ACTA ARITHMETICA
IX (1964)

Class group of cohomologically trivial modules and cyclotomic ideals

by

T. Nakayama (Nagoya)

To L. J. Mordell
on the occasion of his 75th birthday

We wish, in the present short paper, to study the structure of the class group of cohomologically trivial modules over a finite group G, on introducing the notion of this class group in analogy to that of projective class groups; for projective class groups, see Rim [9], [10], Swan [12], [14]. It turns out, mainly by virtue of Schanuel's lemma (cf. Swan [13]) and the characterization of cohomologically trivial modules by projective dimension (Nakayama [7], Rim [9]), that our class group is in fact isomorphic to the projective class group; such isomorphism appears already at the level of Grothendieck groups. The advantage, or reward rather, of dealing with the class group of cohomologically trivial modules is, however, in that modules of finite order may be taken as class representatives. Indeed, we shall prove that the elements of the Grothendieck group of (finitely generated) cohomologically trivial modules represented by modules of finite order form a splitting subgroup isomorphic to the class group of cohomologically trivial modules. Toward the end of our paper, we consider the case where G is a cyclic group of prime order, and we represent the class group in this case by residue-modules of cyclotomic ideals, making use of Rim's result [9] on the projective class group of the group G.

1. Grothendieck group of finite-dimensional modules. Let Λ be a (left) Noetherian ring, and let $\mathfrak{M} = \mathfrak{M}_\Lambda$ be the category of all finitely generated (f.g.) Λ-(left-) modules with finite projective dimension. The Grothendieck group $\mathfrak{G}(\mathfrak{M})$ associated with the category $\mathfrak{M}$, or the Grothendieck group of f.g. finite-dimensional Λ-modules, in short, is by definition the factor group of the free abelian group generated by the (Λ-) isomorphism classes (M) of modules M in $\mathfrak{M}$ modulo the subgroup generated by the elements of form $(M)-(M')-(M'')$ with $M, M', M'' \in \mathfrak{M}$ forming an exact sequence

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

in $\mathfrak{M}$. By $\langle M\rangle$ we denote its element represented by (M), or by M, in short.

In this number we shall show that the group $\mathfrak{G}(\mathfrak{M})$ is isomorphic, in a natural manner, with the Grothendieck group $\mathfrak{G}(\mathfrak{P})$ associated with the category $\mathfrak{P} = \mathfrak{P}_\Lambda$ of all f.g. projective Λ-modules. By the nature of projective modules, this latter group is explained in terms of splitting exact sequences, and thus in terms of direct sum decompositions, which makes both the notion itself and its handling simpler. We denote by $[P]$ the element of the group $\mathfrak{G}(\mathfrak{P})$ represented by (the isomorphism class (P) of) a f.g. projective module P.

Now, let M be a f.g. finite-dimensional Λ-module, i.e. an object in $\mathfrak{M}$, and let

$$0 \leftarrow M \leftarrow P_0 \leftarrow \dots \leftarrow P_h \leftarrow 0 \tag{1}$$

be its projective resolution of finite length with f.g. projective Λ-modules. To M we associate the element

$$[P_0]-[P_1]+\dots\pm[P_h] \tag{2}$$

of $\mathfrak{G}(\mathfrak{P})$. We contend that this element (2) of $\mathfrak{G}(\mathfrak{P})$ is independent of the choice (1) of a projective resolution (of finite length by f.g. projective modules) of M. For, let

$$0 \leftarrow M \leftarrow P'_0 \leftarrow \dots \leftarrow P'_{h'} \leftarrow 0$$

also be a projective resolution of M. Supplementing one of the sequences with terms 0, if necessary, we may assume $h = h'$. And, if $h\ (=h') = 0$, then the contention is trivial. So, suppose $h\ (=h') > 1$. We have

$$\begin{aligned} &0 \leftarrow M \leftarrow P_0 \leftarrow K \leftarrow 0, \\ &0 \leftarrow M \leftarrow P'_0 \leftarrow K' \leftarrow 0 \end{aligned} \tag{3}$$

with K, K' denoting the kernel of the maps $P_0 \leftarrow P_1$, $P'_0 \leftarrow P'_1$ respectively. We have also two exact sequences

$$\begin{aligned} &0 \leftarrow K \leftarrow P_1 \leftarrow P_2 \leftarrow \dots \leftarrow P_h \leftarrow 0, \\ &0 \leftarrow K' \leftarrow P'_1 \leftarrow P'_2 \leftarrow \dots \leftarrow P'_h \leftarrow 0. \end{aligned}$$

From these two exact sequences we derive the exact sequences

$$\begin{aligned} &0 \leftarrow K\oplus P'_0 \leftarrow P_1\oplus P'_0 \leftarrow P_2 \leftarrow \dots \leftarrow P_h \leftarrow 0, \\ &0 \leftarrow K'\oplus P_0 \leftarrow P'_1\oplus P_0 \leftarrow P'_2 \leftarrow \dots \leftarrow P'_h \leftarrow 0, \end{aligned} \tag{4}$$

with easily conceivable significances of first several arrows in each of them.

