

Werk

Titel: Inventiones mathematicae

Jahr: 1969

Kollektion: Mathematica

Digitalisiert: Niedersächsische Staats- und Universitätsbibliothek Göttingen

Werk Id: PPN356556735_0007

PURL: http://resolver.sub.uni-goettingen.de/purl?PPN356556735_0007

LOG Id: LOG_0017

LOG Titel: Invariant Rational Functions and a Problem of Steenrod.

LOG Typ: article

Übergeordnetes Werk

Werk Id: PPN356556735

PURL: <http://resolver.sub.uni-goettingen.de/purl?PPN356556735>

OPAC: <http://opac.sub.uni-goettingen.de/DB=1/PPN?PPN=356556735>

Terms and Conditions

The Goettingen State and University Library provides access to digitized documents strictly for noncommercial educational, research and private purposes and makes no warranty with regard to their use for other purposes. Some of our collections are protected by copyright. Publication and/or broadcast in any form (including electronic) requires prior written permission from the Goettingen State- and University Library.

Each copy of any part of this document must contain there Terms and Conditions. With the usage of the library's online system to access or download a digitized document you accept the Terms and Conditions.

Reproductions of material on the web site may not be made for or donated to other repositories, nor may be further reproduced without written permission from the Goettingen State- and University Library.

For reproduction requests and permissions, please contact us. If citing materials, please give proper attribution of the source.

Contact

Niedersächsische Staats- und Universitätsbibliothek Göttingen
Georg-August-Universität Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen
Germany
Email: gdz@sub.uni-goettingen.de

Invariant Rational Functions and a Problem of Steenrod

RICHARD G. SWAN (Chicago)

Let k be a field and let $x_1, \dots, x_n$ be indeterminates. The symmetric group S_n acts on the field $K = k(x_1, \dots, x_n)$ by permuting $x_1, \dots, x_n$. If G is any subgroup of S_n , the field $L = K^G$ of elements fixed by G may be described as the field of G -invariant rational functions over k . If $G = S_n$, the field L is a pure transcendental extension of k generated by the elementary symmetric functions. It is an old conjecture of Noether [10] that L is a pure transcendental extension of k for any G . The most important case is that in which k is an algebraic number field. If the conjecture is true in this case, it follows from Hilbert's irreducibility theorem that any group G can be realized as a galois group over k [10, 7]. However, very few results on realizing G as a galois group have been obtained in this way [6], since the conjecture has proved to be extremely intractable. I will show here that there is good reason for this. The conjecture is false even in the simplest case of a cyclic permutation group.

Theorem 1. *Let G be the cyclic group of order p acting transitively on the indeterminates $x_1, \dots, x_p$. Let L be the fixed field $\mathbf{Q}(x_1, \dots, x_p)^G$ where $\mathbf{Q}$ is the field of rationals. Then L is not a pure transcendental extension of $\mathbf{Q}$ for $p = 47$.*

Other values of p for which this holds are 113 and 233. Presumably many others could be obtained by the same method.

My original work on this was done on a completely different problem due to Steenrod. A special case of this was reduced by Kahn to showing that a certain ideal I is principal. After I obtained the results in § 1 below, I found the paper of Masuda [9]. In this paper, Masuda considers the field L of Theorem 1. After some work he arrives at exactly the same ideal I and shows that L is a pure transcendental extension of $\mathbf{Q}$ provided that I is principal. As Masuda remarks [9], it is not at all clear that the converse of this holds. However, I was able to establish a partial converse which led to the result stated in Theorem 1.

In § 3, I will consider Steenrod's original problem and will show again that the answer is negative: In general, there does not exist a finite complex which is a Moore space for $\mathbf{Z}_p = \mathbf{Z}/p\mathbf{Z}$ and which admits $\text{Aut}(\mathbf{Z}_p)$ as a group of operators inducing the given action on $\mathbf{Z}_p$.

I would like to thank D. Kahn and N. E. Steenrod for showing me the problems considered in § 1 and § 3 and the relation between them.

§ 1. A Non-Principal Ideal

Let p be a prime and let $\pi = \text{Aut}(\mathbf{Z}_p)$ be the automorphism group of $\mathbf{Z}_p$. The natural action of π on $\mathbf{Z}_p$ makes $\mathbf{Z}_p$ a module over the group ring $\mathbf{Z}\pi$. Let $\eta: \mathbf{Z}\pi \rightarrow \mathbf{Z}_p$ be the unique $\mathbf{Z}\pi$ -epimorphism with $\eta(1)=1$. More explicitly, π is cyclic of order $p-1$ with a generator T . The action of T on $\mathbf{Z}_p$ is given by multiplication by a primitive $(p-1)$ -th root of 1, $t \in \mathbf{Z}_p$. The map η is then given by $\eta(T^i) = t^i$.

Let I be the kernel of η . The following question was raised by Kahn, Masuda, and Steenrod: Is the ideal I principal? The answer, in general, is negative.

Theorem 2. *If $p=47$, I is not principal.*

The same holds for $p=113$ and $p=233$.

Proof. In view of other possible applications, I will present the proof in slightly more general terms than necessary. To begin with, I will only assume $\pi \subset \text{Aut}(\mathbf{Z}_p)$. Let n be the order of π and T a generator of π . As above $Tx = tx$ for all $x \in \mathbf{Z}_p$ where t is a primitive n -th root of 1 in $\mathbf{Z}_p$. Define $\eta: \mathbf{Z}\pi \rightarrow \mathbf{Z}_p$ as above. Then $I = \ker \eta$ is clearly generated by the elements p and $T-r$ where $r \in \mathbf{Z}$, $r \equiv t \pmod{p}$.

