J. Math. Soc. Japan
Vol. 25, No. 1, 1973

Invariants of finite abelian groups

By Shizuo ENDO and Takehiko MIYATA

(Received Oct. 21, 1971)

Introduction.

Let k be a field and let G be a finite group. Let V be a (finite dimensional) kG-module, i.e., a representation module of G over k. Then G acts naturally on the quotient field F of the symmetric algebra $S(V)$ of V as k-automorphisms. We denote the field F with this action of G by $k(V)$.

An extension L/k is said to be rational if L is finitely generated and purely transcendental over k.

To simplify our notation, we say that a triple $\langle k, G, V\rangle$ has the property (R) if $k(V)^G/k$ is rational. Especially, if V is the regular representation module of G, i.e., if $V=kG$, then we use $\langle k, G\rangle$ instead of $\langle k, G, V\rangle$.

The following problem is the classical and basic one (e.g. [**11**]).

Does $\langle k, G, V\rangle$ *have the property* (R)?

It is well known that the answer to the problem is affirmative in each of the following cases:

(i) G is the symmetric group, k is any field and $V=kG$.

(ii) G is an abelian group of exponent e and k is a field whose characteristic does not divide e and which contains a primitive e-th root of unity. (Fisher [**5**], etc.)

(iii) G is a p-group and k is a field of characteristic p. (Kuniyoshi [**6**], etc.)

(iv) k is a field of characteristic 0 and G is a finite group generated by reflections of a k-module V (Chevalley [**2**]).

However the problem has been kept open even in the case where G is abelian and k is an algebraic number field.

K. Masuda proved in [7] and [8] that $\langle Q, G\rangle$ has the property (R) when G is a cyclic group of order $n\leqq 7$ or $n=11$, and reduced the problem to the one on integral representations, in case G is a cyclic group of order p. Recently R. G. Swan [**15**] showed, using the Masuda's result, that $\langle Q, G\rangle$ does not have the property (R) when G is a cyclic group of order $p=47, 113, 233, \cdots$.

In this paper we will refine the Masuda-Swan's method and will give some further consequences on the problem in case G is abelian.

Our main results in this paper are the following:

[I] *Let G be a finite abelian group of exponent*

$$e=2^{l_2}3^{l_3}5^{l_5}7^{l_7}11^{l_{11}}13^{l_{13}}17^{l_{17}}19^{l_{19}}23^{l_{23}}29^{l_{29}}31^{l_{31}}37^{l_{37}}41^{l_{41}}43^{l_{43}}61^{l_{61}}67^{l_{67}}71^{l_{71}}.$$

Suppose that l_3 is arbitrary, that each of l_2, l_5, l_7 is 0, 1 *or* 2 *and that each of $l_{11}, l_{13}, l_{17}, \cdots, l_{71}$ is* 0 *or* 1. *Then $\langle Q, G\rangle$ has the property* (R).

We denote $\langle k, G\rangle$ by $\langle k, n\rangle$ if G is a cyclic group of order n.

[II] *There exist infinitely many primes, p, such that, for some $l_0 \geqq 1$, $\langle Q, p^{l_0}\rangle$ does not have the property* (R). *For example, any of $\langle Q, 2^3\rangle$, $\langle Q, 11^2\rangle$, $\langle Q, 13^2\rangle, \cdots$ does not have the property* (R). (For the more precise description, see § 3.)

[III] *Let G be a finite abelian group of exponent e and k be a field of characteristic* 0.

(i) *Case where e is odd: If k contains $\zeta_p+\zeta_p^{-1}$ for any prime p with $p|e$, then $\langle k, G\rangle$ has the property* (R).

(ii) *Case where e is even: If k contains $\zeta_p+\zeta_p^{-1}$ for any odd prime p with $p|e$ and $\zeta_{2^m}+\zeta_{2^m}^{-1}$ for m such that $2^m|e$ but $2^{m+1}\nmid e$ (or $i=\sqrt{-1}$), then $\langle k, G\rangle$ has the property* (R).

Here ζ_n denotes a primitive n-th root of unity.

H. Kuniyoshi conjectured ([**9**]) that, for any $l \geqq 1$, $\langle k, p^l\rangle$ has the property (R), if k contains ζ_p. [IV] implies that this conjecture is valid if (and only if) p is odd.

[IV] *Let R_0 be the maximal real subfield of the maximal abelian extension of Q and k be a field containing R_0* (e.g. *the real number field R*). *Then, for any finite abelian group G and any kG-module V, $\langle k, G, V\rangle$ has the property* (R).

We should remark that, in most of our results, the assumption that the characteristic of a field k is 0 can be replaced by the weaker one that the characteristic of k does not divide the order of a group G.

§ 1. Quasi-permutation modules and quasi-rational extensions.

The first proposition is only a restatement of the well-known Hilbert's theorem 90 (cf. [**14**]).

PROPOSITION 1.1. *Let K/k be a finite Galois extension with group Π and $K(X_1, X_2, \cdots, X_n)$ be the rational function field with n-variables $X_1, X_2, \cdots, X_n$ over K. Suppose further that Π acts semi-linearly on the vector space $\sum_{i=1}^{n} KX_i$, i.e., as follows:*

$$\sigma(\alpha X_i)=\sigma(\alpha)\sum_{j=1}^{n}\alpha_{ij}(\sigma)X_j\,, \qquad \alpha,\ \alpha_{ij}(\sigma)\in K.$$

Then Π acts naturally on $K(X_1, X_2, \cdots, X_n)$ as k-automorphisms and $K(X_1, X_2, \cdots, X_n)^{\Pi}$ is rational over k.

PROOF. If we put $\chi(\sigma)=[\alpha_{ij}(\sigma)]$, then $\chi(\sigma)$ is a 1-cocycle of the complex $\{C^i(\Pi, GL(n, K))\}$. The Hilbert's theorem 90 means $H^1(\Pi, GL(n, K))=1$. Hence there exists $P\in GL(n, K)$ such that $\chi(\sigma)=\sigma(P)^{-1}\cdot P$. Now put $[Z_1, Z_2, \cdots, Z_n]=[X_1, X_2, \cdots, X_n]\cdot {}^tP$. Then it can easily be shown that $K(X_1, X_2, \cdots, X_n)^\Pi=k(Z_1, Z_2, \cdots, Z_n)$.

COROLLARY 1.2. *Let K, k, Π, $K(X_1, X_2, \cdots, X_n)$ be as in* (1.1) *and let $F=K(Y_1, Y_2, \cdots, Y_m)$ be a subfield of $K(X_1, X_2, \cdots, X_n)$ rational over K. Suppose that $Y_1, Y_2, \cdots, Y_m\in k(X_1, X_2, \cdots, X_n)$ and that the restrictions of Π and $GL(n, K)$ on F induce the automorphisms of F. Then F^Π is rational over k.*

Let Π be a finite group. A finitely generated Z-free $Z\Pi$-module is called briefly a Π-module. A Π-module is called a permutation Π-module if it is expressible as a direct sum of some $\{Z\Pi/\Pi_i\}$ where each Π_i is a subgroup of Π. Further a Π-module M is called a quasi-permutation Π-module if there exists an exact sequence:

$$0 \longrightarrow M \longrightarrow S \longrightarrow S' \longrightarrow 0$$

where S and S' are permutation Π-modules.

Let K/k be a finite Galois extension with group Π. Let M be a Π-module and $\{x_1, x_2, \cdots, x_n\}$ be a Z-basis of M. Let $K(X_1, X_2, \cdots, X_n)$ be the rational function field with n-variables $X_1, X_2, \cdots, X_n$ and define the action of Π on $K(X_1, X_2, \cdots, X_n)$ as follows: for any $\sigma\in\Pi$ and $1\leqq i\leqq n$,

$$\sigma\cdot X_i=\prod_{j=1}^{n} X_j^{m_{ij}} \quad \text{when} \quad \sigma\cdot x_i=\sum_{j=1}^{n} m_{ij}x_j,\ m_{ij}\in Z.$$

Then Π can be regarded as a subgroup of the automorphism group of $K(X_1, X_2, \cdots, X_n)$ and we denote $K(X_1, X_2, \cdots, X_n)$ with this action of Π by $K(M)$. It is easily seen that $K(M)$ does not depend on the choice of Z-basis of M.

An extension F/k is said to be quasi-rational if there exists a rational extension of F which is rational over k.

COROLLARY 1.3. *Let K/k be a Galois extension with group Π. Let M, N be Π-modules and S be a permutation Π-module. Suppose that there is an exact sequence:*

$$0 \longrightarrow M \longrightarrow N \longrightarrow S \longrightarrow 0.$$

Then $K(N)^\Pi$ is rational over $K(M)^\Pi$. Especially $K(M)^\Pi$ is quasi-rational over k if and only if $K(N)^\Pi$ is quasi-rational over k.

COROLLARY 1.4. *Let K/k be a Galois extension with group Π and let I be the augmentation ideal of $Z\Pi$. Then both $K(Z\Pi)^\Pi$ and $K(I)^\Pi$ are rational over k.*

PROOF. The assertion for I can be proved by (1.2).

