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.

elements $e_1, \cdots, e_n \in L$, such that any element of L may be expressed in one and only one way as the sum $x_1 e_1 + \cdots + x_n e_n$ with $x_i \in Z$. We shall also use the fact that, for any $v \in V$, there is an $x \in Z$ such that $xv \in L$, or, otherwise stated, if W is a subspace of V, then $L \cap W$ is a lattice in W.

If G is any abelian group, we define $\mathrm{Tor}(G)$ to be the subgroup of all elements of finite order in G,[2] and the rank of G, $r(G)$, to be the number, from 0 to ∞ inclusive, of Z-independent elements of G. We define $S(G)$ to be the smallest number of elements of $\mathrm{Tor}(G)$ which can generate $\mathrm{Tor}(G)$. If $\mathrm{Tor}(G)$ is trivial, then $S(G) = 1$.

If we make the usual conventions about operations with ∞, and if G and H are abelian groups, then we have

$$G \subseteqq H \quad \text{implies} \quad r(H) = r(H/G) + r(G). \tag{1}$$

It follows that $r(G) \leqq r(H)$ and $r(H/G) \leqq r(H)$. If H is a direct product $H = G \otimes F$, then (1) implies that

$$r(G \otimes F) = r(G) + r(F). \tag{2a}$$

In this case, we also have

$$\mathrm{Tor}(G \otimes F) = \mathrm{Tor}(G) \otimes \mathrm{Tor}(F), \tag{2b}$$

and, if $\mathrm{Tor}(G)$ and $\mathrm{Tor}(F)$ are finite,

$$\mathrm{Max}(S(G), S(F)) \leqq S(G \otimes F) \leqq S(G) + S(F). \tag{2c}$$

If G is finitely generated, it has a free abelian subgroup G' on $r(G) < \infty$ generators, such that $G = G' \otimes \mathrm{Tor}(G)$. In this case, $\mathrm{Tor}(G)$ is finite.

A lattice L in a vector space V, considered as an abelian group, has

$$r(L) = [V:Q], \quad \text{and} \quad \mathrm{Tor}(L) = (0). \tag{3}$$

By an order O in an algebra A, we shall mean a subring of A, containing the identity, whose additive group is a lattice in A. Trivially, every A possesses at least one order.

We shall use the notations:
$O, O_1, \cdots, O', \cdots$ for orders in various algebras,
$U(O)$ for the group of ring units in O,
$\mathrm{Tor}(O)$ for $\mathrm{Tor}(U(O))$,
$r(O)$ for $r(U(O))$,
$S(O)$ for $S(U(O))$.

If K is considered as an algebra over Q, then $O(K)$ is an order in K. $U(O(K)) = U(K)$ is the usual group of units of K. From algebraic number theory we know that

$$\begin{aligned} &\mathrm{Tor}(O(K)) = W(K), \text{ the cyclic group of roots of unity in } K, \\ &r(O(K)) = r(K) = r_1 + r_2 - 1, \end{aligned} \tag{4}$$

[2] This is also known as the periodic subgroup of G.

where r_1 is the number of real, r_2 the number of complex, infinite primes of K.

Finally, let $w(K)$ denote the order of the group $W(K)$.

2. An algebra A is called primary if it has but a single maximal ideal P. P must then be the radical of A, and hence nilpotent. The quotient $A/P = K$ is the algebraic number field associated with A. By a theorem of Wedderburn, we may regard K as imbedded in A, with the unit of A also the unit of K. In this case, we may write A as the direct sum of vector spaces $A = K \dotplus P$. Hence we may regard $O(K)$ as contained in A.

Let O be any order of A containing $O(K)$. Then the group $U(K)$ is a subgroup of $U(O)$. For each $i = 1, 2, \cdots$, let $V_i = 1 + (P^i \cap O)$. Since $1 \in O$, V_i is exactly the set of all elements x of O with $x \equiv 1 \pmod{P^i}$. V_i is evidently closed under multiplication. Let $x = 1 + y \in V_i$, $y \in P^i \cap O$. Then there is a $t \geqq 1$ such that $y^t = 0$. So $x^{-1} = 1 - y + y^2 - \cdots \pm y^{t-1} \in V_i$, since each $y^j \in P^i \cap O$. Hence V_i is a multiplicative subgroup of O, or $V_i \subseteqq U(O)$.

LEMMA 1. $U(O) = U(K) \otimes V_1$.

Proof. Consider the endomorphism $x \to E(x)$ of A onto $K \subseteqq A$ with kernel P. This is just the projection onto the first factor of the vector direct sum $A = K \dotplus P$. Since O is a finite Z-module, so is $E(O)$. Hence any element of $E(O)$ is integral over Z, and $E(O) \subseteqq O(K)$. It follows at once that $E(U(O)) \subseteqq U(K)$. On the other hand, $U(O) \supseteqq U(K)$ and E is the identity map on $U(K) \subseteqq K$. Thus $E(U(O)) = U(K)$. The kernel of the endomorphism induced by E on $U(O)$ is clearly $1 + P = V_1$. And E is identity on $U(K) = E(U(O))$. It follows at once that $U(K) \cap V_1 = (1)$ and $U(K) \cdot V_1 = U(O)$, which imply the desired result.

The structure of $U(K)$ is given by (4) of §1. The structure of V_1 is given by

LEMMA 2. *V_1 is a free abelian group on $[P:Q]$ generators.*

Proof. Consider a fixed $i \geqq 1$ with $P^i \neq (0)$. Since O is a lattice in the vector space A, and P^i is a Q-subspace of A, $P^i \cap O$ is a lattice in P^i. Since P^{i+1} is a Q-subspace of P^i, $(P^i \cap O)/P^{i+1}$ is a lattice in P^i/P^{i+1}. Let $t = [P^i:Q] - [P^{i+1}:Q] = [P^i/P^{i+1}:Q]$. Pick $e_1, \cdots, e_t \in P^i \cap O$, such that $e_1 + P^{i+1}, \cdots, e_t + P^{i+1}$ are a Z-basis of $(P^i \cap O)/P^{i+1}$. Consider the elements $y_1, \cdots, y_t = 1 + e_1, \cdots, 1 + e_t \in V_i$. If $n_1, \cdots, n_t \in Z$ are not all zero, then

$$\begin{aligned} y_1^{n_1} \cdots y_t^{n_t} &= (1 + e_1)^{n_1} \cdots (1 + e_t)^{n_t} \\ &\equiv (1 + n_1 e_1) \cdots (1 + n_t e_t) \pmod{P^{i+1}} \\ &\equiv 1 + (n_1 e_1 + \cdots + n_t e_t) \pmod{P^{i+1}}. \end{aligned}$$