Let ζ be a primitive n -th root of 1. Map $\mathbf{Z}\pi$ into $\mathbf{Q}(\zeta)$ by sending T^i to ζ^i . This is a ring homomorphism whose image is $\mathbf{Z}[\zeta] = \mathfrak{o}$ the ring of integers of $\mathbf{Q}(\zeta)$ [3, Th. 21.13]. Let J be the image of I in $\mathfrak{o}$. If I is principal, J will also be principal. Clearly $J = (p, \zeta - r)$. Since $\mathfrak{o} = \mathbf{Z}[\zeta]$, we see that $\mathfrak{o}/J = \mathbf{Z}_p$ or 0. The latter case is impossible since $J = \mathfrak{o}$ implies that $\zeta - r$ is a local unit at p but $N(\zeta - r) = \Phi_n(r) \equiv \Phi_n(t) \equiv 0 \pmod{p}$ since t is a primitive n -th root of 1. Therefore $N(J) = p$ and our problem is reduced to the following purely number theoretic result.

Theorem 3. *Let $\mathfrak{o}$ be the ring of integers of $\mathbf{Q}(\zeta)$ where ζ is a primitive n -th root of 1. Let $\mathfrak{p}$ be an ideal of $\mathfrak{o}$ with $N\mathfrak{p} = p$. Then $\mathfrak{p}$ is not principal in the following cases: $(p, n) = (47, 23), (47, 46), (113, 112)$, and $(233, 232)$.*

There are, of course, many other cases.

Proof. Suppose $\mathfrak{p} = (\alpha)$. Then $p = N\mathfrak{p} = \pm N_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\alpha)$. If E is any subfield of $\mathbf{Q}(\zeta)$, then $\theta = N_{\mathbf{Q}(\zeta)/E}(\alpha)$ is an integral element with $N_{E/\mathbf{Q}}(\theta) = N_{\mathbf{Q}(\zeta)/\mathbf{Q}}(\alpha) = \pm p$. We apply this to quadratic imaginary subfields of $\mathbf{Q}(\zeta)$. The following (presumably classical) result shows which fields are possible.

Proposition 4. *Let ζ be a primitive n -th root of 1. Then the quadratic subfields of $\mathbf{Q}(\zeta)$ are exactly the fields $\mathbf{Q}(\sqrt{d})$ where $d \in \mathbf{Z}$ is squarefree, $d|n$, $d \neq 1$, and, in addition,*

- (1) *If n or $n/2$ is odd, then $d \equiv 1 \pmod{4}$.*
- (2) *If $4|n$ but $8 \nmid n$, then d is odd.*

The case where n is prime may be found in [18]. In the general case the proof is similar. The primes ramified in $\mathbf{Q}(\sqrt[n]{d})$ will ramify in $\mathbf{Q}(\zeta)$ and so will divide n [4]. This shows that only the fields listed can possibly occur. In case (2), we note instead that all these fields must occur, using case (1) and $\sqrt[n]{-1} \in \mathbf{Q}(\zeta)$. It is now an easy exercise to compute the number of such fields and show that it is equal to the number of quadratic subfields of $\mathbf{Q}(\zeta)$, i.e. to the number of subgroups of index 2 in the galois group $U(\mathbf{Z}_n)$ of $\mathbf{Q}(\zeta)/\mathbf{Q}$.

Now if $p=47$ and $n=23$ or 46, write $p=2m+1$ where $m=23$. By Proposition 4, $\mathbf{Q}(\sqrt{-m}) \subset \mathbf{Q}(\zeta)$ so there would be an integral element $\theta = a + b\frac{1}{2}(1 + \sqrt{-m})$ with $N\theta = p$, i.e. $(2a+b)^2 + mb^2 = 4p$. It is trivial to check that this has no solutions $a, b \in \mathbf{Z}$ for $p=47$, $m=23$.

If $p=113$, write $p=16m+1$ and use $\mathbf{Q}(\sqrt{-2m}) \subset \mathbf{Q}(\zeta)$. If $p=233$, write $p=8m+1$ and use $\mathbf{Q}(\sqrt{-m}) \subset \mathbf{Q}(\zeta)$.

To conclude this section we make some remarks on I and J as modules over $\mathbf{Z}\pi$. Since I is an ideal of finite index p prime to the order n of π , it follows from [15, Prop. 7.1] that I is a projective $\mathbf{Z}\pi$ module. Therefore I is principal if and only if it is free. Since $\mathbf{Z}\pi$ is commutative, a result of Serre [14] shows that I cannot even have a finitely generated free complement if I is not principal.

Let π be cyclic of order n with generator T . Let $\Phi = \Phi_n(T) \in \mathbf{Z}\pi$. Then $\mathbf{Z}\pi/\Phi = \mathbf{Z}[\zeta] = \mathfrak{o}$. If M is a $\mathbf{Z}\pi$ -module, there are two ways to construct an $\mathfrak{o}$ -module from M . Let $M_\Phi = M/\Phi M = \mathbf{Z}\pi/(\Phi) \otimes_{\mathbf{Z}\pi} M$ and $M^\Phi = \{x \in M \mid \Phi x = 0\} = \text{Hom}_{\mathbf{Z}\pi}(\mathbf{Z}\pi/(\Phi), M)$. Define the polynomial $\Psi(x) = (x^n - 1)/\Phi_n(x)$ and let $\Psi = \Psi(T)$. Since $\Psi\Phi = T^n - 1 = 0$, we have $\Psi M \subset M^\Phi$ and we can define a map $\psi: M/\Phi M \rightarrow M^\Phi$ by $\psi(x) = \Psi x$.