Now, by Schanuel's lemma (cf. Swan [13]) the exact sequences (3) entail an isomorphism

$$K\oplus P'_0 \approx K'\oplus P_0. \tag{5}$$

So, in (4) we have, essentially, two projective resolutions of a single module. If we here assume (that $P'_0, P'_1, \dots, P'_h$ are also f.g. and)

$$[P_1\oplus P'_0]-[P_2]+\dots\mp[P_h] = [P'_1\oplus P_0]-[P'_2]+\dots\mp[P'_h],$$

then

$$[P_0]-[P_1]+[P_2]-\dots\pm[P_h] = [P'_0]-[P'_1]+[P'_2]-\dots\pm[P'_h].$$

This reduces the problem to the case of projective resolutions, (4), of length $< h$. Repeating the argument we arrive at a case of two sequences of length 0 (with 3 arrows in each), which is rather trivial.

Thus we have proved, with Schanuel's lemma as the main tool

LEMMA 1. *With each f.g. finite-dimensional Λ-module M, the element (2) of the Grothendieck group $\mathfrak{G}(\mathfrak{P})$ is uniquely associated, where P_i are f.g. projective Λ-modules in an exact sequence* (1).

It is evident that the element (2) is determined uniquely by the isomorphism class of M. So, mapping (M) to (2) (and extending the map) we obtain a homomorphism into $\mathfrak{G}(\mathfrak{P})$ of the free abelian group generated by all isomorphism classes of f.g. finite-dimensional Λ-modules. We assert

LEMMA 2. *In this homomorphism, defined by $(M)\to(2)$ (with (1) exact), an element of form $(M)-(M')-(M'')$ is mapped to 0 of $\mathfrak{G}(\mathfrak{P})$ when we have an exact sequence*

$$0 \to M' \to M \to M'' \to 0. \tag{5}$$

To prove this, we choose h sufficiently large so that we have exact sequences

$$\begin{aligned} &0 \leftarrow M' \leftarrow P'_0 \leftarrow \dots \leftarrow P'_h \leftarrow 0, \\ &0 \leftarrow M'' \leftarrow P''_0 \leftarrow \dots \leftarrow P''_h \leftarrow 0 \end{aligned}$$

with f.g. projective Λ-modules (possibly 0) P'_i, P''_i. By Cartan-Eilenberg [2], Chap. V, Prop. 2.2, there exists then a projective resolution (by f.g. projective modules)

$$0 \leftarrow M \leftarrow P_0 \leftarrow \dots \leftarrow P_h \leftarrow 0$$

of M, such that we have an exact sequence

$$0 \to P'_i \to P_i \to P''_i \to 0$$

for each $i = 0, 1, \ldots, h$. The element $(M)-(M')-(M'')$ is mapped to

$$([P_0]-[P_1]+\ldots\pm[P_h])-([P'_0]-[P'_1]+\ldots\pm[P'_h])-$$
$$-([P''_0]-[P''_1]+\ldots\pm[P''_h])$$
$$=([P_0]-[P'_0]-[P''_0])-([P_1]-[P'_1]-[P''_1])+\ldots\pm$$
$$\pm([P_h]-[P'_h]-[P''_h]) = 0.$$

We now see, by our lemmas, that $\langle M\rangle \to (2)$ (with (1) exact) defines a homomorphism

$$\varrho : \mathfrak{G}(\mathfrak{M}) \to \mathfrak{G}(\mathfrak{P})$$

of $\mathfrak{G}(\mathfrak{M})$ into $\mathfrak{G}(\mathfrak{P})$.

On the other hand, each object in $\mathfrak{P}$ is evidently an object in $\mathfrak{M}$ (and each map in $\mathfrak{P}$ is a map in $\mathfrak{M}$). By $[P] \to \langle P\rangle$ we have thus a homomorphism

$$\iota : \mathfrak{G}(\mathfrak{P}) \to \mathfrak{G}(\mathfrak{M})$$

of $\mathfrak{G}(\mathfrak{P})$ into $\mathfrak{G}(\mathfrak{M})$. ι is epimorphic. For, the exact sequence (1) entails indeed

$$\langle M\rangle = \langle P_0\rangle - \langle P_1\rangle + \langle P_2\rangle - \ldots \pm \langle P_h\rangle .$$

The composite $\varrho\circ\iota$ is the identity map of $\mathfrak{G}(\mathfrak{P})$. It follows, since ι is epimorphic, that both ϱ and ι are isomorphic:

$$\mathfrak{G}(\mathfrak{M}) \approx \mathfrak{G}(\mathfrak{P}).$$

So we have

PROPOSITION 1. *The Grothendieck groups $\mathfrak{G}(\mathfrak{P})$ and $\mathfrak{G}(\mathfrak{M})$, of f.g. projective Λ-modules and f.g. finite-dimensional Λ-modules respectively, are isomorphic by the natural isomorphism associating $[P]$ in $\mathfrak{G}(\mathfrak{P})$ with $\langle P\rangle$ in $\mathfrak{G}(\mathfrak{M})$.*

Remark 1. We have been, as we shall be too, considering (f.g.) (left-) modules over a (left-) Noetherian ring Λ. In the case of a general non-Noetherian ring Λ, we have, in order to make a same thing, merely to restrict ourselves to the category of f.g. finite-dimensional Λ-modules having a resolution of finite length by f.g. projective Λ-modules.

