ISOMORPHIC CONGRUENCE GROUPS AND HECKE OPERATORS

by R. A. RANKIN

(Received 15 October, 1965)

Let G, H, K be groups such that G is normal in K and $G \subseteq H \subseteq K$. Let $I(H, K)$ be the set of inner automorphisms of K restricted to H; thus $\alpha \in I(H, K)$ if and only if, for some $k \in K$, $\alpha(h) = k^{-1}hk$ for all $h \in H$. Let ϕ be an isomorphism of H/G onto a subgroup $H^{(\phi)}/G$ of K/G. An isomorphism Φ of H onto $H^{(\phi)}$ is called an extension of ϕ if

$$\Phi(h)G = \phi(hG) \quad \text{for all} \quad h \in H.$$

Such an extension need not exist in general, nor need the groups H and $H^{(\phi)}$ be isomorphic.

Suppose that such an extension Φ does exist and that $\Phi \in I(H, K)$, so that, as above, $\Phi(h) = k^{-1}hk$. Since $\phi(hG) = \Phi(h)G = k^{-1}hkG = k^{-1}hGk$, it follows that $\phi \in I(H/G, K/G)$.

Let N be a positive integer and put

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad U = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \qquad T = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

Let Ω and Ω_N be the sets of all matrices T with entries in Z, the ring of all integers, and Z_N, the ring of residues modulo N, respectively. Put

$$\Gamma^*(1) = \{T : T \in \Omega, \det T = \pm 1\}, \qquad \Gamma(1) = \{T : T \in \Omega, \det T = 1\},$$
$$\Gamma(N) = \{T : T \in \Gamma(1), T \equiv I \pmod N\}, \qquad K_N = \{T : T \in \Omega_N, (\det T, N) = 1\}.$$

Then K_N contains normal subgroups $G_N \sim \Gamma(1)/\Gamma(N)$, $G_N^* \sim \Gamma^*(1)/\Gamma(N)$ arising from the natural homomorphism $\omega : \Omega \to \Omega_N$.

Let Γ be a subgroup of $\Gamma^*(1)$ containing $\Gamma(N)$, and put $H_N = \omega(\Gamma) \sim \Gamma/\Gamma(N)$. In the theory of Hecke T_n-operators (see my forthcoming paper in *Math. Annalen*) one encounters isomorphisms $\phi \in I(H_N, K_N)$, where $\phi(h) = k^{-1}hk$ for some $k \in K_N$ and all $h \in H_N$, and $\det k = n$ with $(n, N) = 1$. It is of interest to know for what residues n modulo N the isomorphism ϕ has an extension $\Phi \in I(\Gamma, \Gamma^*(1))$. The above remarks show that this can occur only if $\phi \in I(H_N, G_N^*)$, so that we must have $k^{-1}hk = g^{-1}hg$ for some $g \in G_N^*$ and all $h \in H_N$.

A case of particular interest arises when $L^{-1}U^rL \in \Gamma$ for some positive divisor r of $N (r < N)$ and some $L \in \Gamma(1)$. Then, for some $T \in \Omega$ with $\det T = n$ (or $-n$), we must have $T^{-1}U^rT \equiv U^r \pmod N$. It follows easily from this that n (or $-n$) must be congruent to a square modulo N/r.

As a kind of converse of this we show that, if $n \equiv v^2$ or $-n \equiv v^2 \pmod N$, then ϕ always has an extension $\Phi \in I(\Gamma, \Gamma^*(1))$. For we can take $A \in \Omega$ such that $\omega(A) = k$, and we then put $\Phi(S) = A_n^{-1}SA_n$ $(S \in \Gamma)$, where $A_n \in \Gamma^*(1)$ and $vA_n \equiv A \pmod N$. In particular, this is possible for every n prime to N, when $N = 1, 2, 4, p$ or $2p$, where p is a prime and $p \equiv 3 \pmod 4$. [This paper arises from an editorial observation that $167 \equiv 3 \pmod 4$.]

If we demand that $\Phi \in I(\Gamma, \Gamma(1))$, similar arguments apply, except that references to $-n$ are to be omitted.

UNIVERSITY OF GLASGOW
GLASGOW, W. 2