Since $e_1, \cdots, e_t$ are additively independent mod P^{i+1}, it follows that

$$n_1 e_1 + \cdots + n_t e_t \not\equiv 0 \pmod{P^{i+1}}$$

and

$$y_1^{n_1} \cdots y_t^{n_t} \neq 1.$$

Thus the $y_1, \cdots, y_t$ are multiplicatively independent units in V_i. Let $U_i = (y_1, \cdots, y_t)$ be the subgroup of V_i generated by $y_1, \cdots, y_t$. Then U_i is a free abelian group on t generators, and $U_i \cap V_{i+1} = (1)$.

Let $y \in V_i$. Then $y = 1 + p$, $p \in O \cap P^i$. By the choice of $e_1, \cdots, e_t$, there are $n_1, \cdots, n_t \in Z$ such that

$$p \equiv n_1 e_1 + \cdots + n_t e_t \pmod{P^{i+1}},$$

and

$$\begin{aligned} y \cdot (y_1^{n_1} \cdots y_t^{n_t})^{-1} &\equiv (1 + n_1 e_1 + \cdots + n_t e_t)(1 - n_1 e_1 - \cdots - n_t e_t) \pmod{P^{i+1}} \\ &\equiv 1 \pmod{P^{i+1}}. \end{aligned}$$

Thus $y \in U_i \cdot V_{i+1}$ and $V_i = U_i \otimes V_{i+1}$. By induction, we get

$$V_1 = U_1 \otimes V_2 = U_1 \otimes U_2 \otimes V_3 = \cdots = U_1 \otimes U_2 \otimes \cdots \otimes U_s,$$

where s is the minimum integer such that $P^{s+1} = (0)$. (If $s = 0$, then $P = (0)$, and the lemma is trivial, since $V_1 = (1)$.) Since each U_i is free abelian, so is V_1, and

$$\begin{aligned} r(V_1) &= r(U_1) + \cdots + r(U_s) \qquad \text{(by (2))} \\ &= ([P:Q] - [P^2:Q]) + ([P^2:Q] - [P^3:Q]) + \cdots \\ &= [P:Q] - [P^{s+1}:Q] = [P:Q]. \end{aligned}$$

By Lemma 2, $r(V_1) = [P:Q]$ and $\mathrm{Tor}(V_1) = (1)$. Hence, by Lemma 1 and equations (2)

$$\begin{aligned} r(O) &= r(K) + [P:Q] = [A:Q] + r(K) - [K:Q], \\ \mathrm{Tor}(O) &= \mathrm{Tor}(U(K)) = W(K). \end{aligned} \tag{5}$$

Now let us turn to the case of a general algebra A. First we show

LEMMA 3. *If O, O' are two orders of A, then $r(O) = r(O')$.*

Proof. Let $x_1, x_2, \cdots$ be a set of $r(O')$ independent units of $U(O')$. Since O, O' are lattices in the finite-dimensional vector space A over Q, there is an integer $s > 1$ such that $sO' \subseteq O$. The quotient ring O'/sO' is a finite ring with unity, since $1/s \notin O'$. Hence its group of units has finite order g. Each x_i, being a unit in O', is congruent mod sO' to a unit of O'/sO'. Hence $x_i^g \equiv 1 \pmod{sO'}$, for each i. Since $1 \in O$, and $sO' \subseteq O$, this implies $x_i^g \in O$, for each i. Similarly, $(x_i^g)^{-1} = (x_i^{-1})^g \in O$. Thus the x_i are $r(O')$ independent units of O, and $r(O) \geqq r(O')$.

By symmetry, $r(O) = r(O')$.

It is known (see [4]) that any algebra A is a unique direct sum $A = A_1 \oplus \cdots \oplus A_s$ of primary subalgebras A_i. Let $K_i \subseteqq A_i$ be the field associated with A_i. Let O be any order of A, and let O_i be its image under projection from A to A_i. Let O_i' be the module product $O(K_i)\cdot O_i$. Then O_i' is an order of A_i containing $O(K_i)$, to which we may apply the discussion above leading to equations (5).

Let $O' = O_1' \oplus \cdots \oplus O_s'$. Then O' is an order of A containing O. $x = x_1 \oplus \cdots \oplus x_s$ is a unit in O' if and only if each x_i is a unit in O_i'. Thus $U(O')$ is a direct product:

$$U(O') = U(O_1') \otimes \cdots \otimes U(O_s').$$

By Lemma 3 and equations (2),

$$r(O) = r(O') = r(O_1') + \cdots + r(O_s').$$

Since $O \subseteqq O'$, $\mathrm{Tor}(O) \subseteqq \mathrm{Tor}(O')$. Hence

$$\mathrm{Tor}(O) \subseteqq \mathrm{Tor}(O_1') \otimes \cdots \otimes \mathrm{Tor}(O_s').$$

Combining these results with equations (5), we get

THEOREM 1. *Let $A = A_1 \oplus \cdots \oplus A_s$ be a direct sum of primary subalgebras A_i, with associated algebraic number fields $K_i \subseteqq A_i$. Let O be any order of A. Then*

$$r(O) = [A:Q] + \textstyle\sum_{i=1}^{s} (r(K_i) - [K_i:Q]),$$

$$\mathrm{Tor}(O) \subseteqq W(K_1) \otimes \cdots \otimes W(K_s),$$

$$S(O) \leqq s.$$

The last statement follows immediately from the preceding one.

3. Now assume that A is an algebra over K as well as Q. As above, $A = A_1 \oplus \cdots \oplus A_s$, where the A_i are now also K-algebras. If K_i is the field corresponding to A_i, then K_i is also a K-algebra, i.e., an extension field of an isomorphic image of K.