Remark 2. The same argument holds also for the Grothendieck groups of non-f.g. (i.e. not necessarily f.g.) projective modules and non-f.g. finite-dimensional modules (with Λ Noetherian or not). However, their Grothendieck groups (which are thus essentially a same thing) are (essentially a same thing also with the Grothendieck group of free modules, and are) trivial; they are identity groups.

2. Class groups. In the isomorphism of Proposition 1 the subgroup of $\mathfrak{G}(\mathfrak{P})$ generated by elements represented by f.g. free modules corresponds to the subgroup of $\mathfrak{G}(\mathfrak{M})$ generated by elements represented by f.g. free modules. The factor group $\mathfrak{C}(\mathfrak{P})$ of $\mathfrak{G}(\mathfrak{P})$ modulo the said subgroup is called the *projective class group*; cf. Rim [9], [10], Swan [12], [14]. The factor group $\mathfrak{C}(\mathfrak{M})$ of $\mathfrak{G}(\mathfrak{M})$ modulo the above said corresponding subgroup may perhaps properly be called the *class group of finite-dimensional modules*. These two class groups, $\mathfrak{C}(\mathfrak{P})$ and $\mathfrak{C}(\mathfrak{M})$, are thus isomorphic, by the isomorphism induced by the isomorphism of Proposition 1, and are essentially a same thing. The projective class group is sometimes denoted by $\mathfrak{C}(\Lambda)$.

3. Cohomologically trivial modules. Let G be a finite group. We consider the case where Λ is the group ring $Z(G)$ of G over the rational integers Z. A G-(equivalently, $Z(G)$-) module M is called *cohomologically trivial* when its (Artin-Tate) cohomology groups $H^i(G, M)$ $(i = 0, \pm 1, \pm 2, \ldots)$ are all 0. In [7] the writer showed that every f.g. cohomologically trivial module is finite-dimensional (indeed of dimension $\leqslant 1$) (and conversely); Rim [9] has proved, by a much better method, that the same holds for non-f.g. modules too (cf. Serre [11]). Thus, in the case of $\Lambda = Z(G)$ our category $\mathfrak{M}$ of f.g. finite-dimensional (G-, i.e. $Z(G)$-) modules is nothing but the category of f.g. cohomologically trivial (G-) modules, and our result may be interpreted as: *the Grothendieck group of f.g. cohomologically trivial modules* (*resp. the class group of cohomologically trivial modules*) *over a finite group G is essentially the same thing as the Grothendieck group of f.g. projective modules* (*resp. the projective class group*) *over G*. (Here we use the term class group of cohomologically trivial modules in the same way as the term class group of finite-dimensional modules.) The projective class group $\mathfrak{C}(\mathfrak{P})$ in group case is often denoted by $\mathfrak{C}(G)$.

Remark 3. The subgroup of the Grothendieck group $\mathfrak{G}(\mathfrak{M})$ of f.g. cohomologically trivial modules generated by elements represented by f.g. free modules may also be characterized as the subgroup generated by elements represented by f.g. regular modules. For, (a free module is evidently regular while) a regular G-module has, by definition, a form $Z(G)\otimes_Z M_0$ with a Z-module M_0 and, if $M_0 \approx F/F'$ with Z-free modules F, F', we have $Z(G)\otimes_Z M_0 \approx Z(G)\otimes_Z F/Z(G)\otimes_Z F'$ with $Z(G)\otimes_Z F$, $Z(G)\otimes_Z F'$ free over $Z(G)$; if here $Z(G)\otimes_Z M_0$ is ($Z(G)$-, equivalently Z-) f.g. then M_0 (isomorphic with $(Z(G)\otimes_Z M_0)^G$) is (Z-) f.g. and F, F' may be taken f.g.

Remark 4. If M is cohomologically trivial, then proj. dim M is (not only finite but) $\leqslant 1$ as is remarked above. So, M has a projective resolution of form $0 \leftarrow M \leftarrow P_0 \leftarrow P_1 \leftarrow 0$ (P_i projective). If M is f.g.

then P_0, P_1 may be taken f.g., and the element $\langle M\rangle$ in $\mathfrak{G}(\mathfrak{M})$ corresponds, by our map ϱ, to the element $[P_0]-[P_1]$ in $\mathfrak{G}(\mathfrak{P})$. If we further choose P_0 (f.g.) free to have $0 \leftarrow M \leftarrow F \leftarrow P \leftarrow 0$ exact (F f.g. free, P f.g. projective), then the class of $\langle M\rangle$ in $\mathfrak{C}(\mathfrak{M})$ corresponds to the class of $-[P]$ in $\mathfrak{C}(\mathfrak{P}) = \mathfrak{C}(G)$.

