BULL. AUSTRAL. MATH. SOC. MOS 20K30, 20K20, 20H05, 20H25

VOL. 4 (1971), 321-342.

On an infinite integral linear group

I. H. Farouqi

This paper investigates the normal subgroup structure of the automorphism group Γ of a free abelian group A of countably infinite rank. The finitary automorphisms, that is those acting non-trivially only on a direct summand of A of finite rank, form a normal subgroup Φ of Γ ; the sublattice of all normal subgroups of Γ contained in Φ is in fact the sublattice of normal subgroups of Φ and has a quite transparent structure. By contrast there is a profusion of normal subgroups of Γ not contained in Φ . For example, the collection of certain types of these normal subgroups, defined as generalizations of the congruence subgroups of finite dimensional integral linear groups, if partially ordered by inclusion, can be shown to contain infinitely many chains of the order type of the continuum.

0. Introduction

Let A be a free abelian group of countably infinite rank and let Γ be the group of automorphisms of A . In this paper we present some results on the normal subgroups of Γ . The normal subgroups of Γ that we introduce here are defined in terms of direct decompositions of A or infinite descending chains of subgroups of A . To begin with, we define finitary automorphisms of A as those which are the identity on a direct summand of finite codimension. Finitary automorphisms form a normal

Received 19 November 1970. Communicated by Hanna Neumann. This paper is extracted from the author's Ph.D. thesis, submitted to the Australian National University in June 1969. The author is most grateful to Professor Hanna Neumann and to Professor B.H. Neumann for their kind help and encouragement during the preparation of this paper.

subgroup Φ of Γ. It contains, as its subgroups, isomorphic copies of finite dimensional integral linear groups which enables us to find the normal subgroups of Φ by using the results of Brenner [1] and Mennicke [5] on unimodular groups. Congruence subgroups of the finite dimensional unimodular groups have their analogue here; a congruence subgroup of Γ is a normal subgroup of Γ which consists of those automorphisms γ such that $\gamma - 1$ maps every element of A into the characteristic subgroup mA of A. The intersections of Φ with the congruence subgroups turn out to be essentially the only normal subgroups of Φ and consequently all normal subgroups of Φ are normal in Γ also. Φ also has the property that, modulo the centre of Γ, it intersects every other normal subgroup of Γ non-trivially.

The last two sections of this paper are devoted to normal subgroups defined in terms of infinite descending chains of subgroups of A. We show that the class of such normal subgroups is uncountable, and moreover, each normal subgroup of this kind contains infinitely many chains of normal subgroups of Γ, each chain being of the order type of the reals. This 'density' of the normal subgroup structure of Γ is in strong contrast to known results that apply to apparently similar situations.

Rosenberg [6] has studied the group of automorphisms of a vector space of infinite dimension over a division ring. In the case when the vector space has countable dimension, the finitary invertible linear transformations form a unique maximal normal subgroup modulo the centre. Another example of this kind is provided by [7] where it is shown that in a symmetric group of countable degree the finitary permutations form a unique maximal normal subgroup.

The large number of normal subgroups outside the subgroup of finitary automorphisms that we exhibit have no analogue either in the finite dimensional integral linear groups. Their existence is due to the combination of the divisibility properties of the integers and the scope provided by an infinite dimensional structure. Recently, Maxwell [4] has studied a more general system, namely the units of the ring of endomorphisms of an infinite type free module over a commutative ring. He considers the automorphisms which are the identity on a direct summand (of any codimension) and are transvections (see [6]). Thus, what Maxwell deals with is a set related to, but different from the set of finitary automorphisms.

1. Notation and terminology

The following notation will be used in the whole paper.

A :	a free abelian group of countably infinite rank.
Γ :	the group of automorphisms of A .
Z, Z^{+} :	the set of all integers, and of all positive integers, respectively.
$r(H)$, $r(A/H)$:	the rank of a subgroup H , or of a free abelian factor group A/H , of A .
codim(H) :	the rank of a complement of H , H being a direct summand of A .
I, I_n :	an identity matrix of infinite dimension, or of dimension n respectively.
A :	a matrix whose (i, j)-th coefficient, that is, the coefficient in its i-th row and j-th column, is a_{ij} . We shall also write $\mathrm{A}_{m\times n}$ when the shape of A is to be mentioned explicitly.
α^{Γ} :	the normal closure of the automorphism α in Γ ; as usual, we write α^{β} for $\beta^{-1}\alpha\beta$.
$\langle x_1, \ldots, x_n\rangle$:	the subgroup generated by $x_1, \ldots, x_n$.
$\langle X\rangle$:	the subgroup generated by the subset X .
$\mathrm{GL}_n[Z]$:	the general linear group consisting of all $(n\times n)$-matrices with integral coefficients and determinants equal to ± 1 .
$\mathrm{SL}_n[Z]$:	the special linear group consisting of all those elements of $\mathrm{GL}_n[Z]$ of determinant equal to $+1$.
g.c.d. :	abbreviation for "greatest common divisor"; but for two

integers m, n we write usually (m, n) for g.c.d.$\{m, n\}$.

2. Results on free abelian groups

This section contains some properties of free abelian groups of countably infinite rank that will be used subsequently. Most of them are known; we give references or proofs as needed.