Lemma 5. *If P is a projective $\mathbf{Z}\pi$ -module, then $\psi: P/\Phi P \rightarrow P^\Phi$ is an isomorphism.*

Proof. Since both sides preserve direct sums, and P is a direct summand of a free module, it will suffice to do the case $P = \mathbf{Z}\pi$. This amounts to showing that the annihilator of Φ in $\mathbf{Z}\pi$ is (Ψ) while the annihilator of Ψ is (Φ) . Now $\Psi(x)$ is monic with integral coefficients so $\mathbf{Z}\pi/(\Psi) = \mathbf{Z}[x]/(\Psi(x))$ is torsion free. Since $\Psi(x)$ and $\Phi_n(x)$ are relatively prime over $\mathbf{Q}$, the annihilator of $\Phi_n(x)$ in $\mathbf{Z}[x]/(\Psi(x)) \subset \mathbf{Q}[x]/(\Psi(x))$ is 0. Therefore, the annihilator of Φ is (Ψ) . The annihilator of Ψ is (Φ) by the same argument.

Remark. It is clear that in this argument we can replace $\Phi_n(x)$ and $\Psi(x)$ by any pair of polynomials $f(x)$ and $g(x)$ with integral coefficients such that $f(x)g(x) = x^n - 1$.

We now show that J considered as a $\mathbf{Z}\pi$ -module is determined by I as a $\mathbf{Z}\pi$ -module. By definition, J is the image of I under the map $\mathbf{Z}\pi \rightarrow \mathbf{Q}(\zeta)$. This gives an epimorphism $I \rightarrow J$.

Lemma 6. *The kernel of this map $I \rightarrow J$ is ΦI . Therefore $J \approx I_\Phi \approx I^\Phi \approx \Psi I$.*

Proof. Clearly ΦI is contained in the kernel. Since I is projective, $I_\Phi \approx I^\Phi \subset I$ so I_Φ is torsion free. Now $\mathbf{Q} \otimes I = \mathbf{Q} \pi$, $\mathbf{Q} \otimes 0 = \mathbf{Q}(\zeta)$, and $\mathbf{Q} \otimes I_\Phi = (\mathbf{Q} \pi)_\Phi$. Therefore, tensoring the map $I_\Phi \rightarrow J$ with $\mathbf{Q}$ gives $(\mathbf{Q} \pi)_\Phi \rightarrow \mathbf{Q}(\zeta)$, an isomorphism. Therefore, $\ker[I_\Phi \rightarrow J]$ is torsion, but I_Φ is torsion free.

§ 2. Invariant Rational Functions

We first consider a method for defining certain invariants for a field with a group of operators. Let K be a field and π a finite group of automorphisms of K . Let k be a subfield of K which is stable under π . We do not assume that π acts trivially on k . We assume that K has a subring R satisfying the following conditions.

- (1) R is stable under π , $k \subset R$, R is a finitely generated k -algebra, and K is the quotient field of R .
- (2) R is a unique factorization domain and $U(R)/U(k)$ is a finitely generated abelian group.

Here $U(R)$ denotes the group of units of R .

Note that by [12; 7, Ch. II, § 4], the second condition of (2) will hold if k is algebraically closed in K .

By (2), $U(R)/U(k)$ is a finitely generated $\mathbf{Z}\pi$ -module. The invariants will be defined in terms of this module. We begin by investigating its uniqueness.

Definition. A permutation module over $\mathbf{Z}\pi$ is a $\mathbf{Z}\pi$ -module which is free as an abelian group and has a base permuted by π .

Therefore a permutation module is just a direct sum of modules $\mathbf{Z}\pi/\pi'$ where π/π' denotes the left coset space of the subgroup π' .

Lemma 7. *Let $R \subset K$ satisfy (1). Let $a \in R^\pi$ be a non-zero element of R fixed under π . Then $R[a^{-1}]$ also satisfies (1). If in addition R satisfies (2) then $R[a^{-1}]$ satisfies (2) and there is an exact sequence*

$$0 \rightarrow U(R) \rightarrow U(R[a^{-1}]) \rightarrow S \rightarrow 0$$

where S is a finitely generated permutation module over $\mathbf{Z}\pi$.

Consequently, there is an exact sequence

$$(3) \quad 0 \rightarrow U(R)/U(k) \rightarrow U(R[a^{-1}])/U(k) \rightarrow S \rightarrow 0.$$

Proof. It is immediate that $R[a^{-1}]$ satisfies (1). If R is a UFD, so is $R[a^{-1}]$ by [13]. The finite generation of $U(R[a^{-1}])/U(k)$ will follow from the exact sequence (3). Since R is a UFD, we can write $a = up_1^{v_1} \dots p_r^{v_r}$ where u is a unit, $p_1, \dots, p_r$ are non-associated prime elements of R and

$v_i > 0$. If $\sigma \in \pi$, $a = \sigma(a) = \sigma(u) \sigma(p_1)^{v_1} \dots \sigma(p_r)^{v_r}$. By unique factorization, the $\sigma(p_i)$ must be the same as the p_i up to units and a permutation. Therefore, the ideals (p_i) are permuted by π .