4. Cohomologically trivial modules of finite order. In the same note [7] (Proposition 6) the writer also showed that every f.g. projective G-module P has a Z-rank divisible by the order of G. Using this fact and using characters as well as an analysis of a cyclic group case, Swan [12] (Theorem 8.1) showed that $Q\otimes_Z P$ is free over the group ring over the rationals Q. It follows then that there is a (f.g.) free G-submodule F in P such that the residue-module P/F is of finite order. This residue-module $M = P/F$ is evidently cohomologically trivial and $\langle M\rangle$ belongs to the same element (class) in the class group of cohomologically trivial modules as $\langle P\rangle$. Since the class group of cohomologically trivial modules is essentially the same thing as the projective class group, as we have seen, we have thus

PROPOSITION 2. *Every element (class) in the class group $\mathfrak{C}(\mathfrak{M})$ of cohomologically trivial modules over a finite group G contains an element (of the Grothendieck group $\mathfrak{G}(\mathfrak{M})$) represented by cohomologically trivial G-module of finite order.*

Now, consider the category $\mathfrak{N}$ of cohomologically trivial G-modules of finite order. Our proposition entails that the composite of the natural map of the Grothendieck group $\mathfrak{G}(\mathfrak{N})$ to $\mathfrak{C}(\mathfrak{M})$ and the map ϱ in Section 1 (inverse to ι in Section 1) induces an epimorphism of $\mathfrak{C}(\mathfrak{N})$ to the projective class group $\mathfrak{C}(\mathfrak{P}) = \mathfrak{C}(G)$; this is almost equivalent to our proposition, but is somewhat weaker than it.

The kernel, $\mathfrak{K}$, of this epimorphism (or, equivalently, of the epimorphism $\mathfrak{G}(\mathfrak{N}) \to \mathfrak{C}(\mathfrak{M})$ induced by the natural homomorphism $\mathfrak{G}(\mathfrak{N}) \to \mathfrak{G}(\mathfrak{M})$) contains the subgroup, $\mathfrak{S}$, generated by elements represented by regular G-modules of finite order. Indeed, $\mathfrak{S}$ is contained already in the kernel $\mathfrak{K}_0$ of the natural homomorphism of $\mathfrak{S}(\mathfrak{N})$ into $\mathfrak{G}(\mathfrak{M})$; $\mathfrak{S} \subseteq \mathfrak{K}_0$ $(\subseteq \mathfrak{K})$.

For, a (f.g.) regular G-module N is always a rasidue-module of a (f.g.) free module modulo a (f.g.) free submodule (cf. Remark 3), and if N is of finite order, then the two free modules are isomorphic, as we see by considering Z-ranks.

Modulo this subgroup $\mathfrak{S}$ every element of $\mathfrak{G}(\mathfrak{N})$ is represented by (the isomorphism class of) a cohomologically trivial module of finite order itself; observe that every (G-)module of finite order is a residue-module of a regular module of finite order. (The above epimorphism of $\mathfrak{G}(\mathfrak{N})$ to $\mathfrak{C}(\mathfrak{P})$ plus this fact as well as the fact that $\mathfrak{S}$ is contained in the kernel $\mathfrak{K}$ of the epimorphism recovers Proposition 2 entirely).

We now show that our kernels $\mathfrak{K}$ and $\mathfrak{K}_0$, of the epimorphism $\mathfrak{G}(\mathfrak{N}) \to \mathfrak{C}(\mathfrak{M})$ (or, of $\mathfrak{G}(\mathfrak{N}) \to \mathfrak{C}(\mathfrak{P})$) and the homomorphism $\mathfrak{G}(\mathfrak{N}) \to \mathfrak{G}(\mathfrak{M})$ respectively, coincide in fact. For, since $\mathfrak{S}$ is contained in $\mathfrak{K}_0$ and since every element of $\mathfrak{G}(\mathfrak{N})$ is congruent modulo $\mathfrak{S}$ to an element represented by a module itself, it suffices, in order to show $\mathfrak{K} \subseteq$ (whence $=$) $\mathfrak{K}_0$, to prove that an element of $\mathfrak{G}(\mathfrak{N})$ represented by a module N belongs to $\mathfrak{K}_0$ whenever it belongs to $\mathfrak{K}$. However, N is then a residue-module of a f.g. free module modulo a f.g. free submodule, $0 \leftarrow N \leftarrow F_0 \leftarrow F_1 \leftarrow 0$ (exact), as was noted in Remark 4. Here $F_0 \approx F_1$ as a consideration on (Z- or $Z(G)$-) ranks shows. Thus $\mathfrak{K} = \mathfrak{K}_0$. (Instead of Remark 4, we might use merely the existence of a (f.g.) free resolution for N.)

