INTEGRAL REPRESENTATIONS OF CYCLIC GROUPS OF PRIME ORDER

IRVING REINER

1. Elementary facts. In this paper we shall extend a result due to Diederichsen [2] on integral representations of cyclic groups of prime order, and shall simplify the proof thereof. Let \( \mathbb{Z} \) denote the ring of rational integers, \( \mathbb{Q} \) the rational field. If \( R \) is a ring, by a regular \( R \)-module we shall mean a finitely-generated torsion-free \( \mathbb{Z} \)-module.

**Lemma 1** (Zassenhaus [9]). Let \( R \) be a regular \( \mathbb{Z} \)-module contained in a field \( K \), and suppose \( R \) contains a \( \mathbb{Q} \)-basis of \( K \). Then every irreducible regular \( R \)-module is \( R \)-isomorphic to an ideal in \( R \). Two ideals in \( R \) are \( R \)-isomorphic (as \( R \)-modules) if and only if they lie in the same ideal class.

**Remark.** In terms of matrix representations, this lemma implies that there is a one-to-one correspondence between classes (under unimodular equivalence) of irreducible \( \mathbb{Z} \)-representations of \( R \) and ideal classes of \( R \). A full set of inequivalent irreducible matrix representations is obtained by restricting the regular representation of \( R \) to a full set of inequivalent ideals in \( R \). In particular, let \( f(x) \in \mathbb{Z}[x] \) be irreducible, and set \( R = \mathbb{Z}[\theta] \) where \( \theta \) is a zero of \( f(x) \). Since every irreducible representation of \( R \) is described by \( \theta \rightarrow X \), where \( X \) is an integral nonderogatory solution of \( f(X) = 0 \), the number of unimodular classes of such matrix solutions coincides with the class number of \( \mathbb{Z}[\theta] \). (See [5; 8].)

Now let \( \mathfrak{o} \) be a Dedekind ring (see [4]) which is assumed to be a regular \( \mathbb{Z} \)-module. By Lemma 1, every irreducible regular \( \mathfrak{o} \)-module is \( \mathfrak{o} \)-isomorphic to an ideal in \( \mathfrak{o} \).

**Lemma 2** (Steinitz [7], Chevalley [1]. This result can also be deduced from [6]). Every regular \( \mathfrak{o} \)-module is \( \mathfrak{o} \)-isomorphic to a direct sum \( \mathfrak{A}_1 \oplus \cdots \oplus \mathfrak{A}_n \) of ideals in \( \mathfrak{o} \). The \( \mathfrak{o} \)-rank \( n \) and the ideal class of \( \mathfrak{A}_1 \cdots \mathfrak{A}_n \) are the only invariants, and determine the module up to \( \mathfrak{o} \)-isomorphism.

**Remark.** Let \( f(x) \in \mathbb{Z}[x] \) be a monic irreducible polynomial, and let \( f(\theta) = 0 \). Assume that \( \mathbb{Z}[\theta] \) coincides with the ring of all algebraic
integers in $Q(\theta)$. Then $Z[\theta]$ is a Dedekind ring, and the lemma implies that every integral matrix $X$ for which $f(X) = 0$, is integrally decomposable into a direct sum of irreducible matrices satisfying $f(X) = 0$.

**Lemma 3.** Let $\mathfrak{e}$ and $\mathfrak{B}$ be ideals in $\mathfrak{o}$. Then there exists an $\mathfrak{o}$-automorphism of $\mathfrak{o} \oplus \mathfrak{B}$ which maps $\mathfrak{e} \oplus \mathfrak{B}$ isomorphically onto $\mathfrak{o} \oplus \mathfrak{e} \mathfrak{B}$.

**Proof.** Since only ideal classes are involved, we may assume $\mathfrak{e} + \mathfrak{B} = \mathfrak{o}$. Choose $\mathfrak{e}_0 \subseteq \mathfrak{e}$, $\mathfrak{b}_0 \subseteq \mathfrak{B}$ such that $\mathfrak{e}_0 - \mathfrak{b}_0 = 1$. Then define an $\mathfrak{o}$-linear map $\phi: \mathfrak{o} \oplus \mathfrak{B} \to \mathfrak{o} \oplus \mathfrak{B}$ by means of

$$\phi(a, b) = (a + b, ab_0 + \mathfrak{e}_0 b), \quad a \in \mathfrak{o}, \ b \in \mathfrak{B}.$$ 

It is easily verified that $\phi$ is the desired $\mathfrak{o}$-automorphism of $\mathfrak{o} \oplus \mathfrak{B}$.

