Mathematisch Instituut
Roetersstraat 15
Amsterdam - The Netherlands

RATIONAL FUNCTIONS INVARIANT UNDER A FINITE ABELIAN GROUP

H.W. Lenstra Jr

Report 72 - 02

Preprint
Received : June 27, 1972.

July 1972.

Rational functions invariant under a finite abelian group

H.W. Lenstra Jr

Introduction.

Let k be a field, A a finite group and $\{x_g \mid g \in A\}$ a set of indeterminates. We make A act on the field of rational functions $k(\{x_g \mid g \in A\})$ by $g(x_h) = x_{gh}$, $g(c) = c$ (for $g, h \in A$, $c \in k$). The subfield of A-invariants is denoted by k_A. It is an old question of E. Fischer [7] whether k_A is a purely transcendental field extension of k. R.G. Swan [12] proved that this is not true for $k = \mathbb{Q}$ and $A = \mathbb{Z}/47\mathbb{Z}$. In this report we give a complete solution for the case A is abelian. Before stating our main result we introduce some notations.

Let ρ be a finite cyclic group of order n with generator τ, and let $\Phi_n \in \mathbb{Z}[X]$ be the n-th cyclotomic polynomial. The ideal $\Phi_n(\tau)\mathbb{Z}[\rho] \subset \mathbb{Z}[\rho]$ (= group ring of ρ over $\mathbb{Z}$) does not depend on the choice of τ, and we define $\mathbb{Z}(\rho) = \mathbb{Z}[\rho]/\Phi_n(\tau)\mathbb{Z}[\rho]$. Then $\mathbb{Z}(\rho) \cong \mathbb{Z}[\zeta_n]$, with ζ_n a primitive n-th root of unity. Therefore $\mathbb{Z}(\rho)$ is a Dedekind domain, and ρ is in a natural way contained in the group of units of $\mathbb{Z}(\rho)$.

Let $\bar{k}$ be a separable closure of the field k. Consider a subfield $K \subset \bar{k}$ for which

(1) $k \subset K$ is <u>finite cyclic</u> with group ρ_K generated by τ_K,

and let p, s satisfy

(2) p prime, $2 \neq p \neq \mathrm{char}(k)$, $s \in \mathbb{Z}$, $s \geq 1$.

Then the $\mathbb{Z}(\rho_K)$-ideal $\underline{a}_K(p^s)$ is defined by

$\underline{a}_K(p^s) = (\tau_K - t,\ p) \subset \mathbb{Z}(\rho_K)$ if $K = k(\zeta_{p^s})$, $\tau_K(\zeta_p) = \zeta_p^t$, $t \in \mathbb{Z}$,

$\underline{a}_K(p^s) = \mathbb{Z}(\rho_K)$ if $K \neq k(\zeta_{p^s})$.

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

$$\underline{a}_K(A) = \prod_{p,s} \underline{a}_K(p^s)^{m_A(p^s)} \subset \mathbb{Z}(\rho_K),$$

the ideal product ranging over all p and s satisfying (2).

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

Theorem.

Let k be a field and A a finite abelian group. Then k_A is purely transcendental over k if and only if the following two conditions are satisfied:

(i) for every $K \subset \bar{k}$ satisfying (1), the $\mathbb{Z}(\rho_K)$-ideal $\underline{a}_K(A)$ is principal;

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

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

The proof of this theorem is outlined in §§ 1-5. Supplementary results are given in § 6, and § 7 contains some applications.

Our notation and terminology is mostly standard. If a group π acts on a set S, we put $S^{\pi} = \{s \in S \mid \forall \sigma \in \pi : \sigma s = s\}$. For the cohomology groups $\hat{H}^{-1}$ and H^1, see [11]. The group of units of a ring R with 1 is denoted by R^*. By ζ_n we mean a primitive n-th root of unity. The symbol □ means that the remaining part of the proof is left to the reader.