Swan proved in [**15**] the following important

THEOREM 1.5 ([**15**]). *Let K/k be a Galois extension with group Π and let F/K be a rational extension with the action of Π as k-automorphisms compatible with the action on K. Let A be a K-subalgebra of F satisfying the following conditions:*

(i) *The quotient field of A is F.*

(ii) *A is finitely generated over K as algebra.*

(iii) *A is stable under Π.*

(iv) *A is a unique factorization domain.*

(v) *$U(A)/U(K)$ is a finitely generated abelian group.*

If F^{Π}/k is quasi-rational, then $U(A)/U(K)$ is a quasi-permutation Π-module. Here we denote the group of units of a ring R by $U(R)$.

We should remark that the converse to (1.5) is not true. In fact, an example which shows it will be given at the end of § 3.

However, we have

THEOREM 1.6. *Let K/k be a Galois extension with group Π. Then, for any Π-module M, the following conditions are equivalent:*

(1) *M is a quasi-permutation Π-module.*

(2) *$K(M)^{\Pi}$ is quasi-rational over k.*

PROOF. (1)$\Rightarrow$(2) is an immediate consequence of (1.3) and (2)$\Rightarrow$(1) is a special case of (1.5).

COROLLARY 1.7. *Let Π be a finite group. Let M, N be Π-modules and S be a permutation Π-module. Suppose that there is an exact sequence:*

$$0 \longrightarrow M \longrightarrow N \longrightarrow S \longrightarrow 0 .$$

Then M is a quasi-permutation Π-module if and only if N is a quasi-permutation Π-module.

PROPOSITION 1.8. *Let Π be a finite group and P be a projective Π-module. Then P is a quasi-permutation Π-module if and only if there exist permutation Π-modules S, S' such that $P \oplus S' \cong S$. If P is a quasi-permutation Π-module, then the dual $P^* = \mathrm{Hom}_Z(P, Z)$ of P is also a quasi-permutation Π-module.*

PROOF. This is easy, therefore we omit it.

In Chevalley [**1**] we can find an example of a quasi-permutation Π-module M such that M^* is not a quasi-permutation module. Here we give a refinement of the Chevalley's result. (See also [**16**].)

PROPOSITION 1.9. *Let Π be a finite nilpotent group and I be the augmentation ideal of $Z\Pi$. Let K/k be a Galois extension with group Π. Then the following conditions are equivalent:*

(1) *Π is a cyclic group.*

(2) *$K(I^*)^{\Pi}$ is rational over k.*

(3) *I^* is a quasi-permutation Π-module.*

PROOF. (1)$\Rightarrow$(2): If Π is cyclic, then $I \cong I^*$, and hence, by (1.4), $K(I^*)^{\Pi}$ is rational over k. (2)$\Rightarrow$(3) follows directly from (1.6). (3)$\Rightarrow$(1): Suppose that I^* is a quasi-permutation Π-module. Then there exists an exact sequence:

$$0 \longrightarrow S' \longrightarrow S \longrightarrow I \longrightarrow 0$$

where S' and S are permutation Π-modules. For any subgroup Π' of Π, we have $H^n(\Pi, Z\Pi/\Pi') \cong H^n(\Pi', Z)$. Therefore $H^1(\Pi, S) = 0$. Hence, considering the exact sequence of cohomology groups, we obtain

$$0 \longrightarrow H^1(\Pi, I) \longrightarrow H^2(\Pi, S') \qquad \text{(exact)}.$$

Since I is the augmentation ideal of $Z\Pi$, $H^1(\Pi, I)$ is a cyclic group of order $|\Pi|$. A nilpotent group Π is cyclic if and only if $H^2(\Pi, Z)$ contains an element of order $|\Pi|$. Therefore, if Π is not cyclic, then $H^2(\Pi, S')$ does not contain any element of order $|\Pi|$, which contradicts the fact that $H^1(\Pi, I) \subseteq H^2(\Pi, S')$. Thus Π must be cyclic.

PROPOSITION 1.10 ([**12**]). *Let Π be a finite group and let*

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

an exact sequence of Π-modules. Suppose that M'' is a projective Π/Π''-module, putting $\Pi'' = \{\sigma \in \Pi \mid \sigma u'' = u'' \text{ for any } u'' \in M''\}$. Let K/k be a Galois extension with group Π. Then $K(M)^{\Pi}$ is k-isomorphic to $K(M' \oplus M'')^{\Pi}$.

PROOF. See [**12**], Proposition 1.2.2.

Let Π be a cyclic group of order n with generator T and let $\Phi_m(X)$ be the m-th cyclotomic polynomial. Let M be a Π-module and let $m|n$. We put $M_{\Phi_m} = M/\Phi_m(T)M$ and $M^{\Phi_m} = \{u \in M \mid \Phi_m(T)u = 0\}$. Then both M^{Φ_m} and M_{Φ_m} can be regarded as $Z[\zeta_m]$-modules. Especially, if M is Π-projective, then, clearly, $M_{\Phi_m} \cong M^{\Phi_m}$.

In case Π is a cyclic group we give the following remarkable

THEOREM 1.11. *Let Π be a cyclic group of order n. Then, for any projective Π-module P, the following conditions are equivalent:*

(1) *P is a quasi-permutation Π-module.*

(2) *For any $m|n$ P_{Φ_m} is a free $Z[\zeta_m]$-module.*

(3) *For any Galois extension K/k with group Π $K(P)^{\Pi}$ is rational over k.*

PROOF. We may suppose that $P = \mathfrak{A}$ is a projective ideal of $Z\Pi$. If $\mathfrak{A}$ is a quasi-permutation Π-module, then, by (1.8), $\mathfrak{A} \oplus S' \cong S$ for some permutation Π-modules S', S. For any $m|n$ $\mathfrak{A}^{\Phi_m} \oplus S'^{\Phi_m} \cong S^{\Phi_m}$ and both S'^{Φ_m} and S^{Φ_m} are $Z[\zeta_m]$-free. Hence $\mathfrak{A}_{\Phi_m} \cong \mathfrak{A}^{\Phi_m} \cong Z[\zeta_m]$ which proves (1)$\Rightarrow$(2). (3)$\Rightarrow$(1) is a special case of (1.6).

Now we will show (2)$\Rightarrow$(3) by induction. This is trivial for $n=1$. Therefore suppose that $n>1$ and that $\mathfrak{A}_{\Phi_m}$ is $Z[\zeta_m]$-free for any $m|n$. Let

T be a generator of Π. Using the Möbius inversion formula, we can construct the following chain of exact sequences:

$$0 \longrightarrow N_1 \longrightarrow M_1 \longrightarrow \mathfrak{A}/(T^{m_1}-1)\mathfrak{A} \longrightarrow 0$$
$$0 \longrightarrow N_2 \longrightarrow M_1 \longrightarrow \mathfrak{A}/(T^{m_2}-1)\mathfrak{A} \longrightarrow 0$$
$$0 \longrightarrow N_2 \longrightarrow M_2 \longrightarrow \mathfrak{A}/(T^{m_3}-1)\mathfrak{A} \longrightarrow 0$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$0 \longrightarrow N_s \longrightarrow M_{s-1} \longrightarrow \mathfrak{A}/(T^{m_{2s-2}}-1)\mathfrak{A} \longrightarrow 0$$
$$0 \longrightarrow N_s \longrightarrow M_s \longrightarrow \mathfrak{A}/(T^{m_{2s-1}}-1)\mathfrak{A} \longrightarrow 0$$

where $N_1=\mathfrak{A}_{\Phi_n}\cong Z[\zeta_n]$, $M_s=\mathfrak{A}$ and every m_k is a proper divisor of n. Since $\mathfrak{A}$ is Π-projective, each $\mathfrak{A}/(T^{m_k}-1)\mathfrak{A}$ is $\Pi/[T^{m_k}]$-projective. Hence, by (1.10), $K(M_i)^\Pi\cong K(N_i\oplus\mathfrak{A}/(T^{m_{2i-1}}-1)\mathfrak{A})^\Pi$ and $K(M_i)^\Pi\cong K(N_{i+1}\oplus\mathfrak{A}/(T^{m_{2i}}-1)\mathfrak{A})^\Pi$ over k. By induction $K(N_i\oplus\mathfrak{A}/(T^{m_{2i-1}}-1)\mathfrak{A})^\Pi$ is rational over $K(N_i)^\Pi$ and $K(N_{i+1}\oplus\mathfrak{A}/(T^{m_{2i}}-1)\mathfrak{A})^\Pi$ is rational over $K(N_{i+1})^\Pi$. Therefore we get