Let V be a unitary A-module, i.e., one such that the unit 1 of A gives the identity map of V. Then V is a K-vector space, and we shall assume $[V:K] < \infty$.

Let $1 = e_1 \oplus \cdots \oplus e_s$ be the decomposition of 1 into orthogonal idempotents. Then we get a corresponding decomposition of V as an A-module:

$$V = V\cdot 1 = Ve_1 \oplus \cdots \oplus Ve_s = V_1 \oplus \cdots \oplus V_s,$$

where $V_i = Ve_i$. These V_i have the properties:

$$V_i A_j = Ve_i A_j = V\cdot(0) = (0) \qquad \text{if } i \neq j,$$

$$V_i A_i \subseteqq V_i,$$

$$(ve_i)e_i = v(e_i^2) = ve_i \qquad \text{for any } v \in V.$$

Thus each V_i is a unitary A_i-module, and therefore a K_i-vector space. The structures of V_i as K- and K_i-vector spaces match up with the imbedding of an isomorphic image of K in K_i, so that

$$[V_i : K] = [V_i : K_i][K_i : K].$$

Now assume that V is a faithful A-module. Then each V_i is a faithful A_i-module. A_i can be considered as a commutative algebra of K-linear transformations of the vector space V_i. By a theorem of Schur (see [5]), this implies that

$$[A_i : K] \leqq 1 + [n_i^2/4],$$

where $n_i = [V_i : K]$. Summing over i, we get

$$[A : K] = \sum_{i=1}^{s} [A_i : K] \leqq s + \sum_{i=1}^{s} [n_i^2/4]. \tag{6}$$

Since V_i is a faithful A_i-module, $[V_i : K_i] \geqq 1$. If we put $n = [V : K]$, we have

$$n = \sum_{i=1}^{s} n_i = \sum_{i=1}^{s} [V_i : K_i][K_i : K] \geqq \sum_{i=1}^{s} [K_i : K] \geqq s. \tag{7}$$

We reduce the sum on the right side of (6) to a more manageable form by using

LEMMA 4. *If $x, y \in Z$ are both $\geqq 1$, then*

$$[x^2/4] + [y^2/4] \leqq [(x + y - 1)^2/4].$$

Proof. If one of x, y, say x, is equal to 1, then

$$[x^2/4] + [y^2/4] = [y^2/4] = [(x + y - 1)^2/4],$$

and the inequality is trivially satisfied.

Assume both x and $y > 1$. Then

$$2(x - 1)(y - 1) - 1 \geqq 1 > 0.$$

Since the only quadratic residues mod 4 are 1 and 0, we also have

$$[x^2/4] + [y^2/4] = [(x^2 + y^2)/4].$$

Combining these inequalities, we have

$$\begin{aligned}[x^2/4] + [y^2/4] = [(x^2 + y^2)/4] &\leqq [(x^2 + y^2 + 2(x - 1)(y - 1) - 1)/4] \\ &\leqq [(x + y - 1)^2/4].\end{aligned}$$

Since $n_i \geqq 1$ for $i = 1, \cdots, s$, this lemma implies that

$$\begin{aligned}[n_1^2/4] + \cdots + [n_s^2/4] &\leqq [(n_1 + n_2 - 1)^2/4] + [n_3^2/4] + \cdots + [n_s^2/4] \\ &\leqq \cdots \leqq [(n_1 + \cdots + n_s - s + 1)^2/4] \\ &\leqq [(n - s + 1)^2/4].\end{aligned}$$

Substituting this in (6), we obtain

$$[A:K] \leqq s + [(n - s + 1)^2/4]. \tag{8}$$

Let $x = 2$ in Lemma 4. Then we get

$$\text{If } y \geqq 1, \quad \text{then} \quad 1 + [y^2/4] \leqq [(y + 1)^2/4].$$

If $s \leqq n$, then $n - s + 1 \geqq 1$, so this implies that

$$s + [(n - s + 1)^2/4] \leqq (s - 1) + [(n - (s - 1) + 1)^2/4],$$

or

$$s + [(n - s + 1)^2/4] \text{ increases as } s \text{ decreases.} \tag{9}$$

(8) gives us an estimate for one term of the expression for $r(O)$ in Theorem 1. To estimate the other term, we use

LEMMA 5. *Let K' be an extension field of K. Then*

$$r(K') - [K':Q] \leqq r(K) - [K:Q] < 0.$$

Proof. Let R_1 be the set of real infinite primes of K, R_2 the set of imaginary infinite primes. Let R_1', R_2' be the corresponding sets for K'. Let r_1, r_2, r_1', r_2' be the cardinals of R_1, R_2, R_1', R_2', respectively. Let $[K':K] = m$.

Each prime in R_2 splits in K' into m primes in R_2'. Number the primes in R_1 in some order. Suppose that the j^{th} prime in R_1 splits in K' into n_j primes in R_1' and m_j primes in R_2'. Then

$$n_j + m_j \leqq n_j + 2m_j = m \qquad \text{for all } j,$$

$$r_1' = \sum_{j=1}^{r_1} n_j, \qquad r_2' = m \cdot r_2 + \sum_{j=1}^{r_1} m_j,$$

$$[K':Q] = m \cdot [K:Q].$$

Using (4), we have

$$\begin{aligned} r(K') - [K':Q] &= r_1' + r_2' - 1 - m \cdot [K:Q] \\ &= m \cdot r_2 + \sum_{j=1}^{r_1} (n_j + m_j) - 1 - m \cdot [K:Q] \\ &\leqq m \cdot r_2 + m \cdot r_1 - 1 - m \cdot [K:Q] \\ &\leqq (m - 1) \cdot (r_1 + r_2 - [K:Q]) + (r_1 + r_2 - 1) - [K:Q] \\ &\leqq r(K) - [K:Q], \end{aligned}$$

since

$$r_1 + r_2 \leqq r_1 + 2r_2 = [K:Q].$$

This last statement, however, also implies that

$$r(K) = r_1 + r_2 - 1 \leqq [K:Q] - 1 < [K:Q],$$

or

$$r(K) - [K:Q] < 0.$$

Applying (8) and Lemma 5 to the expression for $r(O)$ in Theorem 1, we get

$$\begin{aligned} r(O) &= [A:Q] + \textstyle\sum_{i=1}^{s} (r(K_i) - [K_i:Q]) \\ &\leqq [A:K][K:Q] + s\cdot(r(K) - [K:Q]) \\ &\leqq (s + [(n - s + 1)^2/4])\cdot[K:Q] + s\cdot(r(K) - [K:Q]) \qquad (10) \\ &\leqq [(n - s + 1)^2/4]\cdot[K:Q] + s\cdot r(K). \qquad (11) \end{aligned}$$

By (9) and the second inequality of Lemma 5, both terms in (10) increase as s decreases. So the same holds for (11), i.e.,

(12) If $s \leqq n$, then the expression in (11) increases as s decreases.

