyklische Minimalbasis und komplexe Primzahlen. J. Reine Angew. Math. **156**, 13–42 (1927)
6. Cassels, J. W. S., Fröhlich, A. (eds.): Algebraic Number Theory. London-New York: Academic Press 1967
7. Charnow, A.: On the fixed field of a linear abelian group. J. London Math. Soc. (2) **1**, 348–350 (1969)
8. Chevalley, C.: Invariants of finite groups generated by reflections. Amer. J. Math. **77**, 778–782 (1955)
9. Demazure, M.: Sous-groupes algébriques de rang maximum du groupe de Cremona. Ann. Sci. École Norm. Sup. (4) **3**, 507–588 (1970)
10. Endo, S., Miyata, T.: Invariants of finite abelian groups. J. Math. Soc. Japan **25**, 7–26 (1973)
11. Endo, S., Miyata, T.: Quasi-permutation modules over finite groups. J. Math. Soc. Japan **25**, 397–421 (1973)
12. Fischer, E.: Die Isomorphie der Invariantenkörper der endlichen Abel'schen Gruppen linearer Transformationen. Nachr. Königl. Ges. Wiss. Göttingen, 77–80 (1915)
13. Fischer, E.: Zur Theorie der endlichen Abelschen Gruppen. Math. Ann. **77**, 81–88 (1916)
14. Furtwängler, P.: Über Minimalbasen für Körper rationaler Funktionen. S.-B. Akad. Wiss. Wien **134**, 69–80 (1925)
15. Galkin, V. M.: On an ideal in the group ring of a cyclic group (Russian). Uspehi Mat. Nauk **28**, 233–234 (1973)
16. Gaschütz, W.: Fixkörper von p-Automorphismengruppen rein-transzendenter Körpererweiterungen von p-Charakteristik. Math. Z. **71**, 466–468 (1959)
17. Haeuslein, G.: On the invariants of finite groups having an abelian normal subgroup of prime index. J. London Math. Soc. (2) **3**, 355–360 (1971)
18. Kaplansky, I.: Modules over Dedekind rings and valuation rings. Trans. Amer. Math. Soc. **72**, 327–340 (1952)
19. Kervaire, M.: Fractions rationnelles invariantes. Séminaire Bourbaki, exp. 445 (1973/1974)
20. Kuniyoshi, H.: On purely-transcendency of a certain field. Tôhoku Math. J. **6**, 101–108 (1954)
21. Kuniyoshi, H.: On a problem of Chevalley. Nagoya Math. J. **8**, 65–67 (1955)
22. Kuniyoshi, H.: Certain subfields of rational function fields. In: Proc. int. symp. algebraic number theory, pp. 241–243. Tokyo-Nikko: 1955
23. Kuyk, W.: Over het omkeerprobleem van de Galoistheorie. Thesis, Amsterdam 1960
24. Kuyk, W.: On a theorem of E. Noether. Nederl. Akad. Wetensch. Proc. Ser. A **67**, 32–39 (1964)
25. Kuyk, W., Mullender, P.: On the invariants of finite abelian groups. Nederl. Akad. Wetensch. Proc. Ser. A **66**, 232–237 (1963)
26. Lang, S.: Algebraic Number Theory. Reading: Addison-Wesley 1970
27. Lenstra, Jr., H. W.: Rational functions invariant under a finite abelian group. Report 72-02, Dept. of Math., University of Amsterdam (1972)
28. Martinet, J.: Un contre-exemple à une conjecture d'E. Noether (d'après R. Swan). Séminaire Bourbaki, exp. 372 (1969/1970). In: Lecture Notes in Mathematics **180**, pp. 145–154. Berlin-Heidelberg-New York: Springer 1971

29. Masley, J.M.: On the class number of cyclotomic fields. Thesis, Princeton University 1972
30. Masuda, K.: On a problem of Chevalley. Nagoya Math. J. **8**, 59–63 (1955)
31. Masuda, K.: Application of the theory of the group of classes of projective modules to the existence problem of independent parameters of invariant. J. Math. Soc. Japan **20**, 223–232 (1968)
32. Matsuda, R.: On purely-transcendency of certain fields. Tôhoku Math. J. **16**, 189–202 (1964)
33. Miyata, T.: Invariants of certain groups, I. Nagoya Math. J. **41**, 69–73 (1971)
34. Nagata, M.: A theorem on valuation rings and its applications. Nagoya Math. J. **29**, 85–91 (1967)
35. Noether, E.: Rationale Funktionenkörper. Jber. Deutsch. Math.-Verein. **22**, 316–319 (1913)
36. Noether, E.: Körper und Systeme rationaler Funktionen. Math. Ann. **76**, 161–196 (1915)
37. Noether, E.: Gleichungen mit vorgeschriebener Gruppe. Math. Ann. **78**, 221–229 (1918)
38. Ono, T.: Arithmetic of algebraic tori. Ann. of Math. **74**, 101–139 (1961)
39. Ono, T.: On the Tamagawa number of algebraic tori. Ann. of Math. **78**, 47–73 (1963)
40. Segre, B.: Sur un problème de M. Zariski. In: Colloque d'Algèbre et de Théorie des Nombres, pp. 135–138. Paris: C.N.R.S. 1950
41. Seidelmann, F.: Die Gesamtheit der kubischen und biquadratischen Gleichungen mit Affekt bei beliebigem Rationalitätsbereich. Thesis, Erlangen 1916. Summary: Math. Ann. **78**, 230–233 (1918)
42. Serre, J.-P.: Corps Locaux. Paris: Hermann 1962
43. Speiser, A.: Zahlentheoretische Sätze aus der Gruppentheorie. Math. Z. **5**, 1–6 (1919)
44. Swan, R.G.: Invariant Rational Functions and a Problem of Steenrod. Invent. Math. **7**, 148–158 (1969)
45. Voskresenskiĭ, V.E.: Birational properties of linear algebraic groups (Russian). Izv. Akad. Nauk SSSR Ser. Mat. **34**, 3–19 (1970). English translation: Math. USSR – Izv. **4**, 1–17 (1970)
46. Voskresenskiĭ, V.E.: On the question of the structure of the subfield of invariants of a cyclic group of automorphisms of the field $\mathbf{Q}(x_1, \ldots, x_n)$ (Russian). Izv. Akad. Nauk SSSR Ser. Mat. **34**, 366–375 (1970). English translation: Math. USSR – Izv. **4**, 371–380 (1970)
47. Voskresenskiĭ, V.E.: Rationality of certain algebraic tori (Russian). Izv. Akad. Nauk SSSR Ser. Mat. **35**, 1037–1046 (1971). English translation: Math. USSR – Izv. **5**, 1049–1056 (1971)
48. Voskresenskiĭ, V.E.: Fields of invariants of abelian groups (Russian). Uspehi Mat. Nauk **28**, 77–102 (1973)

H.W. Lenstra, Jr.
Mathematisch Instituut
Roetersstraat 15
Amsterdam
The Netherlands

(Received February 27, 1974)