Remark 5. Our subgroup $\mathfrak{S}$ of $\mathfrak{G}(\mathfrak{N})$, generated by elements represented by regular modules of finite order, is in fact actually smaller than $\mathfrak{K} = \mathfrak{K}_0$ (provided $G \neq 1$). To see this, let r be a prime and let $l_r(N)$ be, for a (cohomologically trivial) module N of finite order, log (r-component of the order of N). $l_r(N)$ is a function of the element in $\mathfrak{G}(\mathfrak{N})$ represented by N, and can be extended to an additive function on $\mathfrak{G}(\mathfrak{N})$ as we readily see. For every element of our subgroup the function takes a value divisible by the order of G, as we see also easily. On the other hand, we shall presently see that if r is congruent to 1 modulo the order of G then Z/rZ (operated by G trivially) represents an element of $\mathfrak{G}(\mathfrak{N})$ belonging to the kernel in question. Clearly $l_r(Z/rZ)$ is 1, and is not divisible by $(G:1)$. Now, for the above contention, observe the isomorphism $Z/rZ \approx Z(G)/\mathfrak{A}$ where $\mathfrak{A}$ is the ideal of $Z(G)$ consisting of elements $\sum_{\sigma\in G} a_\sigma\sigma$ $(a_\sigma \in Z)$ with $\sum_\sigma a_\sigma$ divisible by r. It suffices to show that $\mathfrak{A}$ is isomorphic to $Z(G)$ when $r \equiv 1 \bmod (G:1)$. Let $r = 1+(G:1)h$ and consider the element $u = 1+h\sum_\sigma \sigma$ in $Z(G)$. We want to show $\mathfrak{A} = Z(G)u$ $(= uZ(G))$. Clearly $u \in \mathfrak{A}$. On the other hand, $1-\sigma = (1-\sigma)u \in Z(G)u$ for every $\sigma \in G$. Hence, $\sum_\sigma x_\sigma\sigma \equiv \sum_\sigma x_\sigma \bmod Z(G)u$ for every element $\sum_\sigma x_\sigma$ $(x_\sigma \in Z)$ in $Z(G)$. In particular, $r = 1+h(G:1) \equiv u \bmod Z(G)u$ and $r \in Z(G)u$. For $\sum_\sigma a_\sigma\sigma \in \mathfrak{A}$ we have $\sum_\sigma a_\sigma\sigma \equiv \sum_\sigma a_\sigma \equiv 0 \bmod Z(G)u$. Thus $\mathfrak{A} = Z(G)u$ $(= uZ(G))$ and this relation shows that u is a non-zero-divisor. Hence $\mathfrak{A} \approx Z(G)$ as was asserted. (This is merely an *ad hoc* observation, and it is quite plausible that it is a special case of a more general relation. In fact, in case G is a cyclic group of prime order p, we shall see, in Section 6, that Z/rZ is isomorphic to the residue-module of $Z(G)$ modulo a submodule isomorphic to $Z(G)$ whenever r is an integer prime to p.)

5. Splitting structure of the Grothendieck group $\mathfrak{G}(\mathfrak{M})$ of f.g. cohomologically trivial modules. Leaving $\mathfrak{G}(\mathfrak{N})$ itself, we now consider its image in $\mathfrak{G}(\mathfrak{M})$ (which was our original stand in Proposition 2). That $\mathfrak{K}$ and $\mathfrak{K}_0$ coincide means that the image of $\mathfrak{G}(\mathfrak{N})$ in $\mathfrak{G}(\mathfrak{M})$ intersects with the subgroup of $\mathfrak{G}(\mathfrak{M})$ generated by elements represented by f.g. free modules by 0 only. Further, since every element of $\mathfrak{G}(\mathfrak{N})$ is represented by a module itself modulo $\mathfrak{S}$ ($\subseteq \mathfrak{K}_0$) our image of $\mathfrak{G}(\mathfrak{N})$ in $\mathfrak{G}(\mathfrak{M})$ consists of (not only is generated by) elements represented by modules of finite order. We have thus, naturally aided by Propositions 1, 2 too,

THEOREM 3. *Let G be a finite group. The following three groups are isomorphic in natural way:*

(i) *the subgroup of the Grothendieck group $\mathfrak{G}(\mathfrak{M})$ of f.g. cohomologically trivial G-modules generated by elements represented by (cohomologically trivial G-) modules of finite order; the subgroup in fact consists of such elements,*

(ii) *the class group $\mathfrak{C}(\mathfrak{M})$ of (f.g.) cohomologically trivial G-modules (modulo f.g. free modules, or, equivalently, modulo f.g. regular modules),*

(iii) *the projective class group $\mathfrak{C}(\mathfrak{P}) = \mathfrak{C}(G)$ over G.*

COROLLARY. The *Grothendieck group $\mathfrak{G}(\mathfrak{M})$ of f.g. cohomologically trivial modules* is the *direct product* of the subgroup consisting of elements represented by (cohomologically trivial) modules of finite order and the subgroup generated by elements represented by f.g. free modules (or, equivalently, by elements represented by f.g. regular modules). The same structure is transfered to the *Grothendieck group $\mathfrak{G}(\mathfrak{P})$ of f.g. projective modules*, by the isomorphism in Proposition 1; $\mathfrak{G}(\mathfrak{P})$ is the *direct product* of the subgroup consisting of elements of form $[P]-[F]$ with P and F projective and free, respectively, and of equal Z-ranks (or, equivalently, $Z(G)$-ranks) and the subgroup generated by elements represented by (f.g.) free modules. The last structure of $\mathfrak{G}(\mathfrak{P})$ can in fact directly be obtained from Nakayama, [7], Proposition 6. Then, from it we can obtain the former part, for $\mathfrak{G}(\mathfrak{M})$, of our corollary by means of Swan [12], Theorem 8.1. We followed the above somewhat longer way to our theorem in order to get some informations on $\mathfrak{G}(\mathfrak{N})$ by way.