In particular, the last statement of Theorem 1 gives

$$1 \leqq S(O) \leqq s.$$

Thus

$$\begin{aligned} r(O) &\leqq [(n - S(O) + 1)^2/4]\cdot[K:Q] + S(O)\cdot r(K) \qquad (11') \\ &\leqq [n^2/4]\cdot[K:Q] + r(K). \end{aligned}$$

By the second statement of Theorem 1, the order of $\mathrm{Tor}(O)$ is not larger than

$$\prod_{i=1}^{s} w(K_i). \qquad (13)$$

We wish to find the least upper bound (possibly infinite) $w(n, K)$ for the expression (13) under the conditions

$$\begin{aligned} &K_i \text{ is an extension of } K, && i = 1, \cdots, s, \\ &\textstyle\sum_{i=1}^{s} [K_i:K] \leqq n. \end{aligned} \qquad (14)$$

By (7), this will give us an upper bound for the order of $\mathrm{Tor}(O)$.

For the rest of this section, we are going to manipulate and construct several extension fields of K. For simplicity, we shall assume that all fields lie in a fixed algebraic closure of K. We also adopt the following notation: If K' is a field and N is any positive integer, then $K'\{N\}$ is the field obtained by adjoining a primitive N^{th} root of 1 to K'.[3]

Consider any set of fields $K_1, \cdots, K_s$ satisfying (14). Each K_i contains a primitive $w(K_i)^{\text{th}}$ root of 1, and hence $K\{w(K_i)\}$. Thus

$$[K\{w(K_i)\}:K] \leqq [K_i:K], \qquad i = 1, \cdots, s,$$

[3] On reading the proofs, it occurred to me that the argument from here until Theorem 2 would have been less tortuous had I defined $K'\{N\}$ to be the field obtained from K' by adjoining a primitive N^{th} root of -1 (instead of $+1$ as above). Most of the difficulties of exposition are caused by the fact that, as it is defined now, $w(Q\{N\})$ may be either N or $2N$ depending upon the residue of N modulo 4. In the new definition $w(Q\{N\})$ would always be $2N$, so that no distinct treatment of the two cases would be necessary, as it is now in several places below. This change in notation, of course, would not modify the straightforward reduction argument in the text.

so the fields $K\{w(K_1)\}, \cdots, K\{w(K_s)\}$ also satisfy conditions (14). But $w(K\{w(K_i)\}) = w(K_i)$. Thus, if we replace K_i by $K\{w(K_i)\}$, $i = 1, \cdots, s$, (13) is not reduced. Therefore

In calculating $w(n, K)$, we may assume that each $K_i = K\{N_i\}$, for some N_i.

Let K' be the largest absolutely abelian subfield of K. Let N be some positive integer, and let $\bar{K}$ be some absolutely normal extension of $K\{N\}$. Let G_1 be the subgroup of the Galois group of $\bar{K}/Q$ corresponding to K, and G_2 the subgroup corresponding to $K'\{N\}$. Since K' is absolutely abelian, so is $K'\{N\}$. Hence G_2 is a normal subgroup. By the isomorphism theorems

$$G_1 G_2 / G_2 \cong G_1 / (G_1 \cap G_2).$$

$G_1 G_2$ is the subgroup corresponding to $K' = K \cap K'\{N\}$, and $G_1 \cap G_2$ is the subgroup corresponding to $K\{N\} = KK'\{N\}$. The isomorphism above implies that

$$[K'\{N\}:K'] = [K\{N\}:K].$$

If $K\{N_1\}, \cdots, K\{N_s\}$ is a set of fields satisfying (14), with $N_i = w(K\{N_i\})$, then, by this equation, $K'\{N_1\}, \cdots, K'\{N_s\}$ is a set of fields satisfying (14) with K replaced by K'. Since

$$N_i = w(K\{N_i\}) = w(K'\{N_i\}),$$

replacing $K\{N_i\}$ by $K'\{N_i\}$ leaves (13) unchanged. Therefore

$$w(n, K) = w(n, K').$$

Now assume K absolutely abelian. Then it is a subfield of some cyclotomic field $Q\{N\}$. Since $Q\{N_1\} \cap Q\{N_2\} = Q\{(N_1, N_2)\}$, there is a smallest cyclotomic field containing K. Let this be $Q\{M\}$, where we assume that M is also minimal, i.e., that $M \not\equiv 2 \pmod 4$. Then M is divisible by exactly the ramified primes of K.

Suppose an integer N is divisible only by primes unramified in K. Then $(N, M) = 1$, so that

$$[Q\{M \cdot N\}:Q\{M\}] = \phi(N) = [Q\{N\}:Q].$$

Since $Q \subseteqq K \subseteqq Q\{M\}$, and since $K\{N\} = Q\{N\} \cdot K$, this implies that

$$[K\{N\}:K] = \phi(N). \tag{15}$$

Notice that this holds for any absolutely abelian field K and any N prime to the discriminant of K.