We write "pure" instead of "purely transcendental". A field extension $k \subset L$ is called "stably pure" if there exists a field extension $L \subset L'$ such that L' is pure of finite transcendence degree over both L and k. It seems to be unknown whether "stably pure" implies "pure", cf. [10].

§ 1. Permutation modules and rationality of tori.

Let π be a finite group. A π-module N is called a permutation module [12] if it is free as an abelian group and has a $\mathbb{Z}$-basis permuted by π. For example, free π-modules are permutation modules, and $\mathbb{Z}$ is a permutation module ($\mathbb{Z}$ is a π-module by $\sigma n = n$, for all $\sigma \in \pi$ and $n \in \mathbb{Z}$).

(1.1).

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

Proof: exercise. □

(1.2).
Let N be a direct summand of a permutation module over π, i.e. $N \oplus N'$ is a permutation module for some π-module N'. Let M' be a π-module such that $H^1(\pi', M') = 0$ for every subgroup $\pi' \subset \pi$. Then every exact sequence

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

of π-modules splits.

The proof is left to the reader. Actually, the stated property characterizes direct summands of permutation modules, in the same way as the property of being projective characterizes direct summands of free modules. □

Let l be a field and M a free abelian group of finite $\mathbb{Z}$-rank r, written multiplicatively. Then the group ring $l[M]$ is a domain, $l[M] = l[b_1, \dots, b_r, b_1^{-1}, \dots, b_r^{-1}]$ if $\{b_1, \dots, b_r\}$ is a $\mathbb{Z}$-basis for M, and the quotient field $l(M)$ of $l[M]$ is pure over l of transcendence degree r.

Now suppose π acts faithfully on l as a group of field automorphisms, and M has a π-module structure. We make π act on $l(M)$ by $\sigma(\Sigma_{m\in M} \lambda_m \cdot m) = \Sigma_{m\in M} \sigma\lambda_m \cdot \sigma m$, if $\lambda_m \in l$, $\lambda_m = 0$ for almost all $m \in M$, and $\sigma(a^{-1}b) = \sigma(a)^{-1} \cdot \sigma(b)$, if $a, b \in l[M]$, $a \neq 0$. The field $l(M)^\pi$ is pure over l^π if and only if a certain torus, defined over l^π and splitting over l, is rational over l^π, by [8].

In this section we give a necessary and sufficient condition, in terms of M, that $l(M)^\pi$ be stably pure over l^π.

(1.3).
If N is a finitely generated permutation module over π, then $l(N)^\pi$ is pure over l^π.

Proof: use [4], or look at the torus corresponding to N. □

(1.4).
If N is a direct summand of a permutation module over π, and

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

is an exact sequence of finitely generated $\mathbb{Z}$-free π-modules, then the fields $l(M)^\pi$ and $l(M' \oplus N)^\pi$ are isomorphic over l^π.

This is proved by showing that the corresponding exact sequence of tori admits an " l^π-cross-section", cf. [9, prop. 1.2.2]. Alternatively, apply (1.2) to the sequence

$$0 \to l(M')^* \to l(M')^* . M \xrightarrow{f} N \to 0$$

$$f(\lambda . m) = (m \bmod M') \quad \text{for} \quad \lambda \in l(M')^*, \quad m \in M;$$

here $l(M')^* . M$ is the subgroup of $l(M)^*$ generated by $l(M')^*$ and M. □

(1.5).
If $0 \to M' \to M \to N \to 0$ is an exact sequence of finitely generated $\mathbb{Z}$-free π-modules, and N is a permutation module, then $l(M)^\pi$ is pure over $l(M')^\pi$.