Remark 6. With an arbitrarily given non-zero integer m, every f.g. projective G-module P has a free submodule F such that P/F has a finite order prime to m (see Theorem 7.1 in Swan [12]). It follows that in our theorem (as well as in its corollary) we may replace "of finite order" with "of finite order prime to m". Further, if we make use of the main Theorem 7.2 in [12] (cf. [1], [5]) we may restrict ourselves, in our theorem and corollary, to modules of finite order (prime to m) isomorphic to a residue-module of a (left-) ideal of $Z(G)$ (and, in the corollary, to elements of form $[P]-[Z(G)]$ with a (left-) ideal P of $Z(G)$ (such that $Z(G)/P$ has a finite order prime to m).

6. Cyclic groups of prime order. We now consider the special case where G is a cyclic group of a prime order p. In this case Rim [9] has determined the projective class group $\mathfrak{C}(\mathfrak{P}) = \mathfrak{C}(G)$ explicitly, on making use of Diederichsen's [4] (cf. also Reiner [8]) normal form of (integral) representations of G. Thus, Rim [9] shows that *the projective class group $\mathfrak{C}(\mathfrak{P})$, over G, is isomorphic to the ideal class group of (the integer ring of) the field $Q(s_p)$ of p-th roots of 1 over the rationals Q.* More precisely, with a f.g. projective module P over G and σ denoting a generator of G, the submodule ${}_NP$ of elements annulled by the operator $N = 1 + \ldots + \sigma^{p-1}$ may be regarded as a f.g. projective module over the integer ring J of $Q(s_p)$, a fixed (primitive) pth root s_p of 1 operating as σ, and thus determines, by Chevalley's [3] theory, an ideal class in J. Associating the projective class of P with this ideal class in J, we get the said isomorphism, as is shown in [9]. We denote this isomorphism, of $\mathfrak{C}(\mathfrak{P})$ and the ideal class group $\mathfrak{C}(J)$ of J, by α. Representatives for $\mathfrak{C}(\mathfrak{P})$ are constructed as follows: Let $\mathfrak{a}$ be a non-zero ideal in J. Since $\mathfrak{a}/(\sigma-1)\mathfrak{a} \approx Z/pZ$, there exists an element w in $\mathfrak{a}$ not belonging to $(\sigma-1)\mathfrak{a}$. A well defined G-module structure is given to the direct sum $\mathfrak{a}+Z$ of Z-modules by: $\sigma(a, 0) = (\sigma a, 0)$, $\sigma(0, 1) = (w, 1)$ $(a \in \mathfrak{a})$. We denote the G-module thus obtained by $\mathfrak{a}_w$. $\mathfrak{a}_w$ is projective, and the projective class of $\mathfrak{a}_w$ is independent of a choice of w. Indeed ${}_N(\mathfrak{a}_w)$ is isomorphic to the ideal $\mathfrak{a}$. If we let $\mathfrak{a}$ run over a system of representatives for the ideal class group in J, then $\mathfrak{a}_w$ runs over a representative system for the projective class group $\mathfrak{C}(\mathfrak{P})$ over G.

We now turn to the class group $\mathfrak{C}(\mathfrak{M})$ of cohomologically trivial modules over G. Naturally the above constructed representatives for $\mathfrak{C}(\mathfrak{P})$ form a representative system for $\mathfrak{C}(\mathfrak{M})$ too. We wish, however, to get representatives as modules of finite order. The answer is simple: if $\mathfrak{a}$ runs over a system of representatives prime to p for the ideal class group $\mathfrak{C}(J)$ of J, then $J/\mathfrak{a}$ (regarded as G-module with σ operating as the multiplication of s_p) runs over a representative system for $\mathfrak{C}(\mathfrak{M})$. (Thus, by turning to $\mathfrak{C}(\mathfrak{M})$, from $\mathfrak{C}(\mathfrak{P})$, we may construct class representatives inside of the cyclotomic integer ring J.) To be more precise, denote by α_1 the composite of the isomorphic map of $\mathfrak{C}(\mathfrak{M})$ to $\mathfrak{C}(\mathfrak{P})$, induced by ϱ $(= \iota^{-1}$, Proposition 1), with the isomorphic map α of $\mathfrak{C}(\mathfrak{P})$ to $\mathfrak{C}(J)$. Then we have

PROPOSITION 4. *If $\mathfrak{a}$ is a (non-zero) ideal prime to p in the integer ring J of the cyclotomic field $Q(s_p)$, the cohomologically trivial G-module $J/\mathfrak{a}$ (with σ operating as the multiplication of s_p) of finite order represents an element (class) of the class group $\mathfrak{C}(\mathfrak{M})$ which is mapped by α_1 to the in-*

verse of the ideal class of $\mathfrak{a}$. So, if $\mathfrak{a}$ runs over a system of representatives (prime to p) for the ideal class group $\mathfrak{C}(J)$ of J, then $J/\mathfrak{a}$ runs over a representative system for $\mathfrak{C}(\mathfrak{M})$.

