THE LINEAR CONGRUENCE GROUP MODULO n

F. A. LEWIS

The symbol $GLH[m, n]$ will be used to represent the order of $GLH(m, n)$, the group of linear transformations on m variables whose coefficients are taken modulo n in such a way that the determinant of each transformation is prime to n. In this note we state four theorems on congruence groups, which may be obtained by modifying proofs of corresponding theorems[1] on groups of transformations with coefficients in a Galois field $GF[p^n]$. Theorem 5 gives a set of defining relations for a related abstract group.

THEOREM 1. $GLH[m, n] = \prod_{i=1}^{m} n^{i-1}\phi_i(n)$, *where* $\phi_i(n)$ *represents the ith totient of* n.

THEOREM 2. *The matrix of every transformation of* $GLH(m, n)$ *of determinant* s *equals* BD_s, *where* B *is derived from* $B_{r,c,\lambda}$ *and* D_s *is the diagonal matrix* $(1, 1, \cdots, s)$.

THEOREM 3. $SLH[m, n] = GLH[m, n]/\phi(n)$.

COROLLARY. $SLH[2, n] = n\phi_2(n)$.

THEOREM 4. $SLH(2, n) = \{V, W\}$, *where* V *and* W *are, respectively, the following transformations*: $x_1' = -x_2$, $x_2' = x_1$ *and* $x_1' = x_1$, $x_2' = x_1 + x_2$.

THEOREM[2] 5. *If* $n > 2$, $SLH(2, n)$ *is simply isomorphic with the abstract group whose generators* V *and* W *satisfy*

(a) $V^4 = I$,

(b) $W^n = I$, $WV^2 = V^2W$,

(c) $W^\lambda V W^\mu V W^{(\lambda+1)/(\lambda\mu-1)} V W^{\lambda\mu-1} V W^{(\mu+1)/(\lambda\mu-1)} V = I$, *for all values of* λ *and* μ *such that* $\lambda\mu - 1$ *is prime to* n.

Let g be the order of $G = \{V, W\}$. Since (a), (b), and (c) are satisfied by the generators of $SLH(2, n)$, $g \geqq n\phi_2(n)$.

If μ is prime to n, the substitutions $\lambda = \alpha(1 + 1/\beta)$ and $\mu = 1/\alpha$ in (c) yield

(c′) $W^{\alpha+\alpha/\beta} V W^{1/\alpha} V W^{\alpha+\alpha\beta+\beta} V W^{1/\beta} V W^{\beta+\beta/\alpha} V = I$,

for all α and β prime to n.

In order to simplify the computation, we define

Received by the editors August 4, 1950 and, in revised form, August 9, 1951.

[1] See Dickson, *Linear groups*, pp. 77–82, for statement of corresponding theorems and explanation of notation.

[2] The corresponding theorem on $SLH(2, p^n)$ is due to E. H. Moore; Dickson, loc. cit., p. 300.

$$R_\alpha = W^{1/\alpha}VW^{\alpha}VW^{1/\alpha}V$$

for all values of α prime to n. The following properties of the operator R may be established:

(d) $R_1 = I$,

(e) $(R_\alpha V)^2 = V^2$,

(f) $W^\rho R_\alpha = R_\alpha W^{\rho\alpha^2}$, where α is prime to n and ρ is arbitrary.

(f′) $R_\alpha V = VR_{1/\alpha}$,

(g) $R_{\alpha\beta} = R_\alpha R_\beta$.

Consider the following set of elements

$$\text{(h)} \qquad W^{(c+dx)/(a+bx)}R_{a+bx}V^{-1}W^{-b/(a+bx)}VW^{-x},$$

where (a, b) is prime to n, x is any integer such that $a+bx$ is prime to n, and $ad-bc\equiv 1 \pmod{n}$. The condition

$$W^{(c+dx)/(a+bx)}R_{a+bx}V^{-1}W^{-b/(a+bx)}VW^{-x} = W^{(c+dy)/(a+by)}R_{a+by}V^{-1}W^{-b/(a+by)}VW^{-y}$$

for all values of x and y for which $a+bx$ and $a+by$ are prime to n reduces to an equivalent form of (c). Hence a different choice of x yields the same set (h). Therefore, the number of distinct elements in the set is at most $n\phi_2(n)$.

It we multiply the set on the right by W, the product has the same form as (h). Applying V as a right-hand multiplier, the product of any element of the set by V is an element of the set if

$$W^{(c+dx)/(a+bx)}R_{a+bx}V^{-1}W^{-b/(a+bx)}VW^{-x}V = W^{(d-cy)/(b-ay)}R_{b-ay}V^{-1}W^{a/(b-ay)}VW^{-y},$$

where $b-ay$ is prime to n. This condition may be reduced to (c′) by means of (c) and the fact that x and y may be chosen so that $a+bx$, $b-ay$, and $1+xy$ are each relatively prime to n. Hence $g = n\phi_2(n)$ and the theorem is proved.

THE UNIVERSITY OF ALABAMA