Proof: use (1.4) and (1.3). □

Theorem (1.6).
Let M be a finitely generated $\mathbb{Z}$-free π-module. Then $l(M)^\pi$ is stably pure over l^π if and only if there exists 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. The "if"-part is obvious from (1.5). The "only if"-part follows by the methods of R.G. Swan [12]. The case $\mathrm{char}(l) = 0$ is due to V.E. Voskresenskiĭ [13]. □

(1.7).
Let M be a finitely generated $\mathbb{Z}$-free π-module, and suppose $H^1(\pi', M) = 0$ for every subgroup $\pi' \subset \pi$. Then $l(M)^\pi$ is stably pure over l^π if and only if $M \oplus N_1 \cong N_2$ for some finitely generated permutation modules N_1 and N_2 over π.

Proof: clear from (1.6) and (1.2). □

§ 2. The projective cyclic case.

Let l be a field and π a finite abelian group of automorphisms of l. Put

$$S(\pi) = \{\pi/\pi' \mid \pi' \subset \pi \text{ is a subgroup such that } \pi/\pi' \text{ is cyclic}\}.$$

For $\rho \in S(\pi)$ we have a canonical surjective ring homomorphism $\mathbb{Z}[\pi] \to \mathbb{Z}(\rho)$ (see the introduction for the definition of $\mathbb{Z}(\rho)$). It is well known that the induced map $\mathbb{Z}[\pi] \to \prod_{\rho \in S(\pi)} \mathbb{Z}(\rho)$ becomes an isomorphism when tensored with $\mathbb{Q}$, and that $\Pi_{\rho \in S(\pi)} \mathbb{Z}(\rho)$ can be identified with the integral closure $\mathbb{Z}[\pi]^c$ of $\mathbb{Z}[\pi]$ inside $\mathbb{Q}[\pi]$. If M is a π-module, let M^c be the $\mathbb{Z}[\pi]^c$-module $M \otimes_{\mathbb{Z}[\pi]} \mathbb{Z}[\pi]^c$; this is also a π-module.

The following theorem is our key result.

Theorem (2.1).
Suppose π is cyclic and M is finitely generated π-projective. Then $1(M)^\pi \cong 1(M^c)^\pi$ over 1^π.

The proof is not given here. It can roughly be described as a repeated application of (1.4). Compare [15]. □

(2.2).
Suppose π is cyclic and M is finitely generated π-projective. Then $1(M)^\pi$ is pure over 1^π if and only if M^c is $\mathbb{Z}[\pi]^c$-free.

Proof. The "only if"-part is easy from (1.7). The "if"-part follows from (2.1) and (1.3). □

We will need a result which covers a more general situation than (2.2). Let π be abelian and $\rho \in S(\pi)$. For a π-module M, we put $F_{\pi,\rho}(M) = [M \otimes_{\mathbb{Z}[\pi]} \mathbb{Z}(\rho)] / \{\text{elements of additive finite order}\}$. Then $F_{\pi,\rho}$ is a functor from the category of π-modules to the category of torsion-free $\mathbb{Z}(\rho)$-modules, left adjoint to an obvious functor the other way.

(2.3).
Suppose π is abelian. For every $\rho \in S(\pi)$, let $M_{(\rho)}$ be a finitely generated projective ρ-module; consider $M_{(\rho)}$ as a π-module by the natural map $\pi \to \rho$. Let M be the π-module $\oplus_{\rho \in S(\pi)} M_{(\rho)}$. Then the following three assertions are equivalent:

(i) $1(M)^\pi$ is pure over 1^π;

(ii) $1(M)^\pi$ is stably pure over 1^π;

(iii) for every $\rho \in S(\pi)$, the $\mathbb{Z}(\rho)$-module $F_{\pi,\rho}(M)$ is free.

The proof is analogous to the proof of (2.2). □

§ 3. The modules J_q and I_q.

Let l be a field and π a finite abelian group of automorphisms of l. In this section q denotes a prime power > 1 such that l contains a primitive q-th root of unity ζ_q (so $\operatorname{char}(l) \nmid q$). Put $\pi(q) = \{\sigma \in \pi \mid \sigma(\zeta_q) = \zeta_q\}$ and $\rho(q) = \pi/\pi(q)$. The map $\pi \to (\mathbb{Z}/q\mathbb{Z})^*$, $\tau \mapsto (t \bmod q)$ if $\tau(\zeta_q) = \zeta_q^t$, gives rise to an injective group homomorphism $\varphi_q : \rho(q) \to (\mathbb{Z}/q\mathbb{Z})^*$. This induces a $\rho(q)$-module structure on $\mathbb{Z}/q\mathbb{Z}$.