$$K(M_1)^\Pi\cong K(Z[\zeta_n])^\Pi(Y_1^{(1)}, Y_2^{(1)}, \cdots, Y_{m_1}^{(1)})$$
$$K(M_1)^\Pi\cong K(N_2)^\Pi(Z_1^{(1)}, Z_2^{(1)}, \cdots, Z_{m_2}^{(1)})$$
$$K(M_2)^\Pi\cong K(N_2)^\Pi(Y_1^{(2)}, Y_2^{(2)}, \cdots, Y_{m_3}^{(2)})$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$K(M_{s-1})^\Pi\cong K(N_s)^\Pi(Z_1^{(s-1)}, Z_2^{(s-1)}, \cdots, Z_{m_{2s-2}}^{(s-1)})$$
$$K(\mathfrak{A})^\Pi\cong K(N_s)^\Pi(Y_1^{(s)}, Y_2^{(s)}, \cdots, Y_{m_{2s-1}}^{(s)})$$

where $\{Y_i^{(\alpha)}\}$ and $\{Z_j^{(\beta)}\}$ are indeterminates. From these we get

$$K(\mathfrak{A})^\Pi\cong K(Z[\zeta_n])^\Pi(X_1, X_2, \cdots, X_{n-\varphi(n)})$$

where $X_1, X_2, \cdots, X_{n-\varphi(n)}$ are indeterminates. Especially we have

$$K(Z\Pi)^\Pi\cong K(Z[\zeta_n])^\Pi(X_1, X_2, \cdots, X_{n-\varphi(n)}),$$

hence $K(\mathfrak{A})^\Pi$ is k-isomorphic to $K(Z\Pi)^\Pi$. Since $K(Z\Pi)^\Pi$ is rational over k by (1.4), this concludes that $K(\mathfrak{A})^\Pi$ is rational over k. Thus the proof of (2)$\Rightarrow$(3) is completed.

LEMMA 1.12 ([**15**]). *Let Π be a cyclic group of order n. If M is a quasi-permutation Π-module, then M^{Φ_n} is a free $Z[\zeta_n]$-module.*

PROPOSITION 1.13. *Let Π be a cyclic group of prime order p and let K/k be a Galois extension with group Π. Then for any Π-module M, the following conditions are equivalent:*

(1) *M is a quasi-permutation Π-module.*

(2) *M^{Φ_p} is a free $Z[\zeta_p]$-module.*

(3) *$K(M)^{\Pi}$ is rational over k.*

PROOF. (1)$\Rightarrow$(2) follows directly from (1.12) and (3)$\Rightarrow$(1) follows from (1.6). Further (2)$\Rightarrow$(3) follows from (1.3), (1.4) and the Diederichsen-Reiner's theorem (e.g. [3]).

Generalizations of (1.11) and (1.13) will be given in [4].

§2. The properties (R) and (QR) and the Masuda's modules.

Let G be a finite group and let k be a field. Let V be a (finite dimensional) kG-module. We say that a triple $\langle k, G, V\rangle$ has the property (R) if $k(V)^G$ is rational over k and that a triple $\langle k, G, V\rangle$ has the property (QR) if $k(V)^G$ is quasi-rational over k. Especially, if V is a regular representation module of G, we use $\langle k, G\rangle$ instead of $\langle k, G, V\rangle$. Further, if G is a cyclic group of order n, we use $\langle k, n, V\rangle$ (resp. $\langle k, n\rangle$) instead of $\langle k, G, V\rangle$ (resp. $\langle k, G\rangle$).

PROPOSITION 2.1. *If $\langle k, G, V\rangle$ has the property* (R) (*resp.* (QR)), *then, for any extension L of k, $\langle L, G, L\otimes_k V\rangle$ has the property* (R) (*resp.* (QR)).

PROOF. As this is easy, we omit it.

PROPOSITION 2.2. *Let k be a field of characteristic* 0. *If a kG-module V has a faithful kG-submodule W such that $\langle k, G, W\rangle$ has the property* (R), *then $\langle k, G, V\rangle$ has the property* (R). *If there exists a faithful kG-module V_0 such that $\langle k, G, V_0\rangle$ has the property* (QR), *then, for any faithful kG-module V, $\langle k, G, V\rangle$ has the property* (QR).

PROOF. This follows immediately from (1.1).

THEOREM 2.3. *Let $G_1, G_2, \cdots, G_s$ be finite groups and let k be a field of characteristic* 0. *If every $\langle k, G_i\rangle$ has the property* (R) (*resp.* (QR)), *then $\langle k, \prod_{i=1}^{s} G_i\rangle$ has the property* (R) (*resp.* (QR)).

PROOF. We will prove only the case of (R). Clearly it is sufficient to prove this in the case of $s=2$. Let W_1, W_2, W be the regular representation modules of $G_1, G_2, G_1\times G_2$, respectively and let V_1, V_2 be the augmentation ideals of kG_1, kG_2, respectively. Then V_i and W_i can be regarded naturally as $k(G_1\times G_2)$-modules. Since k is of characteristic 0 we have $W_i\cong V_i\oplus T$, $i=1, 2$, where T denotes the one dimensional trivial representation module of G. $V_1\oplus V_2$ is a faithful kG-module and $V_1\oplus V_2\oplus T\subseteq W$. Now suppose that each $\langle k, G_i\rangle$ has the property (R). Then, by (2.2), it suffices to show that $\langle k, G_1\times G_2, V_1\oplus V_2\oplus T\rangle$ has the property (R). We have

$$k(V_1\oplus V_2\oplus T)^{G_1\times G_2}\cong k(V_1\oplus W_2)^{G_1\times G_2}=[k(V_1\oplus W_2)^{G_2}]^{G_1}.$$

Since G_2 acts trivially on $k(V_1)$, $k(V_1 \oplus W_2)^{G_2} = k(V_1)(W_2)^{G_2}$ is rational over $k(V_1)$ by (2.1). Here we can choose G_1-invariant elements $Y_1, Y_2, \cdots, Y_m$ of $k(V_1 \oplus W_2)^{G_2}$ algebraically independent over $k(V_1)$ such that $k(V_1 \oplus W_2)^{G_2} = k(V_1)(Y_1, Y_2, \cdots, Y_m)$. Therefore we get

$$k(V_1 \oplus V_2 \oplus T)^{G_1 \times G_2} = k(V_1 \oplus W_2)^{G_1 \times G_2} = k(V_1)^{G_1}(Y_1, Y_2, \cdots, Y_m) .$$

Further $k(V_1)^{G_1}(Y_1, Y_2, \cdots, Y_m) = k(V_1)(T)^{G_1}(Y_2, Y_3, \cdots, Y_m) \cong k(W_1)^{G_1}(Y_2, Y_3, \cdots, Y_m)$. Since $k(W_1)^{G_1}$ is rational over k, this implies that $k(V_1 \oplus V_2 \oplus T)^{G_1 \times G_2}$ is rational over k, which completes the proof.

It is remarked that both (2.2) and (2.3) can be proved for any field k using a slight generalization of (1.1) (cf. [**10**]).

We now generalize the Masuda's results in [8]. Let G be a finite abelian group of exponent e and let k be a field of characteristic 0. Let $\zeta(=\zeta_e)$ be a primitive e-th root of unity and put $K = k(\zeta)$. Then K/k is an abelian extension and we denote the Galois group of K/k by Π. Let V be a kG-module. Since K is the splitting field of G, $K \underset{k}{\otimes} V$ can be decomposed to the direct sum of one dimensional KG-modules $W_1, W_2, \cdots, W_s$. Here we can choose a generator Y_i of each W_i such that Π acts on $Y_1, Y_2, \cdots, Y_s$ as permutations. Let S_V be the free abelian group generated multiplicatively by $Y_1, Y_2, \cdots, Y_s$. Then S_V is a permutation Π-module and $K(V) = K(Y_1, Y_2, \cdots, Y_s) = K(S_V)$. Let us put $M_V = \{x \in S_V \mid g(x) = x \text{ for any } g \in G\}$. Then M_V is the Π-submodule of S and $k(V)^G = [K^\Pi(V)]^G = [K(V)^G]^\Pi = K(M_V)^\Pi$. Thus we get

THEOREM 2.4 ([8]). *$k(V)^G = K(M_V)^\Pi$. Especially, if M_V is a permutation Π-module, then $\langle k, G, V\rangle$ has the property* (R), *and M_V is a quasi-permutation Π-module if and only if $\langle k, G, V\rangle$ has the property* (QR).

PROOF. The rest of the assertions follows from (1.3) and (1.6).

The Π-module M_V is said to be the Masuda's module of V. Especially we suppose that G is a cyclic group of order n. Then there exists a faithful irreducible kG-module V. We put $K = k(\zeta_n)$ and $\Pi_k(n) = \mathrm{Gal}(K/k)$. Then we have $S_V \cong Z\Pi_k(n)$ and hence M_V can be regarded as an ideal of $Z\Pi_k(n)$. In this case we call M_V the Masuda's ideal belonging to $\langle k, n\rangle$ and denote it by $I_k(n)$.