To prove this, let $\mathfrak{p}$ be the ideal $(s_p-1)J$. Then $\mathfrak{a} \nsubseteq \mathfrak{p}$ and there exists an element w in $\mathfrak{a}$ not belonging to $\mathfrak{p}$. As $w \notin (\sigma-1)J$ $(=(s_p-1)J=\mathfrak{p})$ (even more) $w \notin (\sigma-1)\mathfrak{a}$, we may construct the G-modules $J_w = J+Z$ and $\mathfrak{a}_w = \mathfrak{a}+Z$ by the procedure described above. $\mathfrak{a}_w$ is, in natural way, a G-submodule of J_w, and we see readily $J_w/\mathfrak{a}_w \approx J/\mathfrak{a}$. Either from this or, more directly, from the fact that the order of $J/\mathfrak{a}$ is prime to the order p of G, the G-module $J/\mathfrak{a}$ is seen to be cohomologically trivial. Further, J_w is a free (G)-module (with a single generator) since ${}_N(J_w) \approx J$ the unit ideal of J. The projective class of $\mathfrak{a}_w$ is mapped by α to the ideal class of $\mathfrak{a}$. It is now clear that $J/\mathfrak{a}$ represents an element of $\mathfrak{C}(\mathfrak{M})$ mapped by α_1 to the inverse of the ideal class of $\mathfrak{a}$.

Remark 7. If $\mathfrak{b}$ is a (non-zero) ideal not prime to p, then the G-module $J/\mathfrak{b}$ is never cohomologically trivial. For, every element of the submodule $\mathfrak{p}^{-1}\mathfrak{b}/\mathfrak{b}$ is invariant by G, while $NJ=0$ and, even more, $N(J/\mathfrak{b})=0$, N denoting the operator $1+\sigma+\ldots+\sigma^{p-1}$ as before.

Let us next rather start with an arbitrary cohomologically trivial G-module M of finite order. We want to determine the ideal class of J corresponding to the element of $\mathfrak{G}(\mathfrak{M})$ represented by M. M is a direct sum of G-submodules each of which has a prime power order. Together with M, these primary components of M are cohomologically trivial. So, it is sufficient to consider a case where M has a power of a prime number l as its order. First, we assume that l is prime to p. Let $l=\mathfrak{l}_1\mathfrak{l}_2\ldots\mathfrak{l}_g$ be the decomposition of l into prime ideals in J; it is, naturally, well known that if f is the smallest positive exponent with $l^f \equiv 1 \bmod p$ then $fg=p-1$, but we do not need to use this. The group ring $(Z/lZ)(G)$ over Z/lZ is decomposed into mutually orthogonal $g+1$ simple ideals. More precisely, it is the direct sum of an ideal, $\mathfrak{z}_0$, isomorphic to Z/lZ and an ideal isomorphic to $(Z/lZ)(G)/N\big((Z/lZ)(G)\big)$, and this last residue-module is, as it is isomorphic with J/lJ, a direct sum $\mathfrak{z}_1+\ldots+\mathfrak{z}_g$ of g ideals $\mathfrak{z}_i$ such that $\mathfrak{z}_i \approx J/\mathfrak{l}_i$. Similarly, for any natural number t the group ring $(Z/l^tZ)(G)$ is a direct sum $\mathfrak{y}_0+\mathfrak{y}_1+\ldots+\mathfrak{y}_g$ of ideals $\mathfrak{y}_i$ such that $\mathfrak{y}_0 \approx Z/l^tZ$ (operated by G trivially) and $\mathfrak{y}_i \approx J/\mathfrak{l}_i^t$ for $i=1,\ldots,g$. As $\mathfrak{l}_1\ldots\mathfrak{l}_g=lJ$ is principal in J, $\mathfrak{z}_1+\ldots+\mathfrak{z}_g$ represents an element of $\mathfrak{G}(\mathfrak{M})$ belonging to the unit class of $\mathfrak{C}(\mathfrak{M})$. Then $\mathfrak{z}_0$ $(\approx Z/lZ)$ represents an element of $\mathfrak{G}(\mathfrak{M})$ belonging to the unit class of $\mathfrak{C}(\mathfrak{M})$, since the same is the case with $\mathfrak{z}_0+(\mathfrak{z}_1+\ldots+\mathfrak{z}_g)=Z(G)/lZ(G)$. The same is the case with Z/l^tZ too. Every $(Z/l^tZ)(G)$-module is, as the theory of uni-serial rings (Köthe [6]) shows, a direct sum of submodules each of which is isomorphic to a residue-module of one of $\mathfrak{y}_0, \mathfrak{y}_1, \ldots, \mathfrak{y}_g$, thus to a module of form Z/l^sZ or $J/\mathfrak{l}_i^s$ $(1<i<g)$. Now, our M is a $(Z/l^tZ)(G)$-module for a sufficiently large t, and our consideration can be applied to it. In view of Proposition 4 and the above observation on Z/l^tZ we have now easily

PROPOSITION 5. *Let M be a (cohomologically trivial) G-module having a finite order prime to p. M is a direct sum of G-submodules M_μ such that, for each μ, M_μ is isomorphic either to a module of form Z/mZ (operated by G trivially) or to a module of form $J/\mathfrak{a}_\mu$ with a non-zero ideal $\mathfrak{a}_\mu$ in J. M represents an element (class) of the class group $\mathfrak{C}(\mathfrak{M})$ mapped by α_1 to the inverse of the ideal class (in J) of the product of those ideals $\mathfrak{a}_\mu$.*

Next, just a word for a cohomologically trivial module of order a power of p. Naturally, G-modules of form $(Z/p^tZ)(G)$ are cohomologically trivial, and, indeed, regular. In fact, every regular G-module of order a power of p is a direct sum of modules of this form. But, there are *cohomologically trivial G-modules of order a power of p* which are *not regular*, as somewhat complicated constructions show. It does not seem to be simple to analize them generally. So we close this short paper by stating a conjecture that every cohomologically trivial G-module of order a power of p represents the unit element of the class group $\mathfrak{C}(\mathfrak{M})$.