Put

$$W = \{ r \in \mathbb{Z} \mid r > 1, \ r \text{ is a prime power}, \ \zeta_r \in l, \text{ and } \rho(r) \text{ is non-cyclic} \}.$$

First suppose $q \notin W$. Let $\mathbb{Z}[\rho(q)] \to \mathbb{Z}/q\mathbb{Z}$ be the ring homomorphism induced by φ_q. This is a $\rho(q)$-linear map, the kernel of which is called J_q. So we have an exact sequence of $\rho(q)$-modules

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

<u>(3.1).</u>

Let $q \notin W$. Then J_q is a projective $\rho(q)$-module except if (3) holds:

$$(3) \qquad q \equiv 0 \bmod 4 \text{ and } \varphi_q[\rho(q)] = \{1, -1\} \subset (\mathbb{Z}/q\mathbb{Z})^*.$$

The <u>proof</u> is not given here. □

<u>(3.2).</u>

Let $q \notin W$, q even. Then $l(J_q)^\pi$ is pure over l^π (here J_q is considered as a π-module by the natural map $\pi \to \rho(q)$).

The <u>proof</u> uses (3.1) and (2.3), handling the case (3) separately. □

<u>(3.3).</u>

Suppose q is odd (then $q \notin W$ automatically). Write $k = l^\pi$, and let $K \subset l$, ρ_K be as in (1) of the introduction. Then:

$F_{\pi,\rho_K}(J_q) \cong \underline{a}_K(\mathbb{Z}/q\mathbb{Z})$ as $\mathbb{Z}(\rho_K)$-modules if $K \subset k(\zeta_q)$;

$F_{\pi,\rho_K}(J_q) = 0$ if $K \not\subset k(\zeta_q)$.

The <u>proof</u> of (3.3) is computational. □

Secondly, consider the case $q \in W$. Then $q \equiv 0 \bmod 8$. Put $C(q) = (\mathbb{Z}/q\mathbb{Z}) - \{0\}$, and let $\mathbb{Z}^{C(q)}$ be a free abelian group of rank $q - 1$ with $\mathbb{Z}$-basis $\{e_c \mid c \in C(q)\}$. Make $\mathbb{Z}^{C(q)}$ into a $\rho(q)$-module by

$\sigma(e_c) = e_{\sigma c}$, for $\sigma \in \rho(q)$, $c \in C(q)$. Then the group homomorphism $\mathbb{Z}^{C(q)} \to \mathbb{Z}/q\mathbb{Z}$, $e_c \mapsto c$ (for $c \in C(q)$), is $\rho(q)$-linear, and its kernel is called I_q. So there is an exact sequence of $\rho(q)$-modules

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

<u>(3.4)</u>.
$H^1(\pi', I_q) = 0$ for every subgroup $\pi' \subset \pi$.

The <u>proof</u> of (3.4) is easy from the exact sequence defining I_q. □

<u>(3.5)</u>.
$\hat{H}^{-1}(\pi', I_q) \neq 0$ for some subgroup $\pi' \subset \pi$.

The <u>proof</u> of (3.5) is not given here. □

<u>§ 4. Reduction to a problem of rationality of tori</u>.

Let k be a field and A a finite abelian group, as in the introduction. Write $A \cong P \oplus A_o$ such that $\mathrm{char}(k) \nmid |A_o|$ while $|P|$ is a power of $\mathrm{char}(k)$.

<u>(4.1)</u>.
k_A is k-isomorphic to a pure field extension of k_{A_o}.

