NORMAL SUBGROUPS OF THE UNIMODULAR GROUP

BY
IRVING REINER

1. Introduction

Let Γ denote the proper unimodular group consisting of all 2×2 matrices with rational integral elements and determinant $+1$. For m a positive integer, define the principal congruence group $\Gamma(m)$ by

$$\Gamma(m) = \{X \in \Gamma : X \equiv I \pmod{m}\}, \tag{1}$$

where I denotes the identity matrix in Γ, and where congruence of matrices is interpreted as elementwise congruence. It is easily seen that the index $(\Gamma : \Gamma(m))$ is finite, and that $\Gamma(m)$ is a normal subgroup of Γ. Therefore, any normal subgroup of Γ which contains $\Gamma(m)$ for some m must be of finite index in Γ.

It was conjectured that, conversely, every normal subgroup of Γ of finite index must contain a principal congruence group $\Gamma(m)$ for some m. In 1887 this conjecture was disproved by R. Fricke [3] and G. Pick [4]. In this note we shall simplify their proofs of the falsity of the conjecture, and shall give a larger class of counterexamples.

The author wishes to thank Professor R. Baer for his helpful suggestions

2. A class of normal subgroups

For p a prime, we know from the results of H. Frasch [2] that $\Gamma(p)$ is a finitely-generated free group. If we let $\Gamma'(p)$ denote the commutator subgroup of $\Gamma(p)$, it then follows that $\Delta(p) = \Gamma(p)/\Gamma'(p)$ is a finitely-generated free abelian group. Therefore $\Delta(p)/\Delta^s(p)$ is finite, where $\Delta^s(p)$ is the subgroup of $\Delta(p)$ generated by

$$\{X^s : X \in \Delta(p)\}.$$

Let $\Omega(p, s)$ be the inverse image of $\Delta^s(p)$ under the canonical mapping of $\Gamma(p)$ onto $\Delta(p)$. Since $\Delta^s(p)$ is a normal subgroup of $\Delta(p)$, we see that $\Omega(p, s)$ is a normal subgroup of $\Gamma(p)$, and in fact

$$\Gamma(p)/\Omega(p, s) \cong \Delta(p)/\Delta^s(p).$$

Therefore $\Omega(p, s)$ is the subgroup of $\Gamma(p)$ generated by $\Gamma'(p)$ and $\{X^s : X \in \Gamma(p)\}$, and is of finite index in Γ. Since $\Gamma(p)$ is a normal subgroup of Γ, and $\Omega(p, s)$ is a characteristic subgroup of $\Gamma(p)$, it follows that $\Omega(p, s)$ is a normal subgroup of Γ. The groups $\Omega(p, s)$ give an infinite set of normal subgroups of Γ of finite index in Γ.

Received April 8, 1957; received in revised form July 27, 1957.

3. Subgroups of $\Omega(p, s)$

Hereafter we assume that $s > 1$ and $(s, p) = 1$. We shall prove that $\Omega(p, s)$ cannot contain any principal congruence group. Suppose to the contrary that for some k we have $\Gamma(k) \subset \Omega(p, s)$. Since $\Gamma(ak) \subset \Gamma(k)$ for any positive integer a, we may assume that

$$\Gamma(p^r st) \subset \Omega(p, s), \tag{2}$$

where r is a non-negative integer, and $(t, p) = 1$.

Set

$$T = \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix}, \qquad U = \begin{pmatrix} 1 & 0 \\ p & 1 \end{pmatrix}. \tag{3}$$

Let q be an integer to be determined in a moment, and set

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = U^q T U T^{st-1}.$$

Then we have

$$b/p = p^2(st - 1) + st, \qquad (d - 1)/p^2 = q(b/p) + st - 1. \tag{4}$$

Therefore $(b/p, pst) = 1$, and so we may choose q so that $(d - 1)/p^2 \equiv 0 \pmod{p^r st}$. With this choice of q, we have $d \equiv 1 \pmod{p^r st}$. Since $ad - bc = 1$, this shows that $a \equiv 1 + bc \pmod{p^r st}$.

The above congruences imply

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 + bc & b \\ c & 1 \end{pmatrix} = B \pmod{p^r st}.$$

Therefore $AB^{-1} \in \Gamma(p^r st)$, and so assuming (2) we deduce that $AB^{-1} \in \Omega(p, s)$. Now $B = T^{b/p} U^{c/p}$, whence

$$AB^{-1} = U^q T U T^{st-1} U^{-c/p} T^{-b/p}. \tag{5}$$

We shall show below that if a power product of T and U lies in $\Omega(p, s)$, then the sum of the exponents to which T occurs must be a multiple of s. Using this, we deduce from $AB^{-1} \in \Omega(p, s)$ that

$$1 + (st - 1) - b/p \equiv 0 \pmod{s}.$$

If we substitute for b/p the expression given in (4), this becomes

$$st - p^2(st - 1) + st \equiv 0 \pmod{s},$$

which is impossible since $(p, s) = 1$. This gives a contradiction, and hence $\Omega(p, s)$ cannot contain a principal congruence group.

We now consider the group $\Gamma(p)$. According to the results of H. Frasch [2], the group $\Gamma(p)$ has a set $\mathcal{S}$ of free generators consisting of T and a collection of generators of the form (λ, μ, ν) (in Frasch's notation). Using his equation (19a), we find that $U = (0, 1, 1)^{-1}$. Frasch's elimination procedure shows that either $(0, 1, 1)$ is one of the free generators, or else it can be expressed in terms of the free generators other than T. Therefore when U is expressed as a power product of elements of $\mathcal{S}$, the generator T does not appear as a factor.[1]

On the other hand, we may characterize $\Gamma'(p)$ in terms of the free generators in $\mathcal{S}$; namely, $\Gamma'(p)$ consists of all power products of the generators in $\mathcal{S}$ for which the exponent sum for each generator is zero. Therefore $\Omega(p, s)$ consists of all power products of the generators in $\mathcal{S}$ for which the exponent sum for each generator is a multiple of s. It follows at once that if a power product of T and U lies in $\Omega(p, s)$, the exponent sum for T must be a multiple of s. This completes the proof.

Remarks.

(i) In the papers of Fricke and Pick, only the groups $\Omega(2, s)$ are given.

(ii) The corresponding conjecture for the $n \times n$ proper unimodular group is as yet unsettled for $n > 2$.

REFERENCES

1. J. L. BRENNER, *Quelques groupes libres de matrices*, C. R. Acad. Sci. Paris, vol. 241 (1955), pp. 1689–1691.
2. H. FRASCH, *Die Erzeugenden der Hauptkongruenzgruppen für Primzahlstufen*, Math. Ann., vol. 108 (1933), pp. 229–252.
3. R. FRICKE, *Ueber die Substitutionsgruppen, welche zu den aus dem Legendre'schen Integralmodul $k^2(\omega)$ gezogenen Wurzeln gehören*, Math. Ann., vol. 28 (1887), pp. 99–118.
4. G. PICK, *Ueber gewisse ganzzahlige lineare Substitutionen, welche sich nicht durch algebraische Congruenzen erklären lassen*, Math. Ann., vol. 28 (1887), pp. 119–124.

UNIVERSITY OF ILLINOIS
URBANA, ILLINOIS

[1] This fact implies the result of J. L. Brenner [1] that T and U generate a free group.