Now let N be any integer. Then $N = N_1 N_2$, where N_1 is divisible only by primes unramified in K, and N_2 only by primes ramified in K. Any prime dividing N_1 is unramified in K and in $Q\{N_2\}$ (since $(N_1, N_2) = 1$),

and hence is unramified in the absolutely abelian field $K\{N_2\}$. Applying (15) to both $K\{N_2\}$ and K, we get

$$[K\{N_1 N_2\}:K] = \phi(N_1)\cdot[K\{N_2\}:K],$$
$$[K\{N_1\}:K] = \phi(N_1).$$

Since 2 divides only one of N_1, N_2 and since we may assume without loss of generality that $N \not\equiv 2 \pmod 4$, we have $N_1 \not\equiv 2 \pmod 4$. Hence $N_1 > 1$ implies $\phi(N_1) > 1$. $K\{N_2\} = K$ if and only if $N_2 \mid w(K)$. In that case we might as well take $N_2 = 1$. Otherwise $[K\{N_2\}:K] \geqq 2$. Hence we have

$$[K\{N\}:K] \geqq 2\phi(N_1) = 2[K\{N_1\}:K] \qquad \text{if } N_2 \neq 1,$$
$$[K\{N\}:K] \geqq 2[K\{N_2\}:K] \qquad \text{if } N_1 \neq 1,$$
$$[K\{N\}:K] \geqq [K\{N_1\}:K] + [K\{N_2\}:K] \qquad \text{if both } N_1 \text{ and } N_2 \neq 1. \tag{16}$$

Now notice that (15) implies that $w(K\{N\}) = N_1 w(K\{N_2\})$. For, if $w = w(K\{N\})$, we may split up $w = w_1 w_2$ as we did N. By (15)

$$[K\{N\}:K] = [K\{w\}:K] = \phi(w_1)\cdot[K\{w_2\}:K].$$

But $K\{w_2\} \supseteqq K\{N_2\}$, since clearly $N_2 \mid w_2$. Thus

$$\phi(N_1)[K\{N_2\}:K] = [K\{N\}:K] \geqq \phi(w_1)\cdot[K\{N_2\}:K],$$

or

$$\phi(N_1) \geqq \phi(w_1).$$

But $N_1 \mid w_1$. So either $w_1 = N_1$ or $w_1 = 2N_1$, according as 2 is or is not ramified in K.

Since $\phi(N_1) = \phi(w_1)$, we must have $K\{w_2\} = K\{N_2\}$. Since $K\{N_2\} \subseteqq Q\{MN_2\}$, the only primes which may divide $w(K\{N_2\})$ are those dividing M and 2. So $W(K\{N_2\}) = W(K\{N\}) \cap K\{N_2\}$ must have order w_2 or $2w_2$ according as 2 is or is not ramified. In the former case $w_1 = N_1$, and in the latter $w_1 = 2N_1$. So, in either case, $w(K\{N\}) = N_1\cdot w(K\{N_2\})$.

Applying this last argument to N and to N_1, we get

$$w(K\{N\}) = N_1\cdot w(K\{N_2\}),$$
$$w(K\{N_1\}) = N_1\cdot w(K).$$

Thus

$$w(K\{N_1 N_2\}) = N_1\cdot w(K\{N_2\}) < N_1\cdot w(K)\cdot w(K\{N_2\}) = w(K\{N_1\})\cdot w(K\{N_2\}).$$

From this and (16), it follows that, if $N_1 \neq 1$ and $N_2 \neq 1$, then we may replace $K\{N_1 N_2\}$, whenever it appears among the K_i, by the two fields $K\{N_1\}$ and $K\{N_2\}$ and increase the expression (13) without increasing (14). Thus we have shown

In calculating $w(n, K)$, we need only consider fields $K\{N_i\}$ where either no prime dividing N_i ramifies or every prime dividing N_i ramifies.

Assume N prime to the discriminant of K. As above, $w(K\{N\}) = Nw(K)$. But $w(K) \geqq 2$ implies that $w(K)^{\phi(N)} \geqq Nw(K)$, except when $w(K) = 2$ and $N = 3$. So, with that single exception, we may replace $K\{N\}$ with $\phi(N) = [K\{N\}:K]$ copies of K. The sum (14) remains unchanged while (13) increases. Hence, the only time we have to consider such an N is when $w(K) = 2$ and $N = 3$.

Assume that only primes dividing M divide N. Then

$$[Q\{M\}\{N\}:Q\{M\}] = N/(M, N) = [Q\{N\}:Q\{(M, N)\}].$$

Since $Q\{(M, N)\} \subseteqq K\{(M, N)\} \subseteqq Q\{M\}$, and since $K\{N\} = Q\{N\}\cdot K\{(M, N)\}$, this implies that

$$[K\{N\}:K\{(M, N)\}] = N/(M, N).$$

Suppose 2 does not ramify in K. Then 2 does not ramify in $K\{N\}$. Let $w = \frac{1}{2}\cdot w(K\{N\})$, $w_1 = \frac{1}{2}\cdot w(K\{(M, N)\})$. Then $W(K\{(M, N)\}) = W(K\{N\}) \cap W(Q\{M\})$ implies $w_1 = (w, M)$. Since $K\{N\} \subseteqq Q\{NM\}$, the only primes dividing w are ramified in K. Therefore, as above,

$$[K\{w\}:K\{(w, M)\}] = w/(w, M) = w/w_1 .$$

But $K\{w\} = K\{N\}$, $K\{(w, M)\} = K\{(M, N)\}$. Hence

$$w/w_1 = N/(M, N),$$

or

$$w(K\{N\}) = (N/(M, N))\cdot w(K\{(M, N)\}).$$

A similar proof shows the same result if 2 ramifies.

If we replace $K\{N\}$ by $N/(M, N)$ copies of $K\{(M, N)\}$, then (14) does not change. But $w(K\{(M, N)\}) \geqq 2$ imples that

$$w(K\{(M, N)\})^{N/(M,N)} \geqq (N/(M, N))\cdot w(K\{(M, N)\}) = w(K\{N\}),$$

so (13) increases. Hence the only such N we have to consider are the divisors of M.

Finally, notice that, if $\sum [K_i:K] < n$, we may always add enough copies of K to make it equal n. We have shown

$$w(n, K) = \text{Max}\,(\prod_{i=1}^{s} w(K\{N_i\})),$$

(17) where either $N_i \mid M$, or $N_i = 3$ and $w(K) = 2$,

$$\sum_{i=1}^{s} [K\{N_i\}:K] = n.$$

Notice that, since there are only a finite number of N_i to consider, there are only a finite number of products to consider, and $w(n, K)$ must be finite.