The <u>proof</u> makes use of a theorem of W. Gaschütz [2]. □

Let e be the exponent of A_o, and $l = k(\zeta_e)$. The Galois group of l over k is called π. As is well known, the character group $B = \mathrm{Hom}(A_o, l^*)$ is, as an abelian group, isomorphic to A_o (non-canonically). We make B into a π-module by $(\sigma b)(a) = \sigma(b(a))$, for $\sigma \in \pi$, $b \in B$, $a \in A_o$. Let $\mathbb{Z}^B$ be a free abelian group with $\{e_b \mid b \in B\}$ as a $\mathbb{Z}$-basis, and make $\mathbb{Z}^B$ into a permutation module over π by $\sigma e_b = e_{\sigma b}$, for $\sigma \in \pi$, $b \in B$. The group homomorphism $\mathbb{Z}^B \to B$ sending e_b to b (for $b \in B$) is π-linear, and its kernel is called J.
So we have an exact sequence of π-modules

$$0 \to J \to \mathbb{Z}^B \to B \to 0 .$$

<u>(4.2)</u>. k_{A_o} and $l(J)^\pi$ are isomorphic over $k = l^\pi$.

The <u>proof</u> of (4.2) is implicitly contained in the literature [1, 3, 4, 14]. □

Write $A_o \cong A_1 \oplus A_2$ such that A_1 has odd order and $|A_2|$ is a power of 2. Let

$$A_1 \cong \oplus_q (\mathbb{Z}/q\mathbb{Z})^{n_1(q)}, \quad A_2 \cong \oplus_q (\mathbb{Z}/q\mathbb{Z})^{n_2(q)},$$

with non-negative integers $n_1(q)$, $n_2(q)$, and q ranging over the set of prime powers > 1. The π - modules I_1, I_2 and I are defined by

$$I_1 = \oplus_{q \notin W} J_q^{n_1(q)}$$

$$I_2 = \oplus_{q \in W} I_q^{n_2(q)}$$

$$I = I_1 \oplus I_2$$

(see § 3 for the definitions of J_q, I_q and W).

(4.3).
$l(J)^\pi$ is l^π - isomorphic to a pure extension of $l(I)^\pi$.

Sketch of the proof :
Put

$$I_3 = \oplus_{q \notin W} J_q^{n_2(q)} .$$

One constructs an exact sequence of finitely generated π - modules

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

in which N is a permutation module. By (1.5) the field $l(J)^\pi$ is pure over $l(I \oplus I_3)^\pi$, and by (3.2) the field $l(I \oplus I_3)^\pi$ is pure over $l(I)^\pi$. □

(4.4).
k_A is k - isomorphic to a pure field extension of $l(I)^\pi$.

Proof : (4.1), (4.2) and (4.3). □

§ 5. Proof of the main theorem.

(5.1).
$H^1(\pi', I) = 0$ for every subgroup $\pi' \subset \pi$.

Proof : (3.1), (3.4) and the definition of I. □

(5.2).
The following three assertions are equivalent:
(i) $l(I_1)^\pi$ is pure over l^π;
(ii) $l(I_1)^\pi$ is stably pure over l^π;
(iii) condition (i) of the main theorem is satisfied.

Proof.
By (3.1) and the definition of I_1 we can apply (2.3) to $M = I_1$. Therefore it suffices to prove that condition (iii) of (2.3), with $M = I_1$, is equivalent to condition (i) of the main theorem. This follows easily from (3.3) and the theory of finitely generated modules over a Dedekind domain. □

We turn to the proof of the main theorem.
First suppose k_A is pure over k. Then $l(I)$ is stably pure over k, by (4.4). Using (5.1) and (1.7) we find $I \oplus N_1 \cong N_2$ for some permutation modules N_1 and N_2 over π. From (3.5) and (1.1) we conclude that $n_2(q) = 0$ for all $q \in W$, that is, we have proved (ii) of the main theorem. It follows that $I = I_1$ and applying (5.2) we find that (i) is also satisfied.