2. **Cyclic groups.** Let $G = \{g\}$ be a cyclic group of prime order $p$, and let $Z[g]$ be its group ring over the integers. We shall use the results of the previous section to classify all $Z$-regular $Z[g]$-modules. Define $s = 1 + g + \cdots + g^{p-1} \in Z[g]$. Let $M$ be a $Z$-regular $Z[g]$-module, and define

$$(1) \quad M_s = \{m \in M: sm = 0\}.$$ 

We may then view $M_s$ as a $Z[g]/(s)$-module, where $(s)$ is the principal ideal generated by $s$. However, $Z[g]/(s) \cong Z[\theta]$, where $\theta$ is a primitive $p$th root of 1. Further, $Z[\theta]$ is a Dedekind ring, hereafter denoted by $\mathfrak{o}$.

Now we observe that

$$(2) \quad M_s \supseteq (g - 1)M \supseteq (\theta - 1)M_s,$$

all considered as $\mathfrak{o}$-modules. By Lemma 2, we may write

$$(3) \quad M_s = \mathfrak{o} \oplus \cdots \oplus \mathfrak{o} \oplus \mathfrak{A},$$

where $n$ (the number of summands) and the ideal class of the ideal $\mathfrak{A}$ in $\mathfrak{o}$ are uniquely determined. Using (2), we find that as $\mathfrak{o}$-module,

$$(4) \quad (g - 1)M = \mathfrak{e}_1 \oplus \cdots \oplus \mathfrak{e}_{n-1} \oplus \mathfrak{e}_n \mathfrak{A},$$

with the $\mathfrak{e}_i$ ideals in $\mathfrak{o}$. From the second inclusion in (2), we see that each $\mathfrak{e}_i$ is either $\mathfrak{o}$ or the principal prime ideal $(\theta - 1)$. By permuting the summands, and using Lemma 3 if necessary, we may then assume that

$$(5) \quad \mathfrak{e}_1 = \cdots = \mathfrak{e}_r = 0, \quad \mathfrak{e}_{r+1} = \cdots = \mathfrak{e}_n = (\theta - 1).$$

In that case, the quotient module

$$B = (g - 1)M/(\theta - 1)M_s \cong o/(\theta - 1) \oplus \cdots \oplus o/(\theta - 1),$$
where \( r \) summands occur. Since \((\theta - 1)\) is an ideal of norm \( p \), we see that \( B \) is an additive abelian group of type \((p, \ldots, p)\), and the integer \( r \) is thus uniquely determined as the rank of \( B \). Let us fix \( \beta_k \) in the \( k \)th summand of \((3)\) so that \( B \) is generated by the cosets \( \beta_1 + (\theta - 1), \ldots, \beta_r + (\theta - 1) \) (or \( \beta_n + (\theta - 1) \mathfrak{N} \) in case \( r = n \)). For example, we may choose \( \beta_k \) to be the unit element in \( \mathfrak{o} \) for \( k < n \), while if \( r = n \), we choose \( \beta_n \in \mathfrak{N} \) such that \( \beta_n \in (\theta - 1) \mathfrak{N} \).

On the other hand, \( M/M_s \) is a regular \( Z \)-module, and therefore \( M_s \) is a \( Z \)-direct summand of \( M \). Choose a regular \( Z \)-module \( X \) such that \( M \) is the direct sum of \( M_s \) and \( X \). Then

\[
(g - 1)M = (\theta - 1)M_s + (g - 1)X,
\]

so that the map \( \phi : X \rightarrow B \) defined by

\[
\phi(x) = (g - 1)x + (\theta - 1)M_s
\]

for \( x \in X \) is a linear map of \( X \) onto \( B \). With each \( x \in X \) we may thus associate an \( r \)-tuple \((\alpha_1, \ldots, \alpha_r)\) (also denoted by \( \phi(x) \)) such that

\[
(g - 1)x \equiv \alpha_1 \beta_1 + \cdots + \alpha_r \beta_r \pmod{(\theta - 1)M_s},
\]

with each \( \alpha_i \in \bar{Z} = Z/pZ \). By choosing a suitable \( Z \)-basis \( x_1, \ldots, x_m \) of \( X \), we may assume that the vectors \( \phi(x_1), \ldots, \phi(x_r) \) are linearly independent over \( \bar{Z} \). Under a further change of \( Z \)-basis of \( X \), we may then take

\[
(g - 1)x_i \equiv c_i \beta_i, \quad (g - 1)x_j \equiv 0 \pmod{(\theta - 1)M_s},
\]

\[
(1 \leq i \leq r, r < j \leq m),
\]

where each \( c_i \in Z \), \( c_i \not\equiv 0 \pmod{p} \). Set \((g - 1)x_i = c_i \beta_i + (g - 1)u_i \), \((g - 1)x_j = (g - 1)u_j \) \((1 \leq i \leq r, r < j \leq m)\), with each \( u_i \in M_s \), and define \( y_i = x_i - u_i \) \((1 \leq i \leq m)\). Then we have

\[
(6) \quad M = M_s \oplus Z y_1 \oplus \cdots \oplus Z y_m,
\]

where

\[
(7) \quad gy_i = y_i + c_i \beta_i, \quad gy_j = y_j \quad (1 \leq i \leq r, r < j \leq m)
\]

and where \( M_s \) defined by \((3)\) is made into a \( Z[g] \)-module by

\[
(8) \quad gm = \theta m \quad \text{for} \ m \in M_s.
\]