COROLLARY 2.5. *Let G be a cyclic group of order n and W be the regular representation module of G. Then we have*

$$k(W)^G \cong k(\zeta_n)(I_k(n))^{\Pi_k(n)}(X_1, X_2, \cdots, X_{n-|\Pi_k(n)|}) ,$$

where $X_1, X_2, \cdots, X_{n-|\Pi_k(n)|}$ are indeterminates.

The action of $\Pi_k(n)$ on ζ_n induces the natural monomorphism $\varphi : \Pi_k(n) \to U(Z/nZ)$. Let $T_1, T_2, \cdots, T_s$ be the generators of $\Pi_k(n)$ and $t_1, t_2, \cdots, t_s$ be representatives of $\varphi(T_1), \varphi(T_2), \cdots, \varphi(T_s)$ in Z, respectively. Then we have

$$I_k(n)=(T_1-t_1,\ T_2-t_2, \cdots, T_s-t_s,\ n).$$

If p is an odd prime, then $\Pi_k(p^l)$ is a cyclic group for any $l \geqq 1$, hence

$$I_k(p^l)=(T-t,\ p^l).$$

On the other hand, $\Pi_k(2^l)$ is a cyclic group or a product of two cyclic groups, hence

$$I_k(2^l)=(T-t,\ 2^l) \qquad \text{or} \qquad (T_1-t_1,\ T_2-t_2,\ 2^l).$$

PROPOSITION 2.6. *If p is an odd prime, then $I_k(p^l)$ is a projective $\Pi_k(p^l)$-module for any $l \geqq 1$. For any $l \geqq 2$ $I_k(2^l)$ is a projective $\Pi_k(2^l)$-module when and only when $\overline{-1} \notin \varphi(\Pi_k(2^l))$ in $U(Z/2^lZ)$.*

PROOF. We put $M=Z\Pi_k(p^l)/I_k(p^l)$. Then M has projective dimension $\leqq 1$ if and only if $\hat{H}^{-1}(\Pi', M)=\hat{H}^0(\Pi', M)=0$ for any Sylow subgroup Π' of Π (e.g. [**14**]). The proof of the proposition can be given by computing directly $\hat{H}^{-1}(\Pi', M)$ and $\hat{H}^0(\Pi', M)$ for each Sylow subgroup Π' of $\Pi_k(p^l)$.

§ 3. Case where G is a cyclic p-group.

In this section we will consider only the case where G is a cyclic p-group.

Let p be a prime and let l be a positive integer. We denote by G_{p^l} the cyclic group of order p^l.

We suppose that p is odd. Let k be a field of characteristic 0 and put $[k(\zeta_{p^l}): k]=p^{m_0}d_0$ where $0 \leqq m \leqq l-1$ and $d_0 | p-1$. Then $\Pi_k(p^l)=\mathrm{Gal}(k(\zeta_{p^l})/k)$ is a cyclic group of order $p^{m_0}d_0$. Let T be a generator of $\Pi_k(p^l)$. Then the Masuda's ideal belonging to $\langle k, p^l \rangle$ has the following form:

$$I_k(p^l)=(T-t,\ p^l) \subsetneqq Z\Pi_k(p^l)$$

where t is a primitive $p^{m_0}d_0$-th root of unity modulo p^l. By virtue of (2.6), $I_k(p^l)$ is a projective $\Pi_k(p^l)$-module. Let us denote by $\Phi_n(X)$ the n-th cyclotomic polynomial. Then we easily see that

$$p | \Phi_{p^m d_0}(t) \quad \text{and} \quad p^2 \nmid \Phi_{p^m d_0}(t) \qquad \text{for any } 0 < m \leqq m_0;$$

$$p^{l-m_0} | \Phi_{d_0}(t);$$

$$p^{l-m_0+1} \nmid \Phi_{d_0}(t) \qquad \text{when } m_0 > 0;$$

$$p \nmid \Phi_{p^m d}(t) \qquad \text{for any } d | d_0,\ d < d_0 \text{ and } 0 \leqq m \leqq m_0.$$

From this it follows immediately that

$$I_k(p^l)_{\Phi_{p^m d}} \cong \begin{cases} (\zeta_{p^m d_0}-t, p) \subsetneqq Z[\zeta_{p^m d_0}] & \text{when } d=d_0 \text{ and } 0<m\leqq m_0 \\ (\zeta_{d_0}-t, p^{l-m_0}) \subsetneqq Z[\zeta_{d_0}] & \text{when } d=d_0 \text{ and } m=0 \ (*) \\ Z[\zeta_{p^m d}] & \text{when } d<d_0 \text{ and } d\,|\,d_0 . \end{cases}$$

For any $0\leqq m\leqq m_0$ we put $J_k^{(m)}(p^l)=(\zeta_{p^m d_0}-t, p)$. Then $J_k^{(m)}(p^l)$ is a prime ideal of $Z[\zeta_{p^m d_0}]$ and $N(J_k^{(m)}(p^l))=p$. Further put

$$J_k(p^l)=\begin{cases} J_k^{(m_0)}(p^l) & \text{when } m_0>0 \\ [J_k^{(0)}(p^l)]^l & \text{when } m_0=0 . \end{cases}$$

Now we give

THEOREM 3.1. *Let p be an odd prime and let l be a positive integer. Let k be a field of characteristic 0 and put $[k(\zeta_{p^l}): k]=p^{m_0}d_0$. Then the following conditions are equivalent:*

(1) *For any faithful kG_{p^l}-module V $\langle k, p^l, V\rangle$ has the property* (R).

(2) *$\langle k, p^l\rangle$ has the property* (R).

(3) *$I_k(p^l)$ is a quasi-permutation $\Pi_k(p^l)$-module.*

(4) *$J_k(p^l)$ is a principal ideal of $Z[\zeta_{p^{m_0}d_0}]$.*

(5) *There exists an element α of $Z[\zeta_{p^{m_0}d_0}]$ such that*

$$N_{Q(\zeta_{p^{m_0}d_0})/Q}(\alpha)=\begin{cases} \pm p & \textit{when } m_0>0 \\ \pm p^l & \textit{when } m_0=0 . \end{cases}$$

Further suppose that $m_0>0$. Then the above conditions are equivalent to each of the following conditions:

(1)′ *For any kG_{p^l}-module V $\langle k, p^l, V\rangle$ has the property* (R).

(2)′ *For any $1\leqq l'\leqq l$ $\langle k, p^{l'}\rangle$ has the property* (R).

PROOF. The implication (1)$\Rightarrow$(2) is evident and the implications (2)$\Leftrightarrow$(3) follow from (1.11) and (2.5). Since any faithful kG_{p^l}-module contains at least one of faithful irreducible kG_{p^l}-modules, the implication (3)$\Rightarrow$(1) follows from (2.2). The implication (3)$\Rightarrow$(4) follows from (1.12) (or (1.11)). Because of $N(J_k^{(m_0)}(p^l))=p$, (4)$\Leftrightarrow$(5) can be shown easily. Suppose that $J_k(p^l)$ is a principal ideal of $Z[\zeta_{p^{m_0}d_0}]$. In case $m_0>0$, $J_k(p^l)=(\zeta_{p^{m_0}d_0}-t, p)$ and there is $\alpha\in Z[\zeta_{p^{m_0}d_0}]$ such that $N_{Q(\zeta_{p^{m_0}d_0})/Q}(\alpha)=\pm p$. We put

$$\alpha_m=N_{Q(\zeta_{p^{m_0}d_0})/Q(\zeta_{p^m d_0})}(\alpha) \qquad \text{for any } 0\leqq m\leqq m_0 .$$

Then $N_{Q(\zeta_{p^m d_0})/Q}(\alpha_m)=\pm p$, hence $J_k^{(m)}(p^l)$ is principal in $Z[\zeta_{p^m d_0}]$. Therefore, by (*) and (1.11), we can conclude that $I_k(p^l)$ is a quasi-permutation $\Pi_k(p^l)$-module. In case $m_0=0$ we can similarly show that $I_k(p^l)$ is a quasi-permutation $\Pi_k(p^l)$-module. Thus the implication (4)$\Rightarrow$(3) is proved, which completes the proof of the first part of the theorem.

Suppose further that $m_0>0$. To prove the second part it suffices to prove that the condition (4) is equivalent to the following condition:

(4)′ *For any* $1\leqq l'\leqq l$, $J_k(p^{l'})$ *is a principal ideal of* $Z[\zeta_{p^{m'}d_0}]$ *where* $[k(\zeta_{p^{l'}}):k]=p^{m'}d_0$.

We suppose that $J_k(p^l)$ is a principal ideal of $Z[\zeta_{p^{m_0}d_0}]$. It has been shown in the proof of (4)⇒(3) that $J_k^{(m)}(p^l)$ is principal in $Z[\zeta_{p^m d_0}]$ for any $0\leqq m\leqq m_0$. However we easily see that

$$J_k(p^{l'})=\begin{cases} J_k^{(m')}(p^l) & \text{when } m'>0 \\ [J_k^{(0)}(p^l)]^{l'} & \text{when } m'=0\,. \end{cases}$$

Hence $J_k(p^{l'})$ is also principal in $Z[\zeta_{p^{m'}d_0}]$. This proves our assertion.