Secondly, assume that (i) and (ii) of the main theorem hold. Then $I = I_1$, and (5.2) tells us that $l(I)^\pi$ is pure over $l^\pi = k$. Application of (4.4) concludes the proof. □

§ 6. Supplementary results.

Two extension fields K and L of a field k are called stably isomorphic over k if there exist pure 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

$$A' \cong P' \oplus A'_o, \qquad A'_o \cong A'_1 \oplus A'_2, \qquad A'_2 \cong \oplus_q (\mathbb{Z}/q\mathbb{Z})^{n'_2(q)}$$

just as we did for A in § 4.

Theorem (6.1).

Let k be a field and A, 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 $K \subset \bar{k}$ satisfying (1) of the introduction, the $\mathbb{Z}(\rho_K)$-ideals $\underline{a}_K(A)$ and $\underline{a}_K(A')$ are in the same ideal class.

(ii) if $\mathrm{char}(k) \neq 2$, then $n_2(q) = n_2'(q)$ for every even prime power q for which the Galois group of $k(\zeta_q)$ over k is non-cyclic.

The proof of (6.1) is more complicated than the proof of the main theorem. □

Next we consider a generalization of the problem posed in the introduction [1]. 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 quotient field $k(V)$ of $S_k(V)$ is pure over k of transcendence degree $\dim_k(V)$, and the A-action on V induces a faithful action of A on $k(V)$ as a group of field isomorphisms over k. We ask whether $k(V)^A$ is pure over k. For $V = k[A]$ (as $k[A]$-module) this is the question of the introduction.

(6.2).

Let V be a finitely generated faithful $k[A]$-module, and $W \subset V$ a faithful $k[A]$-sub-module. Then $k(V)^A$ is pure over $k(W)^A$.

Proof: this is an easy generalization of a remark of T. Miyata [6]. □

(6.3).

Suppose $A \cong P \oplus A_0$, such that $|P|$ is a power of $\mathrm{char}(k)$ and $\mathrm{char}(k) \nmid |A_0|$. Let V be a finitely generated faithful $k[A]$-module. Then V^P is a faithful $k[A_0]$-module, and $k(V)^A$ is pure over $k(V^P)^{A_0}$.

The proof uses a theorem of W. Gaschütz [2]. (4.1) is a special case. □

Theorem (6.4).

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 pure over k if and only if k_A is pure over k. Moreover, if $\dim_k(V) \geq |A|$, then $k(V)^A$ is pure over k if and only if $k(V)^A$ is stably pure over k.

The proof consists mainly of a suitable application of (6.2). The bound $|A|$ is not best possible. □

§ 7. Applications.

This section contains some corollaries of the main theorem.

Theorem (7.1).
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 $k_{\mathbb{Z}/p\mathbb{Z}}$ is pure over k if and only if the ring $\mathbb{Z}[\zeta_d]$ contains a principal ideal of index p.

The proof uses the main theorem and the fact that any two ideals in $\mathbb{Z}[\zeta_d]$ of index p are conjugate over $\mathbb{Z}$. □
The case $k = \mathbb{Q}$ (so $d = p - 1$) of (7.1) is due to V.E. Voskresenskiĭ [15].

Theorem (7.2).
Let k be a field which, as a field, is finitely generated over its prime field. Then $k_{\mathbb{Z}/p\mathbb{Z}}$ is not pure over k for infinitely many prime numbers p.

The proof is an exercise in algebraic number theory. Strangely, (7.2) (for $k = \mathbb{Q}$) is not mentioned by R.G. Swan [12] and V.E. Voskresenskiĭ [14]. □

Theorem (7.3).
Let $n \geq 1$ be an integer. Then $\mathbb{Q}_{\mathbb{Z}/n\mathbb{Z}}$ is pure over $\mathbb{Q}$ if and only if the following two conditions are satisfied:
(i) $n \not\equiv 0 \bmod 8$.
(ii) for every divisor q of n of the form $q = p^s$, with p an odd prime and $s \in \mathbb{Z}$, $s \geq 1$, the ring $\mathbb{Z}[\zeta_{\varphi(q)}]$ contains a principal ideal of index p; here $\varphi(q) = p^{s-1}(p-1)$.