Incidentally, we may compute the odd part of M without going outside of K. For an odd prime p divides M exactly to the exponent $e \geqq 1$ if and only if

(1) p ramifies in K,

(2) p^{e-1} is the degree of wild ramification of p in K.

We have noted condition (1) above. For (2), let $p_1, \cdots, p_t$ be the odd primes dividing M, and let $p_0 = 1$ if $2 \nmid M$ and $p_0 = 4$ if $4 \mid M$. Then $K\{p_0 p_1 \cdots p_t\}$ lies between $Q\{M\}$ and $Q\{p_0 p_1 \cdots p_t\}$. But, by the choice of p_i, the only such intermediate fields are cyclotomic. Since $Q\{M\}$ is the smallest cyclotomic field containing K, we must have

$$K\{p_0 p_1 \cdots p_t\} = Q\{M\}.$$

In passing from K to $K\{p_0 \cdots p_{t-1}\}$, p_t does not ramify, and in passing from $K\{p_0 \cdots p_{t-1}\}$ to $K\{p_0 \cdots p_t\}$, it ramifies tamely if at all, so the degree of wild ramification of p_t in K is the same as its degree of wild ramification in $Q\{M\}$, which is p_t^{e-1}, where p_t^e exactly divides M.

If $4 \mid w(K)$, a similar result holds for $p = 2$. But if $w(K) \equiv 2 \pmod 4$, there seems to be no such easy method of computing the power of 2 dividing M.

Collecting our results from (7), (11′) and (17), we have

THEOREM 2. *Let A be an algebra over K. Let V be a faithful, unitary A-module with $[V:K] = n$. Let O be an order in A. Then*

$$\begin{aligned} 1 &\leqq S(O) \leqq n, \\ r(O) &\leqq [(n - S(O) + 1)^2/4] \cdot [K:Q] + S(O) \cdot r(K) \\ &\leqq [n^2/4] \cdot [K:Q] + r(K), \end{aligned}$$

and the order of $\mathrm{Tor}(O)$ *is bounded by*

$$w(n, K) = \mathrm{Max}\,(\textstyle\prod_{i=1}^{s} w(K\{N_i\})),$$

where the N satisfy $\sum [K\{N_i\}:K] = n$ and either $N_i \mid M$, or $N_i = 3$ and $w(K) = 2$, and where M is the smallest positive element of Z such that $Q\{M\} \cap K$ is the maximal absolutely abelian subfield of K.

4. If n is any natural number and K any algebraic number field, we define the general unimodular group $\Delta_n(K)$ to be the multiplicative group of all $n \times n$ matrices with elements in $O(K)$ whose determinants are in $U(K)$.

Let G be any abelian subgroup of $\Delta_n(K)$. Then G is an abelian multiplicative subgroup of the full matrix algebra $M_n(K)$ over K. Let A be the subalgebra of $M_n(K)$ generated over K by G. Then A is a commutative subalgebra with identity. The imbedding of A in $M_n(K)$ makes a faithful, unitary A-module of K-dimension n out of whatever K-vector space one considers $M_n(K)$ as acting on.

Let O be the set of matrices in A whose elements are in $O(K)$. Then O is an order of A. If $u \in U(O)$, then both u and u^{-1} have elements in $O(K)$. So $u \in \Delta_n(K)$ and $U(O)$ is an abelian subgroup of $\Delta_n(K)$. Evidently $G \subseteqq U(O)$, so that

$$r(G) \leqq r(O), \qquad \mathrm{Tor}(G) \subseteqq \mathrm{Tor}(O), \qquad S(G) \leqq S(O).$$

Applying Theorem 2 and (12), we get

$$r(G) \leqq [(n - S(G) + 1)^2/4]\cdot[K:Q] + S(G)\cdot r(K) \tag{18}$$

$$\leqq [n^2/4]\cdot[K:Q] + r(K), \tag{18'}$$

$$1 \leqq S(G) \leqq n, \tag{19}$$

and the bound $w(n, K)$ for the order of $\mathrm{Tor}(G)$.

Some examples will show that these are the best possible bounds.

Example 1. Let $n = 2m$ be even. Consider all matrices of the form

$$\begin{pmatrix} xI_m & 0_m \\ Y & xI_m \end{pmatrix},$$

where I_m is the $m \times m$ identity matrix, 0_m is the $m \times m$ zero matrix, x is any element of K, and Y any element of $M_m(K)$. These matrices form a commutative algebra A over K of dimension $(n^2/4) + 1 = m^2 + 1$. The ideal P of matrices with $x = 0$ is the radical of A and has K-dimension m^2. A is primary, and K is the field associated with A. The imbedding of K in A is given by $x \to xI_n$, for $x \in K$. Let O be the set of all matrices in A with $x \in O(K)$ and each element of Y in $O(K)$. O is clearly an order of A containing $O(K)$, so Theorem 1 applies, giving

$$r(O) = r(K) - [K:Q] + [A:Q] = r(K) + [n^2/4]\cdot[K:Q].$$

Since each element of O has K-integral entries, $U(O) \subseteqq \Delta_n(K)$. Hence $\Delta_n(K)$ has an abelian subgroup of rank $r(K) + [n^2/4]\cdot[K:Q]$.

Example 2. Let $n = 2m + 1$ be odd. Consider the set of all matrices of the form

$$\begin{pmatrix} xI_{m+1} & 0_{m+1,m} \\ Y & xI_m \end{pmatrix},$$

where I_m, I_{m+1} are identities of the indicated orders, $0_{m+1,m}$ is an $(m + 1) \times m$ zero matrix, $x \in K$, and Y is an arbitrary $m \times (m + 1)$ matrix with elements in K. The analysis is the same as in Example 1, except that the radical has K-dimension $m(m + 1) = (n^2 - 1)/4 = [n^2/4]$. Again $\Delta_n(K)$ has an abelian subgroup of rank $r(K) + [n^2/4]\cdot[K:Q]$.

From these two examples it follows that (18') is a best possible estimate.