Let S be the permutation module with a base $e_1, \dots, e_r$ in one to one correspondence with $(p_1), \dots, (p_r)$. Let π permute $e_1, \dots, e_r$ in the same way as $(p_1), \dots, (p_r)$. Define $U(R[a^{-1}]) \rightarrow S$ by sending $x \in U(R[a^{-1}])$ to $\sum \text{ord}_{p_i}(x) e_i$. This is clearly a $\mathbb{Z}\pi$ -map. If $m_1, \dots, m_r$ and n are positive integers, then $a^{-n} p_1^{m_1} \dots p_r^{m_r}$ is an element of $U(R[a^{-1}])$. Its image in S is $\sum (m_i - n v_i) e_i$. Since all $v_i > 0$ any element of S can be obtained in this way. Thus the map is onto. The kernel consists of elements $y = a^{-n} x \in U(R[a^{-1}])$, $x \in R$, with $\text{ord}_{p_i}(a^{-n} x) = 0$ for all $p_i | a$. Since $\text{ord}_{p_i} a^n = \text{ord}_{p_i} x$ for all $p_i | a^n$, it follows by unique factorization that $a^n | x$, so $y \in R$. Also y^{-1} lies in the kernel so $y^{-1} \in R$ by the same argument. Therefore the kernel of $U(R[a^{-1}]) \rightarrow S$ is $U(R)$.

Lemma 8. *Let $R, R' \subset K$ satisfy (1). Then there are elements $a \in R^\pi$, $a' \in R'^\pi$ with $R[a^{-1}] = R'[a'^{-1}]$.*

Proof. Let $a'_1, \dots, a'_s$ generate R' as a k -algebra. Since K is the quotient field of R we can write $a'_i = x_i/c_i$ with $x_i, c_i \in R$. Let $c = c_1 \dots c_s$ and let $b = \prod \sigma(c)$ taken over all $\sigma \in \pi$. Then $b \in R^\pi$ and $a'_i \in R[b^{-1}]$. Therefore $R' \subset R[b^{-1}]$. If $a \in R[b^{-1}]^\pi$, then $a = d/b^n$ for some $d \in R^\pi$ and $R[b^{-1}] \cdot [a^{-1}] = R[(bd)^{-1}]$. Therefore it will suffice to prove the lemma for $R[b^{-1}]$ and R' . In other words, we can assume $R' \subset R$. By the argument just given, we can find $a \in R'$ such that $R \subset R'[a^{-1}]$. Now $a \in R' \subset R$ so $R'[a^{-1}] \subset R[a^{-1}]$. But the inclusion $R \subset R'[a^{-1}]$ shows that $R[a^{-1}] \subset R'[a^{-1}]$ so $R[a^{-1}] = R'[a^{-1}]$.

It is now easy to define an invariant for the pair of fields $k \subset K$ with the given π -action. Let $G_0(\mathbb{Z}\pi)$ be the Grothendieck group of finitely generated $\mathbb{Z}\pi$ -modules, i.e., the group denoted $G(\mathbb{Z}\pi)$ in [15] and [17]. Let $X \subset G_0(\mathbb{Z}\pi)$ be the subgroup generated by all $[S]$ where S runs over all finitely generated permutation modules over $\mathbb{Z}\pi$. If there is a ring $R \subset K$ satisfying (1) and (2), it follows immediately from Lemmas 7 and 8 that the class $[U(R)/U(k)] \in G_0(\mathbb{Z}\pi)$ is well-defined modulo X . This gives us a well-defined invariant in $G_0(\mathbb{Z}\pi)/X$.

Remark. The requirement that R be a UFD is rather artificial. It would be more natural to require only that R be integrally closed. In this case we must also take account of the divisor class group $C(R)$ [13]. We require this to be finitely generated. The argument of Lemma 7 then leads to an exact sequence

$$0 \rightarrow U(R) \rightarrow U(R[a^{-1}]) \rightarrow S \rightarrow C(R) \rightarrow C(R[a^{-1}]) \rightarrow 0$$

where S is the permutation module corresponding to the permutation representation of π on the set of prime ideals of rank 1 in R which contain

a (cf. [12; 7, Ch. II, § 4]). It follows that $[U(R)/U(k)] - [C(R)] \in G_0(\mathbb{Z}\pi)$ is well-defined mod X . However, the case where R is a UFD, i.e., $C(R) = 0$, will suffice for our purposes.

I will actually use a slightly different invariant in proving Theorem 1. This will be defined in the case where π is cyclic. Suppose π is cyclic of order n with a generator T . Let ζ be a primitive n -th root of 1. As in § 1, map $\mathbb{Z}\pi$ into $\mathbb{Q}(\zeta)$ by sending T to ζ . The image is $\mathbb{Z}[\zeta] = \mathfrak{o}$, the ring of integers of $\mathbb{Q}(\zeta)$. Define $\Phi = \Phi_n(T)$, M_Φ and M^Φ as in § 1 so that M^Φ is an $\mathfrak{o}$ -module, $M^\Phi = \text{Hom}_{\mathbb{Z}\pi}(\mathfrak{o}, M)$.

Lemma 9. *If S is a permutation module over $\mathbb{Z}\pi$ then S^Φ is a free $\mathfrak{o}$ -module. If*

$$0 \rightarrow A \rightarrow B \rightarrow S \rightarrow 0$$

is an exact sequence of $\mathbb{Z}\pi$ -modules where S is a permutation module, then $0 \rightarrow A^\Phi \rightarrow B^\Phi \rightarrow S^\Phi \rightarrow 0$ is an exact sequence.

Thus $B^\Phi \approx A^\Phi \oplus S^\Phi$ as an $\mathfrak{o}$ -module.