The proof is easy from the main theorem. For $n = 8$ this contradicts a result of V.E. Voskresenskiĭ [14]. □

Theorem (7.4).
Let k be a field and A a finite abelian group such that the exponent of A divides $2^2 \cdot 3^m \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43$ for some $m \in \mathbb{Z}$, $m \geq 0$. Then k_A is pure over k.

Proof: exercise. □

Theorem (7.5).

Let k be a field and A a finite abelian group such that:

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

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

Then k_A is pure over k.

The proof uses the fact that the only prime ideal of $\mathbb{Z}[\zeta_{2p^t}]$ (p prime, $t \in \mathbb{Z}$, $t \geq 0$) lying above p is principal. □

Theorem (7.5) confirms a conjecture of H. Kuniyoshi [5] for $p \neq 2$ (for $p = 2$ the conjecture is false). Note that (i) and (ii) are satisfied if $k = \mathbb{R}$.

Theorem (7.6).

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 pure field extension $k \subset L$ of finite transcendence degree, and a Galois extension $L \subset L'$, such that the Galois group of L' over L is isomorphic to A.

The proof uses finiteness of class numbers. □

References.

1. E. Fischer, Die Isomorphie der Invariantenkörper der endlichen Abel'schen Gruppen linearer Transformationen, Nachr. Königl. Ges. Wiss. Göttingen 1915, 77 - 80.

2. W. Gaschütz, Fixkörper von p - Automorphismengruppen rein transzendenter Körpererweiterungen von p - Charakteristik, Math. Z., 71 (1959), 466 - 468.

3. W. Kuyk and P. Mullender, On the invariants of finite abelian groups, Nederl. Akad. Wetensch. Proc. Ser. A, 66 = Indag. Math., 25 (1963), 232 - 237.

4. K. Masuda, On a problem of Chevalley, Nagoya Math. J., 8 (1955), 59 - 63.

5. R. Matsuda, On purely-transcendency of certain fields, Tôhoku Math. J., 16 (1964), 189 - 202.

6. T. Miyata, Invariants of certain groups, I, Nagoya Math. J., 41 (1971), 69 - 73.

7. E. Noether, Körper und Systeme rationaler Funktionen, Math. Ann., 76 (1915), 161 - 196.

8. T. Ono, Arithmetic of algebraic tori, Ann. of Math., 74 (1961), 101-139.

9. T. Ono, On the Tamagawa number of algebraic tori, Ann. of Math., 78 (1963), 47 - 73.

10. B. Segre, Sur un problème de M. Zariski, Colloque d'Algèbre et de Théorie des Nombres, C.N.R.S., Paris, 1950, 135 - 138.

11. J.-P. Serre, Corps Locaux, Hermann, Paris 1962.

12. R.G. Swan, Invariant rational functions and a problem of Steenrod, Invent. Math., 7 (1969), 148 - 158.

13. V.E. Voskresenskiĭ, Birational properties of linear algebraic groups, Izv. Akad. Nauk SSSR Ser. Mat., 34 (1970), 3 - 19 (English translation: Math. USSR - Izv., 4 (1970), 1 - 17).

14. V.E. Voskresenskiĭ, On the question of the structure of the subfield of invariants of a cyclic group of automorphisms of the field $\mathbb{Q}(x_1, \ldots, x_n)$, Izv. Akad. Nauk SSSR Ser. Mat., 34 (1970), 366 - 375 (English translation: Math. USSR - Izv., 4 (1970), 371 - 380).

15. V.E. Voskresenskiĭ, Rationality of certain algebraic tori, Izv. Akad. Nauk SSSR Ser. Mat., 35 (1971), 1037 - 1046 (Russian).