In [**15**] Swan proved (2)⇒(3)⇒(4)⇔(5) in (3.1) when $k=Q$ and $l=1$.

It should be remarked that the second part of (3.1) does not hold always without the assumption that $m_0>0$. In fact, let k_0 be the subfield of $Q(\zeta_{47^2})$ such that $[Q(\zeta_{47^2}):k_0]=46$. Then $k_0(\zeta_{47})=k_0(\zeta_{47^2})$ and $[k_0(\zeta_{47}):k_0]=46$, and therefore $\Pi=\Pi_{k_0}(47)=\Pi_{k_0}(47^2)$ is a cyclic group of order 46. Hence we have $J_{k_0}(47)=(\zeta_{46}-t, 47)$ and $J_{k_0}(47^2)=(\zeta_{46}-t, 47^2)=[J_{k_0}(47)]^2$ where t is a primitive 46-th root of unity modulo 47^2. By a Swan's result in [**15**], $J_{k_0}(47)$ is not principal in $Z[\zeta_{46}]$, i.e., $\langle k_0, 47\rangle$ does not have the property (R). However $J_{k_0}(47^2)$ is principal in $Z[\zeta_{46}]$ because the class number of $Q(\zeta_{46})$ is 2. Hence, by (3.1), $\langle k_0, 47^2\rangle$ has the property (R).

PROPOSITION 3.2. *Let p be an odd prime and let k be a field of characteristic* 0. *If k contains $\zeta_p+\zeta_p^{-1}$, then $\langle k, p^l\rangle$ has the property* (R) *for any $l\geqq 1$.*

PROOF. Since k contains $\zeta_p+\zeta_p^{-1}$, we can put $[k(\zeta_{p^l}):k]=e=2p^{m_0}$ or p^{m_0} for some $0\leqq m_0\leqq l-1$. Now put $\alpha=1-\zeta_{p^{m_0}}$. Then $N_{Q(\zeta_e)/Q}(\alpha)=p$, and therefore, by (3.1), $\langle k, p^l\rangle$ has the property (R). This proves our assertion.

We conjecture that $Q(\zeta_p+\zeta_p^{-1})$ is the smallest algebraic number field such that $\langle k, p^l\rangle$ has the property (R) for any $l\geqq 1$. In fact this conjecture is true if p satisfies one of the following conditions:

(i) $\dfrac{p-1}{2}$ is a prime $\geqq 23$ congruent to -1 modulo 4.

(ii) Any prime divisor of $\dfrac{p-1}{2}$ is congruent to 1 modulo 4.

Let Q be the rational number field. To simplify our notation, we use $\langle p^l\rangle$, $\Pi(p^l)$, $I(p^l)$ and $J(p^l)$ instead of $\langle Q, p^l\rangle$, $\Pi_Q(p^l)$, $I_Q(p^l)$ and $J_Q(p^l)$ respectively.

Putting $p=3$ in (3.2), we get

COROLLARY 3.3. *For any $l\geqq 1$ $\langle 3^l\rangle$ has the property* (R).

However for $p\geqq 5$ it is difficult to determine p^l such that $\langle p^l\rangle$ has the property (R). Here we give only the following

PROPOSITION 3.4. (1) *Let p be one of the following primes:* 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 61, 67, 71. *Then $\langle p\rangle$ has the property* (R).

(2) *For each of* $p=5$, 7, $\langle p^2\rangle$ *has the property* (R).

PROOF. By virtue of (3.1) it suffices to show the existence of α of $Z[\zeta_{p^{l-1}(p-1)}]$ such that $N_{Q(\zeta_{p^{l-1}(p-1)})/Q}(\alpha)=\pm p$. By direct computations (or by [13]), we obtain the following table.

p^l	α	p^l	α	p^l	α
5	$\zeta^2+\zeta-1$	23	$\zeta^5-\zeta^3+1$	43	$\zeta^6+\zeta-1$
7	$\zeta^3-\zeta-1$	25	$\zeta^5-\zeta^3+1$	49	$\zeta^4-\zeta-1$
11	$\zeta^3+\zeta^2-1$	29	$\zeta^5-\zeta^2+1$	61	$\zeta^6-\zeta-1$
13	$\zeta^4-\zeta-1$	31	$\zeta^3+\zeta+1$	67	$\zeta^6+\zeta+1$
17	$\zeta^3-\zeta^2-1$	37	$\zeta^5+\zeta^2+1$	71	$\zeta^7-\zeta^3+1$
19	$\zeta^4+\zeta+1$	41	$\zeta^8-\zeta^5+1$	Here $\zeta=\zeta_{p^{l-1}(p-1)}$.	

If the class number $c(Q(\zeta_{p^{l-1}(p-1)}))$ is 1, $\langle p^l\rangle$ has the property (R). For example, it is known that $c(Q(\zeta_m))=1$ for any $m<23$, and hence, we can conclude without using the above list that $\langle p^l\rangle$ has the property (R) if p^l is one of 5, 7, $\cdots$, 23, 25, 31, 43, 49. In fact, for any p^l in the proposition, $c(Q(\zeta_{p^{l-1}(p-1)}))$ may be 1.

In [7] and [8] Masuda proved that $I(p)$ is principal for $p\leqq 11$. One might have a conjecture: $I(p)$ is principal if $\langle p\rangle$ has the property (R). But this conjecture is false. In fact the second named author proved in an unpublished note that $I(13)$ is not principal.

Next, by the Swan's method, we will determine odd primes, p, such that $\langle p\rangle$ or $\langle p^2\rangle$ does not have the property (R).

By virtue of (3.1), $\langle p^l\rangle$ does not have the property (R) when there exists a subfield F of $Q(\zeta_{p^{l-1}(p-1)})$ containing no algebraic integer γ with $N_{F/Q}(\gamma)=\pm p$. Swan proved, using the imaginary quadratic subfields, that, for $p=47$, 113, 233, $\cdots$, $\langle p\rangle$ does not have the property (R).

We can find all quadratic subfields of $Q(\zeta_n)$ by the following

LEMMA 3.5 ([15]). *Let d be a square-free integer. Then* $Q(\sqrt{d})\subseteqq Q(\zeta_n)$ *if and only if* $d|n$ *and, in addition,* (i) $d\equiv 1 \bmod 4$ *if n or $n/2$ is odd and* (ii) d *is odd if* $4|n$ *but* $8\nmid n$.

As a little more general result containing the Swan's examples, we have

PROPOSITION 3.6. *Let p be an odd prime satisfying one of the following conditions*:

(i) $p=2q+1$ *where* $q\equiv -1 \bmod 4$, *q is square-free, and any of* $4p-q$ *and* $q+1$ *is not square.*

(ii) $p=8q+1$ *where* $q\not\equiv -1 \bmod 4$, *q is square-free, and any of* $p-q$ *and*

$p-4q$ is not square.
Then $\langle p\rangle$ does not have the property (R).

PROOF. This can be done by taking $Q(\sqrt{-q})$ and $Q(\sqrt{-2q})$ respectively.

For the purpose the imaginary quadratic subfields are the most useful, because their class numbers are fairly big. However, for example, we can show that $\langle 317\rangle$ does not have the property (R), by using the real quadratic field $Q(\sqrt{79})$, and that $\langle 241\rangle$ does not have the property (R) by using the biquadratic field $Q(\sqrt{2}, \sqrt{-15})$.

In appendix we will give the table of odd primes $p<2000$ such that $\langle p\rangle$ does not have the property (R), which can be determined by using quadratic subfields or biquadratic subfields.

For $l=2$, we have a much better result.

PROPOSITION 3.7. *Let $p>7$ be an odd prime which does not satisfy any of the following conditions:*

(i) $p=2\cdot 3^s+1$, $s\geqq 2$ *where* $s\not\equiv -1 \bmod 4$.

(ii) $p=2\cdot 11^{2s+1}+1$, $s\geqq 0$.

(iii) $p=2\cdot q^{2s+1}+1$, $s\geqq 1$ *where q is an odd prime such that* $q\equiv -1 \bmod 12$, $q\geqq 23$.

Then $\langle p^2\rangle$ does not have the property (R).

PROOF. We can prove this by taking $Q(\sqrt{-pm})$ for some square-free positive divisor m of $p-1$.

For example, for $7<p<10^5$, there exist only seven primes 19, 23, 163, 487, 1459, 2663, 39367, satisfying one of the conditions in (3.7). Further (3.7) implies the existence of infinitely many primes, p, such that $\langle p^2\rangle$ does not have the property (R), because there exist infinitely many primes congruent to 1 modulo 4. We conjecture that $\langle p^2\rangle$ does not have the property (R) except $p=3$, 5, 7.