Example 3. Consider all matrices of the form

$$\begin{pmatrix} M_1 & & & & & \\ & x_1 & & & & \\ & & x_2 & & & \\ & & & \cdot & & \\ & & & & \cdot & \\ & & & & & \cdot \\ & & & & & x_{s-1} \end{pmatrix},$$

where M_1 is any $(n - s + 1) \times (n - s + 1)$ matrix of the type of Example 1 or 2, whichever applies, $x_1, x_2, \cdots, x_{s-1}$ are any elements of K, and the blank spaces are zeroes. These matrices form an algebra over K. If A_1 is the subalgebra generated by the M_1, then

$$A \cong A_1 \oplus K \oplus K \oplus \cdots \oplus K,$$

where there are $s - 1$ K's. The elements of A with integral entries form an order O in A. By Theorem 1

$$\begin{aligned} r(O) &= [A:Q] + s\cdot(r(K) - [K:Q]) \\ &= ([(n - s + 1)^2/4] + 1 + \cdots + 1)[K:Q] - s\cdot[K:Q] + s\cdot r(K) \\ &= [(n - s + 1)^2/4]\cdot[K:Q] + s\cdot r(K), \end{aligned}$$

$$\mathrm{Tor}(O) = W(K) \otimes \cdots \otimes W(K) \qquad (s \text{ factors}).$$

Since $W(K) \neq (1)$, we see immediately that $S(O) = s$. It follows that (18) is also a best estimate. Since we may take $s = n$, (19) is best, too.

Example 4. Let $N_1, \cdots, N_s$ be positive integers such that

$$\sum [K\{N_i\}:K] = n$$

and $N_i = w(K\{N_i\})$, $i = 1, \cdots, s$. Let $f_i(X)$ be the monic irreducible polynomial satisfied over K by some primitive N_i^{th} root of 1. Then f_i has degree $[K\{N_i\}:K]$, and, since the roots of unity are algebraic integers, f_i has coefficients in $O(K)$. Let C_i be the companion matrix of the polynomial f_i. Since $f_i(C_i) = 0$, C_i is a matrix of multiplicative order $N_i : C_i^{N_i} = I$. C_i has coefficients in $O(K)$, as does its inverse $C_i^{N_i - 1}$. Hence $C_i \in \Delta_{[K\{N_i\}:K]}(K)$. Consider all matrices of the form

$$\begin{pmatrix} C_1^{x_1} & & & \\ & \cdot & & \\ & & \cdot & \\ & & & \cdot \\ & & & & C_s^{x_s} \end{pmatrix},$$

where the blank spaces are zeroes and the $x_i \in Z$ satisfy $0 \leqq x_i < N_i$, $i = 1, \cdots, s$. Since $\sum [K\{N_i\}:K] = n$, these matrices have order n. They all have integral elements, and they form an abelian group of order $N_1 \cdot \cdots \cdot N_s = \prod w(K\{N_i\})$. Hence $w(n, K)$ is a best possible bound on the order of $\mathrm{Tor}(G)$.

At first glance, $w(n, K)$ may not appear to be a very calculable bound. Actually it is fairly easy to compute once we know how K fits into $Q\{M\}$ (if we assume K absolutely abelian, which we can do without loss of generality). For example, if $K = Q\{M\}$ is itself cyclotomic, then for all

$N \mid M$, $K\{N\} = K$, so, by (17), we need only consider the case $N = 1$, or $N = 3$ if $w(K) = 2$. Thus we get

If $K = Q\{M\}$ is cyclotomic, then

$$\begin{aligned} w(n, K) &= w(K)^n && K \neq Q \\ &= 6^{n/2} && K = Q, \quad n \text{ even} \\ &= 2 \cdot 6^{[n/2]} && K = Q, \quad n \text{ odd.} \end{aligned}$$

For a more complicated example, consider the field $Q\{3^2 \cdot 7\}$. Let G be its Galois group over Q. Let a be a generator of the cyclic subgroup $\langle a \rangle$ corresponding to $Q\{7\}$, b a generator of the cyclic subgroup corresponding to $Q\{3^2\}$. Then a, b both have order 6, and $G = \langle a, b \rangle$ is the direct product of the subgroups $\langle a \rangle$, $\langle b \rangle$. The cyclotomic subfields of $Q\{3^2 \cdot 7\}$ then correspond to the subgroups

$$\begin{aligned} Q\{3^2 \cdot 7\} &\leftrightarrow \langle 1 \rangle \\ Q\{7\} &\leftrightarrow \langle a \rangle \\ Q\{3^2\} &\leftrightarrow \langle b \rangle \\ Q\{3\} &\leftrightarrow \langle a^2, b \rangle \\ Q\{3 \cdot 7\} &\leftrightarrow \langle a^2 \rangle \\ Q &\leftrightarrow \langle a, b \rangle. \end{aligned} \tag{20}$$

Let K be the field corresponding to the subgroup $\langle ab \rangle$. Since a, b both have order 6, it is clear that this subgroup contains none of the proper subgroups listed in (20). Hence no cyclotomic field smaller than $Q\{3^2 \cdot 7\}$ contains K, and we must have $M = 3^2 \cdot 7$. For the significant $N \mid M$, we have

$$\begin{aligned} K &\leftrightarrow \langle ab \rangle \\ K\{7\} &\leftrightarrow \langle ab \rangle \cap \langle a \rangle = \langle 1 \rangle \\ K\{3\} &\leftrightarrow \langle ab \rangle \cap \langle a^2, b \rangle = \langle a^2 b^2 \rangle \\ K\{3^2\} &\leftrightarrow \langle ab \rangle \cap \langle b \rangle = \langle 1 \rangle. \end{aligned} \tag{21}$$

For any field K, $w(K)$ is the largest positive integer w such that $Q\{w\} \subseteqq K$. So the inclusion relations among the subgroups in (20) and (21), and the relative indices of the subgroups in (21) give

$$\begin{aligned} [K:K] &= 1, & w(K) &= 2, \\ [K\{7\}:K] &= 6, & w(K\{7\}) &= 2 \cdot 3^2 \cdot 7, \\ [K\{3\}:K] &= 2, & w(K\{3\}) &= 2 \cdot 3. \end{aligned}$$

Since $2^3 \cdot 3^3 > 2 \cdot 3^2 \cdot 7$, we may replace $K\{7\}$ by three copies of $K\{3\}$ wherever it appears. Hence we get $w(n, K) = w(n, Q)$.