Proof. Since S is torsion-free, so is $S^\Phi \subset S$. Since S is a permutation module, it is a direct sum of modules of the form $\mathbb{Z}\pi/\pi'$ where π' runs over various subgroups of π . If $\pi' \neq 1$, $\mathbb{Z}\pi/\pi' = \mathbb{Z}[T]/(T^d - 1)$ where $d = [\pi:\pi']$. Therefore $L = \mathbb{Z}\pi/\pi'$ is annihilated by $T^d - 1$ so L^Φ is annihilated by $\zeta^d - 1$, the image of $T^d - 1$ in $\mathfrak{o}$. Since $d < n$, $\zeta^d - 1 \neq 0$ so L^Φ is a torsion module over $\mathfrak{o}$ and thus also over $\mathbb{Z}$. Since it is torsion free, $L^\Phi = 0$. Now let S' be the sum of all the summands $\mathbb{Z}\pi/\pi'$ of S with $\pi' \neq 1$ and let S'' be the sum of the remaining ones. Then $S = S' \oplus S''$ and S'' is $\mathbb{Z}\pi$ -free. The argument just given shows that $S'^\Phi = 0$. By Lemma 5, $S''^\Phi = S''_\Phi = \mathfrak{o} \otimes_{\mathbb{Z}\pi} S''$. This is clearly a free $\mathfrak{o}$ -module.

Suppose now we have an exact sequence

$$0 \rightarrow A \rightarrow B \xrightarrow{j} S \rightarrow 0.$$

Using the notation just introduced, define $C = j^{-1}(S')$. Then we have the exact sequences

$$(4) \quad 0 \rightarrow A \rightarrow C \rightarrow S' \rightarrow 0,$$

$$(5) \quad 0 \rightarrow C \rightarrow B \rightarrow S'' \rightarrow 0.$$

Since $A^\Phi = \text{Hom}_{\mathbb{Z}\pi}(\mathfrak{o}, A)$ is a left exact functor in A , the sequence (4) gives

$$0 \rightarrow A^\Phi \rightarrow C^\Phi \rightarrow S'^\Phi.$$

Since we have just seen that $S'^\Phi = 0$, it follows that $A^\Phi \rightarrow C^\Phi$ is an isomorphism. Now S'' is free so the sequence (5) splits. Therefore

$$0 \rightarrow C^\Phi \rightarrow B^\Phi \rightarrow S^\Phi \rightarrow 0$$

is exact. Combining this with $A^\Phi = C^\Phi$ gives the required result.

Returning now to our fields $k \subset K$, we assume that π is cyclic and that there is a ring $R \subset K$ satisfying (1) and (2). Consider the $\mathfrak{o}$ -module $(U(R)/U(k))^\Phi$. It follows from Lemmas 7, 8, and 9 that this module is determined up to a free summand by the fields $k \subset K$ and the given π -action. This gives us a number of invariants. The torsion submodule is a well-defined invariant. Since $\mathfrak{o}$ is a Dedekind ring, such modules are classified by a chain of non-zero ideals in $\mathfrak{o}$ [3, 5]. The ideal class of the torsion free part is also an invariant. For our purposes it will suffice to note that $G_0(\mathfrak{o}) = K_0(\mathfrak{o}) = \mathbf{Z} \oplus C(\mathfrak{o})$ where the summand $\mathbf{Z}$ is the subgroup of $G_0(\mathfrak{o})$ generated by the classes of free modules and $C(\mathfrak{o})$ is the class group of $\mathfrak{o}$ [11, Th. 6.19]. Consider the class $[(U(R)/U(k))^\Phi] = (n, \alpha) \in \mathbf{Z} \oplus C(\mathfrak{o})$. Adding or deleting free summands will only change the component n . Therefore $\alpha \in C(\mathfrak{o})$ is an invariant of $k \subset K$ with the given π -action. We write $\alpha = \alpha(k, K, \pi)$.

We now turn to the problem of invariant rational functions and begin by recalling the results of Masuda [9]. Let F be a field and let ζ be a primitive p -th root of 1. We assume that $[F(\zeta):F] = p-1$. This is certainly satisfied for $F = \mathbf{Q}$. Let $x_1, \dots, x_p$ be indeterminates. Let G be a cyclic group of order p permuting $x_1, \dots, x_p$ cyclically. Let $K = F(x_1, \dots, x_p)$. Then G acts on K . Let L be the subfield of G -fixed elements of K . The problem is to determine whether L is a pure transcendental extension of F . Masuda proceeds as follows. Let $\bar{F} = F(\zeta)$. Then $\bar{F}$ and K are linearly disjoint over F . Form the composite fields $\bar{K} = \bar{F}K = \bar{F}(x_1, \dots, x_p)$ and $\bar{L} = \bar{F}L \subset \bar{K}$. Then G acts on $\bar{K}$ and $\bar{K}^G = \bar{L}$. Let

