INTEGRAL REPRESENTATIONS OF CYCLIC GROUPS OF PRIME ORDER

IRVING REINER[1]

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 Z denote the ring of rational integers, Q the rational field. If R is a ring, by a *regular* R-module we shall mean a finitely-generated torsion-free R-module.

LEMMA 1 (Zassenhaus [9]). *Let R be a regular Z-module contained in a field K, and suppose R contains a 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 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 $f(x) \in Z[x]$ be irreducible, and set $R = Z[\theta]$ where θ is a zero of $f(x)$. Since every irreducible representation of R is described by $\theta \to X$, 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 $Z[\theta]$. (See [5; 8].)

Now let $\mathfrak{o}$ be a Dedekind ring (see [4]) which is assumed to be a regular 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 $f(x) \in Z[x]$ be a monic irreducible polynomial, and let $f(\theta) = 0$. Assume that $Z[\theta]$ coincides with the ring of all algebraic

Presented to the Society, September 2, 1955; received by the editors February 28, 1956.

[1] Part of this work was supported by a research contract with the National Science Foundation. The author wishes to thank the referee for his helpful suggestions.

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 $e_0\in\mathfrak{e}$, $b_0\in\mathfrak{B}$ such that $e_0-b_0=1$. Then define an $\mathfrak{o}$-linear map ϕ: $\mathfrak{o}\oplus\mathfrak{B}\to\mathfrak{o}\oplus\mathfrak{B}$ by means of

$$\phi(a, b) = (a + b, ab_0 + e_0b), \qquad a \in \mathfrak{o}, b \in \mathfrak{B}.$$

It is easily verified that ϕ is the desired 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

$$M_s = \{m \in M: sm = 0\}. \tag{1}$$

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 θ is a primitive pth root of 1. Further, $Z[\theta]$ is a Dedekind ring, hereafter denoted by $\mathfrak{o}$.

Now we observe that

$$M_s \supset (g - 1)M \supset (\theta - 1)M_s, \tag{2}$$

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

$$M_s = \mathfrak{o} \oplus \cdots \oplus \mathfrak{o} \oplus \mathfrak{A}, \tag{3}$$

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,

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

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

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

In that case, the quotient module

$$B = (g - 1)M/(\theta - 1)M_s \cong \mathfrak{o}/(\theta - 1) \oplus \cdots \oplus \mathfrak{o}/(\theta - 1),$$

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

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 $\phi: X \to B$ defined by

$$\phi(x) = (g-1)x + (\theta-1)M_s \qquad \text{for } x \in X$$

is a linear map of X onto B. With each $x \in X$ we may thus associate an r-tuple $(\alpha_1, \cdots, \alpha_r)$ (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 $\alpha_i \in \overline{Z} = Z/pZ$. By choosing a suitable Z-basis $x_1, \cdots, x_m$ of X, we may assume that the vectors $\phi(x_1), \cdots, \phi(x_r)$ are linearly independent over $\overline{Z}$. Under a further change of Z-basis of X, we may then take

$$(g-1)x_i \equiv c_i\beta_i,\ (g-1)x_j \equiv 0 \pmod{(\theta-1)M_s},$$
$$(1 \leqq i \leqq r,\ r < j \leqq m),$$

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

$$M = M_s \oplus Zy_1 \oplus \cdots \oplus Zy_m, \tag{6}$$

where

$$gy_i = y_i + c_i\beta_i, \qquad gy_j = y_j \qquad (1 \leqq i \leqq r,\ r < j \leqq m) \tag{7}$$

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

$$gm = \theta m \qquad \text{for } m \in M_s. \tag{8}$$

The structure of M is completely determined by the ideal class of $\mathfrak{A}$, the integers $r = Z$-rank of B, $m = Z$-rank of M/M_s, $n = \mathfrak{o}$-rank of M_s, and by the constants $c_1, \cdots, c_r$. 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 $c\in Z$, $c\not\equiv 0 \pmod{p}$. Let $M_1=\mathfrak{A}\oplus Zy_1$ be made into a $Z[g]$-module by defining $ga=\theta a$ for $a\in\mathfrak{A}$, $gy_1=y_1+\beta$. Let $M=\mathfrak{A}\oplus Zy_2$ be made into a $Z[g]$-module by defining $ga=\theta a$ for $a\in\mathfrak{A}$, $gy_2=y_2+c\beta$. Then M_1 and M are $Z[g]$-isomorphic.*

PROOF. Set $u=1+\theta+\cdots+\theta^{c-1}=$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 ϕ: $M_1\to M$ by

$$\phi(a) = ua, \quad a\in\mathfrak{A}, \quad \phi(y_1) = y_2 + t.$$

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

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

Thus ϕ is a $Z[g]$-isomorphism of M_1 onto M.

To summarize, we have thus shown:

THEOREM. *Every Z-regular $Z[g]$-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_s, $m=Z$-rank of M/M_s, and $r=Z$-rank of $(g-1)M/(\theta-1)M_s$; the only restrictions on these invariants are the conditions $r\leqq m$, $r\leqq n$. Conversely, for any such choice of invariants, equations* (3), (6), (7), *and* (8) *define a $Z[g]$-module with the given invariants.*

COROLLARY (See [2; 3].) *The integrally-indecomposable regular $Z[g]$-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. C. Chevalley, *L'arithmétique dans les algèbres de matrices*, Actualités Scientifiques et Industrielles vol. 323 (1936) Paris.

2. F. E. Diederichsen, *Über die Ausreduktion ganzzahliger Gruppendarstellungen bei arithmetischer Äquivalenz*, Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg vol. 14 (1938) pp. 357–412.

3. L. K. Hua and I. Reiner, *Automorphisms of the unimodular group*, Trans. Amer. Math. Soc. vol. 71 (1951) pp. 331–348.

4. I. Kaplansky, *Modules over Dedekind rings and valuation rings*, Trans. Amer. Math. Soc. vol. 72 (1952) pp. 327–340.

5. C. G. Latimer and C. C. MacDuffee, *A correspondence between classes of ideals and classes of matrices*, Ann. of Math. vol. 34 (1933) pp. 313–316.

6. I. Reiner, *Maschke modules over Dedekind rings*, in Canadian Journal of Mathematics vol. 8 (1956) pp. 329–334.

7. E. Steinitz, *Rechteckige Systeme und Moduln in algebraischen Zahlkörpern*, Math. Ann. vol. 71 (1911) pp. 328–354, vol. 72 (1912) pp. 297–345.

8. O. Taussky, *On a theorem of Latimer and MacDuffee*, Canadian Journal of Mathematics vol. 1 (1949) pp. 300–302.

9. H. Zassenhaus, *Neuer Beweis der Endlichkeit der Klassenzahl bei unimodularer Äquivalenz endlicher ganzzahliger Substitutionsgruppen*, Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg vol. 12 (1938) pp. 276–288.

UNIVERSITY OF ILLINOIS

FLEXIBLE ALMOST ALTERNATIVE ALGEBRAS[1]

D. M. MERRIELL

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

$$(1)\qquad \begin{aligned} z(xy) = {} & \alpha(zx)y + \beta(zy)x + \gamma(xz)y + \delta(yz)x + \epsilon y(zx) \\ & + \eta x(zy) + \sigma y(xz) + \tau x(yz) \end{aligned}$$

for elements $\alpha, \beta, \gamma, \delta, \epsilon, \eta, \sigma, \tau$ 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.