We noted in the last paragraph that, if $p_1, \cdots, p_t$ are the distinct ramified primes in the absolutely abelian field K, and if 2 does not ramify, then $K\{p_1 \cdots p_t\} = Q\{M\}$. In the example above we had $K\{7\} = Q\{M\}$, so some of the p_i may be superfluous. Also note that $K\{3\} \neq K\{3^2\}$, so the following statement is not true: $K\{p_i\}$ contains a primitive $p_i^{e^{\text{th}}}$ root of 1, where p_i^{e-1} exactly divides M. You must adjoin all the p_i^{th} roots of 1 before this happens.

We define the restricted unimodular group $\Gamma_n(K)$ to be the subgroup of $\Delta_n(K)$ consisting of those matrices of determinant 1. Let $D_n(K)$ be the center of $\Delta_n(K)$, $C_n(K)$ the center of $\Gamma_n(K)$. Then $D_n(K)$ consists of all matrices xI_n, where $x \in U(K)$. So $D_n(K)$ is isomorphic to $U(K)$. $C_n(K)$ consists of all xI_n, where $x^n = 1$. So $C_n(K) \subseteqq D_n(K)$, and $C_n(K)$ is cyclic of order $(w(K), n)$.

If G is any abelian subgroup of $\Gamma_n(K)$, then G commutes elementwise with the center $D_n(K)$ in $\Delta_n(K)$. Since $G \cap D_n(K) \subseteqq G \cap C_n(K) \subseteqq \mathrm{Tor}(G)$, we have

$$r(G \cdot D_n(K)) = r(G) + r(D_n(K)) = r(G) + r(K).$$

Also $G \subseteqq G \cdot D_n(K)$ implies

$$S(G) \leqq S(G \cdot D_n(K)) \leqq n.$$

Using this, (18), and (12), we get

$$\begin{aligned} r(G) &= r(G \cdot D_n(K)) - r(K) \\ &\leqq [(n - S(G \cdot D_n(K)) + 1)^2/4] \cdot [K:Q] + (S(G \cdot D_n(K)) - 1) \cdot r(K) \\ &\leqq [(n - S(G) + 1)^2/4] \cdot [K:Q] + (S(G) - 1) \cdot r(K) \\ &\leqq [n^2/4] \cdot [K:Q]. \end{aligned}$$

That this last bound on $r(G)$ is a best possible result may be seen by considering the intersections with $\Gamma_n(K)$ of the groups of Examples 1 and 2.

If H is a finite abelian subgroup of $\Delta_n(K)$ with $S(H) = n$, then H is equivalent to a subgroup of the group of all matrices of the form

$$\begin{pmatrix} x_1 & & & & \\ & x_2 & & & \\ & & \cdot & & \\ & & & \cdot & \\ & & & & \cdot \\ & & & & & x_n \end{pmatrix},$$

where $x_1, \cdots, x_n \in W(K)$, and the blank spaces are zeroes. Since equivalence preserves determinants, $H \cap \Gamma_n(K)$ must be equivalent to a subgroup of the group F of all such matrices with $x_1 x_2 \cdots x_n = 1$. This group F has $S(F) = n - 1$, so $S(H \cap \Gamma_n(K)) \leqq n - 1$. Thus, for any abelian subgroup

G of $\Gamma_n(K)$, we must have

$$S(G) \leqq n - 1.$$

The example of F shows that this bound is best possible.

Since $C_n(K) \subseteqq \Gamma_n(K)$, we may assume that $C_n(K) \subseteqq G$. Then $\mathrm{Tor}(G \cdot D_n(K)) = \mathrm{Tor}(G) \cdot \mathrm{Tor}(D_n(K))$ has order $w(K)/(n, w(K))$ times the order of $\mathrm{Tor}(G)$. Hence we have the bound

$$w(n, K) \cdot (n, w(K))/w(K)$$

for the order of $\mathrm{Tor}(G)$.

Collecting these statements with those of (18) and (19), we finally come to

THEOREM 3. *Let G be an abelian subgroup of $\Delta_n(K)$. Then*

$$1 \leqq S(G) \leqq n, \qquad *$$

$$r(G) \leqq [(n - S(G) + 1)^2/4] \cdot [K:Q] + S(G) \cdot r(K) \qquad *$$

$$\leqq [n^2/4] \cdot [K:Q] + r(K), \qquad *$$

$$\text{order of } \mathrm{Tor}(G) \leqq w(n, K). \qquad *$$

If G is also a subgroup of $\Gamma_n(K)$, then

$$1 \leqq S(G) \leqq n - 1, \qquad *$$

$$r(G) \leqq [(n - S(G) + 1)^2/4] \cdot [K:Q] + (S(G) - 1) \cdot r(K)$$

$$\leqq [n^2/4] \cdot [K:Q], \qquad *$$

$$\text{order of } \mathrm{Tor}(G) \leqq w(n, K) \cdot (n, w(K))/w(K).$$

The bounds marked * are best possible.

REFERENCES

1. KARL GOLDBERG, *Unimodular matrices of order 2 that commute*, J. Washington Acad. Sci., vol. 46 (1956), p. 337–338.
2. O. TAUSSKY AND J. TODD, *Commuting bilinear transformations and matrices*, J. Washington Acad. Sci., vol. 46 (1956), p. 373–375.
3. H. S. M. COXETER, *On subgroups of the modular group*, J. Math. Pures Appl., vol. 37 (1958), pp. 317–319.
4. O. ZARISKI AND P. SAMUEL, *Commutative algebra*, Princeton, Van Nostrand, 1958, p. 205, Theorem 3.
5. J. SCHUR, *Zur Theorie der vertauschbaren Matrizen*, J. Reine Angew. Math., vol. 130 (1906), p. 66–76.

HARVARD UNIVERSITY
CAMBRIDGE, MASSACHUSETTS
NATIONAL BUREAU OF STANDARDS
WASHINGTON, D. C.