ABELIAN GROUPS OF UNIMODULAR MATRICES[1]

BY

EVERETT C. DADE

This paper offers a generalization of the theorems of K. Goldberg [1], O. Taussky and J. Todd [2], and H. S. M. Coxeter [3] on the possible structures of abelian subgroups of the group $\Gamma_n(K)$ of $n \times n$ restricted unimodular matrices over an algebraic number field K. The basic result (see Theorem 3 below) is

The rank $r(G)$ of an abelian subgroup G of $\Gamma_n(K)$ is $\leqq [n^2/4]\,[K:Q]$. The minimum number $S(G)$ of generators of the periodic subgroup of G is $\leqq n - 1$.

We also obtain a bound on the order of any finite abelian subgroup, and a bound for $r(G)$ depending on $S(G)$ which shows that, when $S(G)$ is large, $r(G)$ must be small, and vice versa.

The idea of the proof is to consider an abelian subgroup of the group $\Delta_n(K)$ of extended unimodular matrices as a subgroup of the group of units in an order of an abelian subalgebra of the $n \times n$ matrix algebra. After some preliminary definitions and notations in Section 1, we investigate the structure of such unit groups in an abstract algebra in Section 2. Then we consider an algebra with a faithful module in Section 3 and find bounds for the structural constants of the unit group in terms of the dimension of the module and the structure of the field K. Finally, in Section 4, we consider subgroups of $\Delta_n(K)$ and $\Gamma_n(K)$, passing from the former to the latter by means of their centers. We also give several examples in this section to show that various bounds are best possible.

1. For the purposes of this paper, we shall adopt the following notations:

Q is the field of rational numbers.

Z is the ring of rational integers.

$K, K_1, K_2, \cdots$ are algebraic number fields.

$O(K)$ is the ring of integers of K.

$U(K)$ is the group of units of K (i.e., of $O(K)$).

$[V:K]$ is the dimension of the vector space V over the field K.

$A, A_1, A_2, \cdots$ are *commutative*, finite-dimensional algebras with identities over Q.

$[x]$ is the largest element of Z which is not larger than the real number x.

Let V be a finite-dimensional vector space over Q. By a lattice L in V we shall mean an additive, finitely-generated subgroup of V, spanning V over Q. We shall use the fact that any lattice L in V has a Z-basis of $n = [V:Q]$

Received September 16, 1957.

[1] This paper was submitted to the Mathematics Department of Harvard University in partial fulfillment of the requirements for an A.B. degree.