NORMAL CONGRUENCE SUBGROUPS OF THE $t\times t$ MODULAR GROUP[1]

BY M. NEWMAN

Communicated by A. M. Gleason, June 5, 1963

Let Γ denote the group of rational integral $t\times t$ matrices of determinant 1. If n is a positive integer, $\Gamma(n)$ denotes the *principal congruence subgroup* of Γ of *level n*, consisting of all elements of Γ congruent modulo n to a scalar matrix. The subgroup of $\Gamma(n)$ consisting of all elements of Γ congruent modulo n to the identity matrix is denoted by $\Gamma_1(n)$. Then $\Gamma(n)$, $\Gamma_1(n)$ are normal subgroups of Γ. A subgroup G of Γ containing a principal congruence subgroup $\Gamma(n)$ is termed a *congruence subgroup*, and is said to be of *level n* if n is the least such integer. Notice that $\Gamma_1(n)$ is not in general a congruence subgroup, according to the definition above.

Let p be a prime. Let $SL(t, p)$ denote the group of $t\times t$ matrices with elements from $GF(p)$ and determinant 1, and let $H(t, p)$ denote the normal subgroup of $SL(t, p)$ consisting of all scalar matrices. Then

$$SL(t, p) \cong \Gamma/\Gamma_1(p), \qquad H(t, p) \cong \Gamma(p)/\Gamma_1(p),$$

and $SL(t, p)$, $H(t, p)$ are of orders

$$p^{t^2-1}\prod_{j=2}^{t}(1-p^{-j}),\ (t, p-1)$$

respectively. In his book on the linear groups [1] Dickson proves that for $t>2$, $H(t, p)$ is a maximal normal subgroup of $SL(t, p)$ and this of course implies that $\Gamma(p)$ *is a maximal normal subgroup of* Γ. This result is used to prove the theorem that follows:

THEOREM 1. *Suppose that $t>2$. Then every normal congruence subgroup of odd level of Γ is a principal congruence subgroup.*

The theorem is also true for $t=2$, if the level is prime to 6. (The case $t=2$ for the group of linear fractional transformations has been treated in [3].) Since the structure of the proof of Theorem 1 is identical with that of the proof for $t=2$ given in [3], we only indicate the points of difference, and refer the reader to [3] for full details. The proof is arranged for an induction and what is actually proved is the slightly more general theorem that follows:

[1] The preparation of this note was supported by the Office of Naval Research.

THEOREM 2. *Suppose that $t>2$. Let m, n be positive integers, m odd. Let G be a normal subgroup of Γ such that $\Gamma(n)\supset G\supset\Gamma(mn)$. Then $G=\Gamma(nd)$, $d\mid m$.*

In order to prove this theorem generally it is necessary to give special proofs for the cases when m is a prime or the square of a prime. If m is any prime and $(m, n)=1$ then the theorem of Dickson referred to above implies the result. If m is an odd prime and $m\mid n$, then $\Gamma(n)/\Gamma(mn)$ is abelian of type $(m, m, \cdots, m)$ and it is not difficult to show that the normality of G implies that $G=\Gamma(n)$ or $\Gamma(mn)$. If m is the square of an odd prime, then the proofs given in [3] go over unchanged, with one exception: the commutator subgroup Γ' of Γ is no longer of index 6 in Γ (as is the case for $t=2$ and Γ the group of linear fractional transformations) but is in fact just Γ itself. This has been proved by Hua and Reiner (see [2]), although some care must be taken in interpreting their results since they consider the more general unimodular group in which the determinant is allowed to be -1 as well. The formal structure of the induction remains unchanged.

REFERENCES

1. L. E. Dickson, *Linear groups*, Dover, New York, 1958.

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

3. M. Newman, *Normal congruence subgroups of the modular group*, Amer. J. Math. (to appear).

NATIONAL BUREAU OF STANDARDS