Finally we consider the case of $p=2$. Let us put $R_1=Q$, $R_m=Q(\cos(\pi/2^m))$ $=Q(\zeta_{2^{m+1}}+\zeta_{2^{m+1}}^{-1})$, $S_m=Q(i\sin(\pi/2^m))$, $Q_m=Q(\zeta_{2^m})$ for any $m\geqq 2$ and further $R_\infty=\bigcup_{m\geqq 1} R_m$, $Q_\infty=\bigcup_{m\geqq 2} S_m=\bigcup_{m\geqq 2} Q_m$. Then we see

$$\begin{tikzcd}
Q_2 \arrow[rr, hook] & & Q_3 \arrow[rr, hook, dashed] & & Q_m \arrow[rr, hook] & & Q_{m+1} \arrow[rr, hook, dashed] & & Q_\infty \\
& S_2 \arrow[ur, hook] & & & & S_m \arrow[ur, hook] & & & \\
Q=R_1 \arrow[uu, hook] \arrow[ur, hook] \arrow[rr, hook] & & R_2 \arrow[uu, hook] \arrow[ur, hook, dashed] \arrow[rr, hook, dashed] & & R_{m-1} \arrow[uu, hook] \arrow[ur, hook] \arrow[rr, hook] & & R_m \arrow[uu, hook] \arrow[ur, hook, dashed] \arrow[rr, hook, dashed] & & R_\infty \arrow[uu, hook]
\end{tikzcd}$$

These are all the subfields of Q_∞.

Let k be a field of characteristic 0. By (2.6), for any $l\geqq 2$, $I_k(2^l)$ is $\Pi_k(2^l)$-projective if and only if k contains i or $i\sin(\pi/2^m)$ for some $m\geqq 2$. If k contains i or $i\sin(\pi/2^m)$ for some $m\geqq 2$, then $\Pi_k(2^l)$ is cyclic. Therefore, using the same method as in (3.2) we can prove

PROPOSITION 3.8. *If k contains i or $i\sin(\pi/2^m)$ for some $m\geqq 2$, i.e., if $k\cap Q_\infty=Q_\infty$, Q_m or S_m for some $m\geqq 2$, then $\langle k, 2^l\rangle$ has the property* (R) *for any $l\geqq 1$.*

PROOF. We may assume that $k=Q_2$ or that $k=S_m$, $m\geqq 2$. It is evident that $\langle Q_2, 2^l\rangle$ has the property (R) for $l\leqq 2$. If $l\geqq 3$, $\Pi_{Q_2}(2^l)$ is of order 2^{l-2} and $I_{Q_2}(2^l)=(T-5, 2^l)$. Then we easily see that, for any $1\leqq l'\leqq l-2$,

$$I_{Q_2}(2^l)_{\Phi_{2^{l'}}}\cong(\zeta_{2^{l'}}-5, 2)=(\zeta_{2^{l'}}-1)\,.$$

According to (1.11) and (2.5) we can conclude that $\langle Q_2, 2^l\rangle$ has the property (R). It is also clear that $\langle S_m, 2^l\rangle$ has the property (R) for $l\leqq m+1$ because $\Pi_{S_m}(2^l)$ is of order 2. If $l\geqq m+2$, $\Pi_{S_m}(2^l)$ is of order 2^{l-m} and $I_{S_m}(2^l)=(T+5^{2^{m-2}}, 2^l)$. For any $1\leqq l'\leqq l-m$,

$$I_{Q_2}(2^l)_{\Phi_{2^{l'}}}\cong(\zeta_{2^{l'}}+5^{2^{m-2}}, 2)=(\zeta_{2^{l'}}-1)\,.$$

Again by (1.11) and (2.5) we see that $\langle S_m, 2^l\rangle$ has the property (R). Thus the proof is completed.

We here remark that (3.2) and (3.8) include the Matsuda's result in [**9**].

In the case where $I_k(2^l)$ is not $\Pi_k(2^l)$-projective, we need a different method.

PROPOSITION 3.9. *If $k\cap Q_\infty=R_m$ for some $m\geqq 1$, then, for any $l\leqq m+1$, $\langle k, 2^l\rangle$ has the property* (R), *but, for any $l\geqq m+2$, $\langle k, 2^l\rangle$ does not have the property* (QR). *If $k\cap Q_\infty=R_\infty$, then, for any $l\geqq 1$, $\langle k, 2^l\rangle$ has the property* (R).

PROOF. In any case it is clear that $\langle k, 2\rangle$ has the property (R). Hence we have only to prove this for $l\geqq 2$. Now suppose that $k\cap Q_\infty=R_m$ for some $m\geqq 1$. Then, for any $2\leqq l\leqq m+1$, $[k(\zeta_{2^l}):k]=2$, hence $\Pi_k(2^l)$ is a cyclic group of order 2. Thus it follows from (2.5) and (1.13) that $\langle k, 2^l\rangle$ has the property (R). Let $l\geqq m+2$. Then $\Pi_k(2^l)$ can be identified with $\Pi_{R_m}(2^l)$ and, under this identification, $I_k(2^l)=I_{R_m}(2^l)$. Therefore we may assume $k=R_m$. If $\langle R_{l-2}, 2^l\rangle$ does not have the property (QR), then $\langle R_m, 2^l\rangle$ does not have the property (QR) ((2.1)). Hence it suffices to show that $\langle R_{l-2}, 2^l\rangle$ does not have the property (QR). The group $\Pi=\Pi_{R_{l-2}}(2^l)$ is the direct product of two cyclic groups of order 2, and the Masuda's ideal has the following form:

$$I=I_{R_{l-2}}(2^l)=(T_1-2^{l-1}-1,\ T_2+1,\ 2^l)\,.$$

Let $\tilde{I}=(T_1+1, T_2+1, 2^{l-2}+1)$ and $I'=(T_1-2^{l-1}-1, T_2+1)$. Then $I'=\tilde{I}\cap I=\tilde{I}\cdot I$ and $\tilde{I}$ is Π-projective. As is easily seen, there exists an exact sequence:

$$0\longrightarrow Z\Pi/(T_2+1)\longrightarrow\tilde{I}\longrightarrow Z\Pi/[T_2]\longrightarrow 0\,,$$

hence $\tilde{I}$ is a quasi-permutation Π-module by (1.7). On the other hand, $I'=(T_1-1-2^{l-2}(T_2-1), T_2+1)$ and $I'\cap(T_1-1, T_2-1)=(T_1-1+2^{l-2}(T_2-1))$, and hence we get the exact sequence:

$$0 \longrightarrow (T_1-1+2^{l-2}(T_2-1)) \longrightarrow I' \longrightarrow Z \longrightarrow 0.$$

However $(T_1-1+2^{l-2}(T_2-1))=Z\Pi/(T_1T_2+T_1+T_2+1)=(T_1-1, T_2-1)^*$ and, by virtue of (1.9), $(T_1-1, T_2-1)^*$ is not a quasi-permutation Π-module. Again by (1.7) I' is also not a quasi-permutation Π-module. Since $I'=\tilde{I}^{-1}\cdot I=\tilde{I}^{-1}\otimes_{Z\Pi} I$, from (1.8) it follows that I is not a quasi-permutation Π-module. Thus $\langle R_{2l-2}, 2^l\rangle$ does not have the property (QR) by (1.6) and (2.5).

If $k\cap Q_\infty=R_\infty$, again using (2.5) and (1.13) we can conclude that $\langle k, 2^l\rangle$ has the property (R) for $l\geqq 2$.

COROLLARY 3.10. *For $l\leqq 2$ $\langle 2^l\rangle$ has the property* (R), *but, for any $l\geqq 3$, $\langle 2^l\rangle$ does not have the property* (QR).

Here we give an example which shows that the converse to (1.5) is not true.

Let Π' be a cyclic group of order 8 and σ' be a generator of Π'. Let $\Pi=\Pi'/[\sigma'^4]$ and let V', V be the regular representation modules of Π', Π over Q, respectively. Let us put $K=Q(V)$ and $F'=Q(V\oplus V')=K(V')$. Then, by (3.9), $K^{\Pi'}=K^{\Pi}$ is rational over Q and, by (2.2) and (the proof of) (3.9), $F'^{\Pi'}$ is not quasi-rational over Q. Therefore $F'^{\Pi'}$ is not quasi-rational over $K^{\Pi'}$. Let $\{Y_1, Y_2, \cdots, Y_8\}$ be the basis of V' such that

$$\sigma'(Y_1)=Y_2, \qquad \sigma'(Y_2)=Y_3, \cdots, \sigma'(Y_8)=Y_1.$$

Further put $V'_0=Q\cdot(Y_1+Y_5)+Q\cdot(Y_2+Y_6)+Q\cdot(Y_3+Y_7)+Q\cdot(Y_4+Y_8)$ and $V'_1=Q\cdot(Y_1-Y_5)+Q\cdot(Y_2-Y_6)+Q\cdot(Y_3-Y_7)+Q\cdot(Y_4-Y_8)$. Then $V'_0\cong V$ and $V'=V'_0\oplus V'_1$, and $F'^{\Pi'}$ is rational over $K(V'_1)^{\Pi'}$ by (2.2). We put $X_1=\frac{Y_2-Y_6}{Y_1-Y_5}$, $X_2=\frac{Y_3-Y_7}{Y_1-Y_5}$, $X_3=\frac{Y_4-Y_8}{Y_1-Y_5}$ and $F=K(X_1, X_2, X_3)$. Since Π' acts naturally on F and $\sigma'^4(X_i)=X_i$ for each i, Π acts on F. By virtue of [**10**], Lemma, we can see that $K(V')^{\Pi'}$ is rational over F^{Π}. Hence F^{Π} is not quasi-rational over K^{Π}. On the other hand, $A=K[X_1, X_1^{-1}, X_2, X_2^{-1}, X_3, X_3^{-1}]$ satisfies the conditions in (1.5), and $U(A)/U(K)$ is isomorphic to the augmentation ideal of $Z\Pi$, i.e., it is a quasi-permutation Π-module. Thus $\{K/K^{\Pi}, \Pi, F, A\}$ is as required.