The structure of \( M \) is completely determined by the ideal class of \( \mathfrak{N} \), the integers \( r = Z \)-rank of \( B \), \( m = Z \)-rank of \( M/M_s \), \( n = \mathfrak{a} \)-rank of \( M_s \), and by the constants \( c_1, \ldots, c_r \). We show now that we may in fact take each \( c_i = 1 \); this is a consequence of the following:
Lemma 4. Let $\mathfrak{a}$ be an ideal in $\mathfrak{o}$, let $\beta \in \mathfrak{a}$ be fixed, and let $c \in \mathbb{Z}$, $c \not\equiv 0 \pmod{p}$. Let $M_1 = \mathfrak{a} \oplus \mathbb{Z}y_1$ be made into a $\mathbb{Z}[g]$-module by defining $ga = \theta a$ for $a \in \mathfrak{a}$, $gy_1 = y_1 + \beta$. Let $M = \mathfrak{a} \oplus \mathbb{Z}y_2$ be made into a $\mathbb{Z}[g]$-module by defining $ga = \theta a$ for $a \in \mathfrak{a}$, $gy_2 = y_2 + c\beta$. Then $M_1$ and $M$ are $\mathbb{Z}[g]$-isomorphic.

Proof. Set $u = 1 + \theta + \cdots + \theta^{c-1} = \text{unit in } \mathfrak{o}$. Since $u - c = (\theta - 1) + (\theta^2 - 1) + \cdots + (\theta^{c-1} - 1)$, we may choose $t \in \mathfrak{a}$ so that $(\theta - 1)t = (u - c)\beta$. Now define a linear map $\phi: M_1 \to M$ by

$$\phi(a) = ua, \quad a \in \mathfrak{a}, \quad \phi(y_1) = y_1 + t.$$  

Then $g\phi(a) = \phi ga$ for all $a \in \mathfrak{a}$, and also

$$g\phi(y_1) = g(y_2 + t) = y_2 + c\beta + \theta t = y_2 + t + u\beta = \phi(y_1).$$  

Thus $\phi$ is a $\mathbb{Z}[g]$-isomorphism of $M_1$ onto $M$.

To summarize, we have thus shown:

Theorem. Every $\mathbb{Z}$-regular $\mathbb{Z}[g]$-module is operator-isomorphic to a module defined by (3), (6), (7), and (8), with $c_1 = \cdots = c_r = 1$. The invariants which uniquely determine such a module (up to isomorphism) are: the ideal class of $\mathfrak{a}$, $n = \mathfrak{o}$-rank of $M_1$, $m = \mathbb{Z}$-rank of $M/M_1$, and $r = \mathbb{Z}$-rank of $(g - 1)M/(\theta - 1)M_1$; the only restrictions on these invariants are the conditions $r \leq m$, $r \leq n$. Conversely, for any such choice of invariants, equations (3), (6), (7), and (8) define a $\mathbb{Z}[g]$-module with the given invariants.

Corollary (See [2; 3].) The integrally-indecomposable regular $\mathbb{Z}[g]$-modules are those for which either $r = n = 0$, $m = 1$, or $r = m = 0$, $n = 1$, or $r = m = n = 1$. The number of nonisomorphic modules of these types is $2h + 1$, where $h$ is the class number of $\mathfrak{o}$.

References

1. Introduction. Almost left alternative algebras were defined by Albert in [1]. They are algebras $A$ over a field $F$ of characteristic not two which satisfy these postulates:

I. The elements of $A$ satisfy an identity of the form

$$z(xy) = a(zx)y + p(zy)x + r(xy)y + q(yz)x + e(yz)x + r(xz)y + s(xz)y$$

for elements $a, p, r, q, e, r, <r, r$ in $F$ which are independent of $x, y, z$ in $A$.

II. The relation $xx^2 = x^2x$ holds for every $x$ of $A$.

III. There exists an algebra $B$ with a unity quantity $e$ such that $B$ satisfies (1) and is not a commutative algebra.

An algebra is called almost right alternative if I, II, and III hold with (1) replaced by an identity of the same form but with $z(xy)$ replaced by $(xy)z$. These two identities are the general shrinkability conditions of level one, as defined by Albert in [2]. An almost alternative algebra is one which is both almost left alternative and almost right alternative.

Reference is made in [1] to several results which are proved here. In addition to the above postulates, we assume the flexible law, that is, $(xy)x = x(yx)$ for every $x$ and $y$ in $A$. This makes Postulate II redundant. Albert confined his investigation in [1] to nonflexible algebras.

Received by the editors February 20, 1956.

1 This paper is a portion of a Ph.D. thesis supervised by A. A. Albert and submitted to the University of Chicago in 1951. The author is now at Robert College, Istanbul.