$$y_i = \sum_{j=1}^p \zeta^{ij} x_j \quad \text{for } i=0, 1, \dots, p-1.$$

This transformation has a Vandermonde matrix. Therefore $\bar{K} = \bar{F}(y_0, \dots, y_{p-1})$. Now let π be the galois group of $\bar{F}/F$. Thus π is cyclic of order $p-1$. By linear disjointness, π is also the galois group of $\bar{K}/K$ and $\bar{L}/L$. Clearly, π fixes y_0 and it is easy to see that π permutes $y_1, \dots, y_{p-1}$ freely. Let $\bar{M}$ be the subgroup of $U(\bar{K})$ generated by $y_1, \dots, y_{p-1}$. Then $\bar{M}$ is a free $\mathbf{Z}\pi$ -module on y_1 . Let $M = \bar{M} \cap \bar{L}$. This is a $\mathbf{Z}\pi$ -submodule of $\bar{M}$. Masuda shows that if M is $\mathbf{Z}\pi$ -free, then L is purely transcendental over F [8]. He also shows that $M \approx I$, the ideal considered in § 1. This is done as follows. Let σ be the generator of G . Then $\sigma(y_i) = \zeta^i y_i$. Therefore $y_1^{-i} y_i \in M$ and $y_1^p \in M$. These elements generate a submodule of $\bar{M}$ of index p which must be M . The only other possibility would be $M = \bar{M}$. This would imply $\bar{M} \subset \bar{L}$ so $\bar{K} = \bar{F}(\bar{M}) \subset \bar{L}$, a contradiction. Let T be a generator of π . Then $T(\zeta) = \zeta^t$ where t is a primitive $(p-1)$ -th root of 1 mod p . Therefore $T(y_i) = y_{ti}$. If we identify the free module $\bar{M}$ with $\mathbf{Z}\pi$ by letting y_1 correspond to 1, the elements $y_1^{-t^i} y_i^t$ and y_1^p will cor-

respond to $T^v - t^v$ and p respectively. Therefore M corresponds to the ideal I generated by p and $T - t$, i.e., the ideal I of § 1.

We will also need the fact that $\bar{L} = \bar{F}(M, y_0)$. Masuda proves this by observing that $\bar{K} \supset \bar{L} \supset \bar{F}(M, y_0)$ while $\bar{K} = \bar{F}(\bar{M}, y_0) = \bar{F}(M, y_0)(y_1)$ has degree $\leq p = [\bar{K} : \bar{L}]$ over $\bar{F}(M, y_0)$.

To obtain the converse of Masuda's results we use the invariants $\alpha(\bar{F}, \bar{L}, \pi)$ defined above. For the ring R we use the subring $R = \bar{F}[M, y_0]$ generated over $\bar{F}$ by y_0 and the elements of M . Now M is free abelian of rank $p - 1$. Let $m_1, \dots, m_{p-1}$ be a base for M . Then

$$R = \bar{F}[y_0, m_1, m_1^{-1}, \dots, m_{p-1}, m_{p-1}^{-1}].$$

Since $\bar{L} = \bar{F}(y_0, m_1, \dots, m_{p-1})$ has transcendence degree p over $\bar{F}$, the elements $y_0, m_1, \dots, m_{p-1}$ must be algebraically independent over $\bar{F}$. It follows that R is a UFD and that $U(R)/U(\bar{F})$ is free abelian on $m_1, \dots, m_{p-1}$, i.e., $U(R)/U(\bar{F}) = M$. The conditions (1), (2) are obviously satisfied. Therefore $\alpha(\bar{F}, \bar{L}, \pi) = [M^\Phi] = [I^\Phi] = [J] \in C(\mathfrak{o})$ by Lemma 6.

Suppose now that L is a pure transcendental extension of F . Let $L = F(z_1, \dots, z_p)$ where $z_1, \dots, z_p$ are algebraically independent over F . Then $\bar{L} = \bar{F}L = \bar{F}(z_1, \dots, z_p)$. Let $R' = \bar{F}[z_1, \dots, z_p]$. Since the z_i are fixed under π , R' is stable under π . Conditions (1) and (2) are satisfied so $\alpha(\bar{F}, \bar{L}, \pi) = [(U(R')/U(\bar{F}))^\Phi]$ but $U(R')/U(\bar{F}) = 1$. Therefore our assumption implies that $[J] = 0$ in $C(\mathfrak{o})$. This is false for $p = 47$ by Theorem 3. Thus we have proved the following result which includes Theorem 1.

Theorem 10. *Let F be a field such that $[F(\zeta):F] = p - 1$ where ζ is a primitive $(p - 1)$ -th root of 1. Let $x_1, \dots, x_p$ be indeterminates and let G be a cyclic group of order p permuting $x_1, \dots, x_p$ transitively. Let L be the fixed field $F(x_1, \dots, x_p)^G$. Then L is not a pure transcendental extension of F if $p = 47$.*

Other possible values are $p = 113$ and $p = 233$.

§ 3. Steenrod's Problem

The following problem was proposed by Steenrod in 1960: Let A be a finitely generated abelian group and π a finite group of automorphisms of A . Let n be a positive integer. Is there a finite complex K with $\hat{H}_i(K) = 0$ for $i \neq n$, $H_n(K) = A$ such that π acts on K , preserving the cellular structure, and induces the given action on $A = H_n(K)$?

The simplest non-trivial case is the one in which $A = \mathbb{Z}_p$. It will clearly suffice to look at the case $\pi = \text{Aut}(\mathbb{Z}_p)$ the full automorphism group of $\mathbb{Z}_p$. In this case Kahn observed that it would be sufficient for the ideal I of § 1 to be free. His argument runs as follows. Let L be a bouquet of n -spheres permuted freely by π . Then $H_n(L) = \mathbb{Z}\pi$. Let $\alpha \in \mathbb{Z}\pi$

be a generator of I . Represent α by a map $f: S^n \rightarrow L$ and attach $(n+1)$ -cells to L by the maps σf , $\sigma \in \pi$. Let π permute these $(n+1)$ -cells freely in the obvious way. The resulting complex will be the required K . This argument obviously generalizes to show that K exists provided that there is an exact sequence

$$0 \rightarrow F' \rightarrow F \rightarrow A \rightarrow 0$$

with F and F' finitely generated free $\mathbf{Z}\pi$ -modules. If A has finite projective dimension over $\mathbf{Z}\pi$, there will be a sequence

$$0 \rightarrow P \rightarrow F \rightarrow A \rightarrow 0$$

with P projective [11, Th. 4.12]. We use here the finiteness of π . By a well-known remark of Eilenberg [16, p. 276] [1], if F' is a sufficiently big free module, $P \oplus F'$ will be free. Applying Kahn's method to the resolution

$$0 \rightarrow P \oplus F' \rightarrow F \oplus F' \rightarrow A \rightarrow 0$$

shows that we can find an *infinite* complex K with the required properties provided that A has finite projective dimension over $\mathbf{Z}\pi$.