In this example the group Π is a cyclic group of order 4. It is noted that, for any finite non-cyclic group Π, such example can be constructed using (1.9).

§ 4. General case.

By summarizing (2.3), (3.3), (3.4) and (3.10), we get

THEOREM 4.1. *Let G be a finite abelian group of exponent* $e=2^{l_2}3^{l_3}5^{l_5}7^{l_7}11^{l_{11}}13^{l_{13}}17^{l_{17}}19^{l_{19}}23^{l_{23}}29^{l_{29}}31^{l_{31}}37^{l_{37}}41^{l_{41}}43^{l_{43}}61^{l_{61}}67^{l_{67}}71^{l_{71}}$. *Suppose that l_3 is arbitrary, that l_2, l_5, l_7 are* 0, 1 *or* 2, *respectively, and that $l_{11}, l_{13}, l_{17}, \cdots, l_{71}$ are* 0 *or* 1, *respectively. Then $\langle Q, G\rangle$ has the property* (R).

Also, from (2.3), (3.2) and (3.8), we get

THEOREM 4.2. *Let G be a finite abelian group of exponent e and k be a field of characteristic* 0.

(i) *If e is odd and if k contains $\zeta_p+\zeta_p^{-1}$ for any prime p with $p|e$, then $\langle k, G\rangle$ has the property* (R).

(ii) *If e is even and if k contains $\zeta_p+\zeta_p^{-1}$ for any odd prime p with $p|e$ and $\zeta_{2m}+\zeta_{2m}^{-1}$ (or $i=\sqrt{-1}$) where m is the integer such that $2^m|e$ but $2^{m+1}\nmid e$, then $\langle k, G\rangle$ has the property* (R).

We conjecture that, under the assumptions in (4.2), $\langle k, G, V\rangle$ has the property (R) for any kG-module V. In fact it was shown in § 3 that the conjecture is true if G is a cyclic p-group. However we did not succeed in proving this in the general case. Here, as an application of (2.4), we give only

THEOREM 4.3. *Let R_0 be the maximal real subfield of the maximal abelian extension of Q and let k be a field containing R_0. Then, for any finite abelian group G and any kG-module V, $\langle k, G, V\rangle$ has the property* (R).

PROOF. Let e be the exponent of G. Then $[k(\zeta_e):k]=1$ or 2 by the assumption. Hence this follows directly from (1.13) and (2.4).

As another application of (2.4) we will show

THEOREM 4.4. *Let G be a finite abelian group of odd order and k be a field of characteristic* 0. *Then there exists an integer $m>0$ such that $\langle k, G^{(m)}\rangle$ has the property* (R).

PROOF. By (2.1) and (2.3) it suffices to prove this in case G is a cyclic p-group and $k=Q$. Hence we assume that G is a cyclic p-group of order p^l and that $k=Q$. Since p is odd, the Masuda's ideal $I(p^l)$ is $\Pi(p^l)$-projective. It is well known that the Picard group $\mathrm{Pic}(Z\Pi(p^l))$ is finite. Therefore there exists an integer $m>0$ such that $I(p^l)^{(m)}\cong Z\Pi(p^l)^{(m)}$. Now the faithful irreducible QG-module V can be considered as a $QG^{(m)}$-module through the projection of $G^{(m)}$ on the i-th component, $1\leqq i\leqq m$ and we denote it by V_i. If we put $V_0=\sum_{i=1}^{m}\oplus V_i$, then V_0 is a faithful $QG^{(m)}$-module which is a $QG^{(m)}$-direct summand of the regular representation module W of $G^{(m)}$. We easily see $M_{V_0}\cong\sum_{i=1}^{m}\oplus M_{V_i}\cong I(p^l)^{(m)}\cong Z\Pi(p^l)^{(m)}$, hence $Q(V_0)^{G^{(m)}}=Q(\zeta_{p^l})(Z\Pi(p^l)^{(m)})^{\Pi(p^l)}$

by (2.4). Therefore $Q(V_0)^{G^{(m)}}$ is rational over Q. Consequently $Q(W)^{G^{(m)}}$ must be rational over Q by (2.2), which completes our proof.

The assertion in (4.4) is not always true for a finite abelian group of even order. For example, if G is a cyclic group of order 8, $\langle Q, G^{(m)}\rangle$ does not have the property (QR) for any $m>0$. (See the proofs of (1.9) and (3.9).)

It was shown in (4.4) that the converse to (2.3) is not always true. However, we have the following partial converse to (2.3).

For any prime p we put $Q_p = \bigcup_{l\geqq 1} Q(\zeta_{p^l})$. Further, for any field k of characteristic 0, we put $k^{(p)} = k \cap Q_p$.

PROPOSITION 4.5. *Let $p_1, p_2, \cdots, p_s$ be primes different from each other. For each $1\leqq i\leqq s$ let G_i be a finite abelian p_i-group. Let k be a field of characteristic 0 such that $k=k^{(p_1)}\cdot k^{(p_2)}\cdot \cdots \cdot k^{(p_s)}$. If $\langle k, G_1\times G_2\times \cdots \times G_s\rangle$ has the property* (QR), *then each $\langle k, G_i\rangle$ has the property* (QR).

PROOF. For each i put $\exp G_i = p_i^{l_i}$ and $k_i = k(\zeta_{\prod_{j\neq i} p_j^{l_j}})$. Further put $W_i = kG_i$, $W_i^{(j)} = k_jG_i$ and $G=G_1\times G_2\times \cdots \times G_s$. Each W_i can be considered as a kG-module and then $W_1\oplus W_2\oplus \cdots \oplus W_s$ is a faithful kG-module. Now suppose that $\langle k, G\rangle$ has the property (QR). By (2.2) $\langle k, G, W_1\oplus W_2\oplus \cdots\oplus W_s\rangle$ has the property (QR) and hence $\langle k_i, G, W_1^{(i)}\oplus W_2^{(i)}\oplus \cdots \oplus W_s^{(i)}\rangle$ has also the property (QR). We see

$$\begin{aligned} &k_i(W_1^{(i)}\oplus \cdots \oplus W_i^{(i)}\oplus \cdots \oplus W_s^{(i)})^G \\ &\quad = k_i(W_i^{(i)})^{G_i}(W_1^{(i)}\oplus \cdots \oplus W_{i-1}^{(i)}\oplus W_{i+1}^{(i)}\oplus \cdots \oplus W_s^{(i)})^{\prod_{j\neq i} G_j}. \end{aligned}$$

Since $\exp \prod_{j\neq i} G_j = \prod_{j\neq i} p_j^{l_j}$ and $\zeta_{\prod_{j\neq i} p_j^{l_j}} \in k_i$, this shows that $k_i(W_1^{(i)}\oplus \cdots \oplus W_i^{(i)}\oplus \cdots \oplus W_s^{(i)})^G$ is rational over $k_i(W_i^{(i)})^{G_i}$. Therefore $\langle k_i, G_i\rangle$ has the property (QR). Since $[k_i(\zeta_{p_i^{l_i}}): k_i] = [k(\zeta_{p_i^{l_i}}): k]$ by the assumption on k, the Masuda's module $M_{W_i^{(i)}}$ of $W_i^{(i)}$ can be identified with the one M_{W_i} of W_i. Thus it follows from (2.4) that each $\langle k, G_i\rangle$ has the property (QR).

The assertion in (4.5) is not always true without the assumption that $k=k^{(p_1)}\cdot k^{(p_2)}\cdot \cdots \cdot k^{(p_s)}$. In fact, let $p_1=47$ and $p_2=139$ and let k_0 be a subfield of $Q(\zeta_{p_1p_2})$ such that $Q(\zeta_{p_1})\subseteqq\!\!\!\!/\; k_0$, $Q(\zeta_{p_2})\subseteqq\!\!\!\!/\; k_0$ and $[Q(\zeta_{p_1p_2}): k_0]=23$. Then $\langle k_0, p_1p_2\rangle$ has the property (R) but any of $\langle k_0, p_1\rangle$ and $\langle k_0, p_2\rangle$ does not have the property (QR).