Addendum: Just after I had finished proof-reading of the present note (May 17, 1964), I was given, by the kindness of Dieudonné, a chance to see the galley-proofs of a paper "The Whitehead group of a polynomial extension" by Bass, Heller and Swan, to appear in Publ. Math. IHÉS., 1964. Proposition 1 in § 1 of the present note is given, in a more general setting of abelian categories (satisfying certain conditions), in § 4 of this joint paper. As is stated there, the result was essentially given by Grothendieck, in the case of categories of coherent sheaves over a connected algebraic variety; Théorème 2, Borel-Serre, *Le théorème de Riemann-Roch,* Bull. Soc. Math. France 86(1959), pp. 97-136.

References

[1] H. Bass, *Projective modules over algebras,* Ann. Math. 73 (1961), pp. 532-542.

[2] H. Cartan and S. Eilenberg, *Homological Algebra,* Princeton 1956.

[3] C. Chevalley, *L'Arithmetique dans des Algèbres de Matrices,* Act. Sci. et Ind. 232, Paris 1936.

[4] F. E. Diederichsen, *Über die Ausreduktion ganzzahliger Gruppendarstellungen bei arithmetischer Äquivalenz,* Abh. Math. Sem. Hamburg 13 (1938), pp. 357-412.

[5] A. Hattori, *Integral representations and projective modules* (in Japanese), Rep. Symposium on Algebra 1 (1961).

[6] G. Köthe, *Verallgemeinerte Abelsche Gruppe mit hyperkomplexem Operatorring,* Math. Zeits. 39 (1934), pp. 31-44.

[7] T. Nakayama, *On modules of trivial cohomology over a finite group, II*, Nagoya Math. J. 12 (1957), pp. 171-176.

[8] I. Reiner, *Integral representation of cyclic groups of prime order*, Proc. Amer. Math. Soc. 8 (1957), pp. 142-146.

[9] D. S. Rim, *Modules over finite groups*, Ann. of Math. 69 (1959), pp. 700-712.

[10] — *On projective class groups*, Trans. Amer. Math. Soc. 98 (1961), pp. 459-467.

[11] J. P. Serre, *Corps locaux*, Act. Sci. et Ind. 1296, Paris 1962.

[12] R. G. Swan, *Induced representations and projective modules*, Ann. of Math. 71 (1960), pp. 552-578.

[13] — *Periodic resolutions for finite groups*, Ann. of Math. 72 (1960), pp. 267-291.

[14] — *Projective modules over group rings and maximal orders*, Ann. Math. 76 (1962), pp. 55-61.

NAGOYA UNIVERSITY

Reçu par la Rédaction le 13. 12. 1963

ACTA ARITHMETICA
IX (1964)

Remark concerning integer sequences

by

K. F. Roth (London)

It seems highly plausible that there are various limitations to the extent to which a sequence of natural numbers can be well-distributed simultaneously among and within all congruence classes; unless the sequence is in some sense "nearly" the sequence of all natural numbers or the empty sequence. Many conjectures of this type appear to be very intractable, particularly those closely related to the well-known conjecture that every sequence of positive upper asymptotic density contains arbitrarily long arithmetic progressions. The object of this note is to remark that, on the other hand, a very simple argument yields at least some information concerning irregularities of distribution of an arbitrary sequence with respect to congruence classes. The theorem below is representative of the type of result that can be proved in this way.

THEOREM. *Let N be a natural number and let $\mathcal{N}$ be a set of distinct natural numbers not exceeding N. For any natural number $m \leqslant N$ and any congruence class h modulo q, we denote by $\Phi_{q,h}(\mathcal{N};\, m)$ the number of elements of $\mathcal{N}$ which do not exceed m and lie in the congruence class; and we denote by $\Phi^*_{q,h}(\mathcal{N};\, m)$ the corresponding "expectation", namely*

$$\Phi^*_{q,h}(\mathcal{N};\, m) = \eta\Phi_{q,h}(\mathcal{I};\, m)$$

where $\mathcal{I}$ is the set $\{1, 2, \ldots, N\}$ and

$$\eta = N^{-1}\sum_{\substack{n=1\\ n\in\mathcal{N}}}^{N} 1. \tag{1}$$

For each m, and every natural number q, we define

$$V_q(m) = \sum_{h=1}^{q} \{\Phi_{q,h}(\mathcal{N};\, m) - \Phi^*_{q,h}(\mathcal{N};\, m)\}^2. \tag{2}$$

Then, for all natural numbers Q,

$$\sum_{q=1}^{Q} q^{-1} \sum_{m=1}^{N} V_q(m) + Q\sum_{q=1}^{Q} V_q(N) \gg \eta(1-\eta)Q^2N, \tag{3}$$

where the implicit constant is absolute.