I will now show that in general it is not possible to find a finite complex K with the above properties, even in the case $A = \mathbf{Z}_p$. It is not necessary to use the full automorphism group for this.

Theorem 11. *Let $p=47$ and let $\pi \subset \text{Aut}(\mathbf{Z}_p)$ have order 23. Then there is no finite complex K with $\tilde{H}_i(K)=0$ for $i \neq n$, $H_n(K)=\mathbf{Z}_p$ which admits π as a group of operators, preserving the cellular structure, and inducing the given action on $\mathbf{Z}_p = H_n(K)$.*

Proof. Assume such a complex K exists. Let C be its augmented chain complex. Then each C_i is a $\mathbf{Z}\pi$ -module. As an abelian group, C_i is free and has a base permuted up to sign by π , i.e., the base consisting of the i -cells of K . I will refer to such a $\mathbf{Z}\pi$ -module as a signed permutation module. Theorem 11 is now a consequence of the following algebraic result.

Theorem 12. *Let $p=47$ and let $\pi \subset \text{Aut}(\mathbf{Z}_p)$ have order 23. Then there is no finite dimensional chain complex C over $\mathbf{Z}\pi$ such that each C_i is a finitely generated signed permutation module, $H_i(C)=0$ for $i \neq n$, and $H_n(C)=\mathbf{Z}_p$ with the given action of π .*

Proof. Assume there is such a complex. Consider the Grothendieck group $G_0(\mathbf{Z}\pi)$ of all finitely generated $\mathbf{Z}\pi$ -modules (denoted $G(\mathbf{Z}\pi)$ in [15] and [17]). If C is a finite dimensional chain complex of finitely generated $\mathbf{Z}\pi$ -modules, the usual Euler characteristic argument shows that $\sum (-1)^i [C_i] = \sum (-1)^i [H_i(C)]$ in $G_0(\mathbf{Z}\pi)$. We merely consider the sequences $0 \rightarrow Z_i \rightarrow C_i \rightarrow B_{i-1} \rightarrow 0$ and $0 \rightarrow B_i \rightarrow Z_i \rightarrow H_i \rightarrow 0$. Therefore $[\mathbf{Z}_p]$ lies in the subgroup of $G_0(\mathbf{Z}\pi)$ generated by the classes of signed permutation modules.

Let T be a generator of π . Let S be a signed permutation module and let e be one of the basis elements specified by the definition of such a module. Since π is cyclic of prime order, the orbit of $\{\pm e\}$ under π is either $\{\pm e\}$ or $\{\pm e_1, \dots, \pm e_p\}$ where $e = e_1, e_2, \dots, e_p$ are distinct basis elements. If it is $\{\pm e\}$, we have $Te = \pm e$. Since T has odd order, we must have $Te = e$. In the other case, the $T^i e$, $0 \leq i < p$ must be independent. This shows that any signed permutation module over $\mathbf{Z}\pi$ for π cyclic of odd prime order must be a direct sum of copies of $\mathbf{Z}\pi$ and $\mathbf{Z}$. We conclude that $[\mathbf{Z}_p]$ lies in the subgroup of $G_0(\mathbf{Z}\pi)$ generated by $[\mathbf{Z}\pi]$ and $[\mathbf{Z}]$. Since $[\mathbf{Z}_p] = [\mathbf{Z}\pi] - [I]$ where I is as in § 1, we conclude that $[I]$ lies in this subgroup.

Now $\mathbf{Q}\pi = \mathbf{Q} \times \mathbf{Q}(\zeta)$ where ζ is a primitive 23-rd root of 1. This has the unique maximal order $A = \mathbf{Z} \times \mathfrak{o}$. In [17, § 13], I showed that

$$G_0(\mathbf{Z}\pi) \approx G_0(A) = G_0(\mathbf{Z}) \times G_0(\mathfrak{o}) = \mathbf{Z} \oplus \mathbf{Z} \oplus C_0(\mathfrak{o}),$$

where $C_0(\mathfrak{o})$ is the class group of $\mathfrak{o}$, and the two factors $\mathbf{Z}$ are generated by the elements $[\mathbf{Z}]$ and $[\mathfrak{o}]$ respectively. The map $G_0(A) \rightarrow G_0(\mathbf{Z}\pi)$ is given by sending each $[M]$ into $[M]$ where M is regarded as a $\mathbf{Z}\pi$ -module. The exact sequence $0 \rightarrow \mathbf{Z} \rightarrow \mathbf{Z}\pi \rightarrow \mathfrak{o} \rightarrow 0$ shows that in $G_0(\mathbf{Z}\pi)$, $[\mathfrak{o}] = [\mathbf{Z}\pi] - [\mathbf{Z}]$. Therefore the subgroup of $G_0(\mathbf{Z}\pi)$ generated by $[\mathbf{Z}]$ and $[\mathbf{Z}\pi]$ corresponds under the above isomorphism to the summand $\mathbf{Z} \oplus \mathbf{Z}$ of $G_0(A)$.