THEOREM 4.6. *For any finite abelian group G the following conditions are equivalent:*

(1) *$\langle Q, G\rangle$ has the property* (R).

(2) *$\langle Q, G\rangle$ has the property* (QR).

(3) *There is a faithful QG-module V such that the Masuda's module M_V is a quasi-permutation module.*

PROOF. The implication (1)$\Rightarrow$(2) is obvious and the implications (2)$\Leftrightarrow$(3)

follow from (2.2) and (2.4). Hence we have only to prove the implication (2)$\Rightarrow$(1). By (4.5) and (2.3) it suffices to prove this in case G is a p-group.

Let G be a finite abelian p-group of exponent p^l $(l>0)$. We decompose G as follows:

$$G \cong H_{l_1}^{(n_1)} \times H_{l_2}^{(n_2)} \times \cdots \times H_{l_t}^{(n_t)}$$

where $n_i>0$, $1 \leqq l_1 < l_2 < \cdots < l_t = l$ and each H_{l_i} is a cyclic group of order p^{l_i}. Let V_{l_i} be a faithful irreducible QH_{l_i}-module for each i. Let us put $\Pi = \mathrm{Gal}\,(Q(\zeta_{p^l})/Q)$. By (2.4) we have

$$Q(V_{l_1}^{(n_1)} \oplus V_{l_2}^{(n_2)} \oplus \cdots \oplus V_{l_t}^{(n_t)})^G \cong Q(\zeta_{p^l})(I(p^{l_1})^{(n_1)} \oplus I(p^{l_2})^{(n_2)} \oplus \cdots \oplus I(p^{l_t})^{(n_t)}).$$

Here it is remarked that each $I(p^{l_i})$ can be regarded as a Π-module because $\Pi(p^{l_i})$ is the factor group of Π.

Now suppose that $\langle Q, G\rangle$ has the property (QR). Then $I(p^{l_1})^{(n_1)} \oplus I(p^{l_2})^{(n_2)} \oplus \cdots \oplus I(p^{l_t})^{(n_t)}$ is a quasi-permutation Π-module by (2.2) and (2.4). If p is odd, Π is cyclic and each $I(p^{l_i})$ is $\Pi(p^{l_i})$-projective. We see

$$[I(p^{l_1})^{(n_1)} \oplus I(p^{l_2})^{(n_2)} \oplus \cdots \oplus I(p^{l_t})^{(n_t)}]_{\Phi_{p^{l-1}(p-1)}} \cong J(p^{l_t})^{(n_t)}.$$

By (1.11) $J(p^{l_t})^{(n_t)}$ is $Z[\zeta_{p^{l_t-1}(p-1)}]$-free. Hence it follows from the proof of (3.1) that $I(p^{l_t})^{(n_t)}$ is a quasi-permutation Π-module. Then $I(p^{l_1})^{(n_1)} \oplus I(p^{l_2})^{(n_2)} \oplus \cdots \oplus I(p^{l_{t-1}})^{(n_{t-1})}$ is a quasi-permutation Π-module. It can be shown inductively that, for each $1 \leqq i \leqq t$, $I(p^{l_i})^{(n_i)}$ is a quasi-permutation $\Pi(p^{l_i})$-module. Using (1.11) we can conclude that $\langle Q, V_{l_1}^{(n_1)} \oplus V_{l_2}^{(n_2)} \oplus \cdots \oplus V_{l_t}^{(n_t)}\rangle$ has the property (R). On the other hand, if $p=2$, we have $l_t \leqq 2$ (See the proofs of (1.9) and (3.9)), and therefore, by (1.13), we see also that $\langle Q, V_{l_1}^{(n_1)} \oplus V_{l_2}^{(n_2)} \oplus \cdots \oplus V_{l_t}^{(n_t)}\rangle$ has the property (R). It is clear that $V_{l_1}^{(n_1)} \oplus V_{l_2}^{(n_2)} \oplus \cdots \oplus V_{l_t}^{(n_t)}$ can be regarded as a QG-submodule of QG. Consequently $\langle Q, G\rangle$ has the property (R) which completes the proof of the theorem.

Appendix

Primes $p<2000$ such that $J(p)$ is not principal, determined by using a quadratic or biquadratic subfield of $Q(\zeta_{p-1})$	The rest of primes $p<2000$ (except $p=2$ and those in (3.4).)
47 79	53 59 73 83 89 97
113 137 139 167 191	101 103 107 109 127 131 149 151 157 163 173 179 181 193 197 199
223 229 233 239 241 263 277 281 283	211 227 251 257 269 271 293
311 313 317 331 337 349 359 367 373 383	307 347 353 379 389 397

409 421 431 439 457 461 463 479 499	401 419 433 443 449 467 487 491
503 521 523 569 571 593 599	509 541 547 557 563 577 587
601 607 617 619 643 659 661 683	613 631 641 647 653 673 677 691
709 719 733 761 787	701 727 739 743 751 757 769 773 797
809 821 823 829 839 853 857 859 863 877 881 887	811 827 883
907 911 937 941 947 953 967 977 983 991 997	919 929 971
1009 1013 1021 1031 1033 1039 1049 1061 1069 1087 1091 1093 1097	1019 1051 1063
1103 1129 1163 1193	1109 1117 1123 1151 1153 1171 1181 1187
1201 1213 1217 1223 1231 1237 1249 1277 1279 1289 1291	1229 1259 1283 1297
1301 1303 1319 1321 1327 1361 1381 1399	1307 1373
1423 1427 1429 1433 1439 1447 1451 1481 1483 1487 1489 1499	1409 1453 1459 1471 1493
1511 1531 1543 1549 1553 1559 1571 1579 1583 1597	1523 1567
1609 1613 1627 1657 1663 1667 1669 1693 1697 1699	1601 1607 1610 1621 1637
1709 1721 1723 1741 1747 1753 1759 1777 1787 1789	1733 1783
1801 1811 1823 1831 1847 1861 1867 1871 1873 1877 1879 1889	
1913 1933 1951 1973 1979 1987 1993 1997 1999	1901 1907 1931 1949

Added in proof (September 2, 1972). (1) The referee has pointed out to us that the similar result to (2.3) was given by W. Kuyk: Over het omkeer-probleem van de Galoistheorie, Thesis, Amsterdam, 1960. However this paper is not available.

(2) In the case where $k=Q$ and $l=1$, some of the results in § 3 have been shown independently by V. E. Voskresenskii: On the question of the structure of the subfield of invariants of a cyclic group of automorphisms of the field $Q(x_1, x_2, \cdots, x_n)$, Izv. Akad. Nauk USSR, **34** (1970), 366-375; Rationality of certain algebraic tori, Izv. Akad. Nauk USSR, **35** (1971), 1037-1046.

(3) Recently J. Masley has determined all of the positive integers n such

that $c(Q(\zeta_n))=1$. From this it follows directly that $c(Q(\zeta_{p^{l-1}(p-1)}))=1$ if and only if p is one of those in (3.4) ($p\neq 2, 3$).

Department of Mathematics
Tokyo Metropolitan University
Fukazawa, Setagaya-ku, Tokyo, Japan

Department of Mathematics
Osaka City University
Sugimoto, Sumiyoshi-ku
Osaka-shi, Japan

References

[1] C. Chevalley, On algebraic group varieties, J. Math. Soc. Japan, **6** (1954), 303–324.
[2] C. Chevalley, Invariants of finite groups generated by reflexions, Amer. J. Math., 77 (1955), 778–782.
[3] C. W. Curtis and I. Reiner, Representation theory of finite groups and associative algebras, Interscience, 1962.
[4] S. Endo and T. Miyata, Quasi-permutation modules over finite groups, to appear.
[5] E. Fisher, Zur Theorie der Endlichen Abelschen Gruppen, Math. Ann., **77** (1915), 81–88.
[6] H. Kuniyoshi, On a problem of Chevalley, Nagoya Math. J., **8** (1955), 65–67.
[7] K. Masuda, On a problem of Chevalley, Nagoya Math. J., **8** (1955), 59–63.
[8] K. Masuda, Applications 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** (1968), 223–232.
[9] R. Matsuda, On purely-transcendency of certain fields, Tôhoku Math. J., **16** (1964), 189–202.
[10] T. Miyata, Invariants of certain groups, Nagoya Math. J., **41** (1971), 69–73.
[11] E. Noether, Gleichungen mit vorgeschriebener Gruppe, Math. Ann., **78** (1916), 221–229.
[12] T. Ono, On the Tamagawa number of algebraic tori, Ann. of Math., **78** (1963), 47–73.
[13] C. G. Reuschle, Tafeln komplexer Primzahlen, welche aus Wurzeln der Einheit gebildet, Berlin, 1875.
[14] J. P. Serre, Corps locaux, Hermann, Paris, 1962.
[15] R. G. Swan, Invariant rational functions and a problem of Steenrod, Invent. Math., **7** (1969), 148–158.
[16] V. E. Voskresenskiĭ, Birational properties of linear algebraic groups, Izv. Akad. Nauk USSR, **34** (1970), 189–202.