We must now determine the image of $[I]$ in $G_0(A)$. Since I is torsion free we can apply the map given in [17, § 13] and conclude that the image of $[I]$ in $G_0(\mathfrak{o})$ is $[\Psi_n(T)I] = [J]$ by Lemma 6. Now $[J] - [\mathfrak{o}] \in C_0(\mathfrak{o})$ is the class of the ideal J . This is non-zero by Theorem 3. Therefore $[J]$ does not lie in the summand $\mathbf{Z}$ of $G_0(\mathfrak{o}) = \mathbf{Z} \oplus C_0(\mathfrak{o})$. This gives the required contradiction.

Remark. This argument can obviously be extended to give other examples. If we consider subgroups π not of prime order, several additional difficulties appear. The results of [17, § 13] no longer apply. Instead we define directly a map from $G_0(\mathbf{Z}\pi)$ to $G_0(\mathfrak{o})$ by sending $[M]$ to $[M^\Phi]$ as in § 1. This is not well defined since $M \rightarrow M^\Phi$ is not exact. However, $M^\Phi = \text{Hom}_{\mathbf{Z}\pi}(\mathfrak{o}, M)$ so $0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$ leads to

$$0 \rightarrow M'^\Phi \rightarrow M^\Phi \rightarrow M''^\Phi \rightarrow \text{Ext}_{\mathbf{Z}\pi}^1(\mathfrak{o}, M').$$

Since $\mathfrak{o}$ is $\mathbf{Z}$ -free, $\text{Ext}_{\mathbf{Z}\pi}^1(\mathfrak{o}, M') = H^1(\pi, \text{Hom}(\mathfrak{o}, M'))$ by [2, Ch. XV, § 7 (6)]. This is annihilated by n by [2, Ch. XII, Prop. 2.5]. Therefore if we let $W \subset C_0(\mathfrak{o})$ be the subgroup generated by the classes of ideals dividing n , we get a well-defined map $G_0(\mathbf{Z}\pi) \rightarrow G_0(\mathfrak{o})/W$ and thus a map $\delta: G_0(\mathbf{Z}\pi) \rightarrow C_0(\mathfrak{o})/W$. Using Lemma 5 and the remark following it, it is easy to show that S^Φ is $\mathfrak{o}$ -free if S is a signed permutation module. There-

fore the existence of a complex as in Theorem 12 implies that $\delta[I]=0$ or that $[J] \in W$. Therefore there is an ideal $\mathfrak{a} \subset \mathfrak{o}$ composed of primes dividing n with $\mathfrak{a}J$ principal. If E is a subfield of $\mathbf{Q}(\zeta)$, we conclude that there is an integral element θ of E with $N\theta = \pm mp$ where all primes dividing m also divide n . If E is quadratic and all primes dividing n are ramified or inertial in E , we can easily reduce to the case where m is squarefree. This gives a finite number of possibilities. My original version of Theorem 11 used this method for $p=233$, $\pi = \text{Aut}(\mathbf{Z}_p)$. I then noticed that the proof could be simplified by restricting to the subgroup of order 29 of $\text{Aut}(\mathbf{Z}_p)$.

Finally, it should be noted that Steenrod's problem remains open if the finiteness condition on K is omitted.

References

1. Bass, H.: Big projective modules are free. III. *J. Math.* **7**, 24–31 (1963).
2. Cartan, H., and S. Eilenberg: *Homological algebra*. Princeton, 1956.
3. Curtis, C.W., and I. Reiner: *Representation theory of finite groups and associative algebras*. New York: Interscience 1962.
4. Hasse, H.: *Zahlentheorie*. Berlin: Akademie-Verlag 1963.
5. Kaplansky, I.: Modules over Dedekind rings and valuation rings. *Trans. Amer. Math. Soc.* **72**, 327–340 (1952).
6. Kuyk, W.: On a theorem of E. Noether. *Nederl. Akad. Wetensch. Proc., Ser. A* **67**, 32–39 (1964).
7. Lang, S.: *Diophantine geometry*. New York: Interscience 1962.
8. Masuda, K.: On a problem of Chevalley. *Nagoya Math. J.* **8**, 59–63 (1955).
9. — 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).
10. Noether, E.: Gleichungen mit vorgeschriebener Gruppe. *Math. Ann.* **78**, 221–229 (1916).
11. Rim, D. S.: Modules over finite groups. *Ann. of Math.* **69**, 700–712 (1959).
12. Roquette, P.: Einheiten und Divisorenklassen in endlich erzeugbaren Körpern. *J. Deutsch. Math. Verein* **60**, 1–27 (1958).
13. Samuel, P.: Sur les anneaux factoriels. *Bull. Soc. Math. France* **89**, 155–173 (1961).
14. Serre, J.-P.: Modules projectifs et espaces fibrés à fibre vectorielle. *Sem. Dubreil, Paris* 1958.
15. Swan, R. G.: Induced representations and projective modules. *Ann. of Math.* **71**, 552–578 (1960).
16. — Periodic resolutions for finite groups. *Ann. of Math.* **72**, 267–291 (1960).
17. — The Grothendieck ring of a finite group. *Topology* **2**, 85–110 (1963).
18. Zariski, O., and P. Samuel: *Commutative algebra*. Vol. I. Princeton: Van Nostrand 1958.

Richard G. Swan
The University of Chicago
Department of Mathematics
Chicago, Ill. 60637 (USA)

(Received October 24, 1968)