2.1. *H is a direct summand of A if and only if A/H is free abelian.*

Hence, as subgroups of A are free, we have

2.1.1. *The kernel of an endomorphism of A is a direct summand.*

2.2 ([3], Example 51c). *The intersection of any number of direct summands of A is a direct summand of A .*

2.2.1. *Let H be a subgroup of A . There is a unique least direct summand B of A containing H ; B and H have the same rank.*

2.3. *Let again $H \leq A$ and let B be the least direct summand of A containing H . If an automorphism $\gamma \in \Gamma$ maps H onto itself then it maps B onto itself.*

Proof. The direct summand B may be obtained as the intersection of all direct summands of A that contain H . As $H\gamma = H$, γ induces a permutation on the set of all these direct summands and so maps their intersection onto itself.

2.4. *Let K_1 and K_2 be direct summands of A , both of finite codimension (that is, a complement has finite rank). Then $K_1 \cap K_2$ also has finite codimension.*

2.5 ([2], §2). *If H is a direct summand of A and the subgroup B of A contains H , then H is a direct summand of B .*

Hence, easily

2.6. *Let $A = H \oplus K$ and let B be another direct summand of A containing H . Then we can write $A = B \oplus C$ where $C \leq K$.*

Proof. Consider $B \cap K$ which is a direct summand of A , hence of K . Thus we have $K = (B \cap K) \oplus C$ for some C , and now

https://doi.org/10.1017/S0004972700046670 Published online by Cambridge University Press

$A = H \oplus (B \cap K) \oplus C = B \oplus C$.

3. The finitary automorphisms and the congruence subgroups

Finitary automorphisms of A have been defined in the introduction as those automorphisms which are the identity on some direct summand of A which is of finite codimension. The following theorem gives several characterizations of such an automorphism.

THEOREM 3.1. *Let* $\varphi \in \Gamma$ *be an automorphism of* A . *The following properties of* φ *are equivalent:*

(i) *the endomorphism* $\rho = \varphi - \iota$, *where* ι *is the identity on* A , *has image* $A\rho$ *of finite rank;*

(ii) φ *maps a direct summand of* A *of finite codimension identically onto itself;*

(iii) *there exists a basis* $\left\{x_i \mid i \in Z^+\right\}$ *for* A *and a positive integer* n *such that* $x_i\varphi = x_i$ *for all* $i > n$;

(iv) *there exists a direct decomposition of* A , $A = H \oplus K$ *say, such that* H *is of finite rank,* $H\varphi = H$, *and* φ *is the identity on* K .

Proof. *(i)* $\Rightarrow$ *(ii)*. Let $\rho = \varphi - \iota$ and assume that $A\rho$ has finite rank. Since ρ is an endomorphism of A , $\ker\rho$ is a direct summand of A . Then $\ker\rho$ is mapped identically onto itself by φ ; and $\ker\rho$ has finite codimension, since $A/\ker\rho \cong A\rho$.

The equivalence *(ii)* $\Leftrightarrow$ *(iii)* is obvious, and so is the implication *(iv)* $\Rightarrow$ *(i)*.

We only show now that *(ii)* implies *(iv)*. We have $A = H \oplus K$ with φ being the identity on K and H of finite rank. Set $H^* = \langle H \cup H\varphi \rangle$. Then H^* has finite rank and moreover $H^*\varphi = H^*$. To see this, note that $H^*\varphi = \langle H\varphi \cup H\varphi^2 \rangle$; but for $h \in H$, $h\varphi = h' + k$ uniquely (where $h' \in H$, $k \in K$), and now $h\varphi^2 = h'\varphi + k \in H^*$ as $k = h\varphi - h' \in H^*$. Now let B be the least direct summand of A containing H^* . B has finite rank and we can write $A = B \oplus C$ where $C \leq K$ so that C is mapped identically onto itself by φ .

https://doi.org/10.1017/S0004972700046670 Published online by Cambridge University Press

From now on, we shall use these equivalent characterizations of a finitary automorphism without further reference. For a finitary automorphism φ of A we shall say that $A = H \oplus K$ is a decomposition of A with respect to φ, or corresponding to φ, if and only if $H\varphi = H$, φ restricted to K is the identity on K and H has finite rank. Again, we call a basis $X = \{x_i \mid i \in Z^+\}$ a basis of A with respect to φ, or corresponding to φ, if $x_i\varphi = \sum_{j=1}^{n} a_{ij}x_j$, $1 \le i \le n$ for some $n \in Z^+$ and $x_i\varphi = x_i$ for $i > n$; the matrix A representing φ in this basis is of the form $A_{n\times n} \dot{+} I$ where I is the infinite identity matrix. It is often convenient to look upon φ as represented by the matrix $A_{n\times n}$.

THEOREM 3.2. *The subset* Φ *of* Γ *consisting of all finitary automorphisms of* A *is a normal subgroup of* Γ.

Proof. Let $\alpha, \beta \in \Phi$ and suppose that $A = H_1 \oplus K_1 = H_2 \oplus K_2$ are two decompositions of A corresponding to α and β respectively. By 2.4 $K_1 \cap K_2$ is a direct summand of A and has finite codimension. Clearly, $\alpha\beta$ maps $K_1 \cap K_2$ identically onto itself. Hence by Theorem 3.1 $\alpha\beta$ is finitary. Then, α^{-1} is the identity on K_1 and so α^{-1} also is finitary. Finally, let $\gamma \in \Gamma$. Then $A = H_1\gamma \oplus K_1\gamma$ and $\gamma^{-1}\alpha\gamma$ is the identity on $K_1\gamma$ where $K_1\gamma$ has finite codimension. Thus $\gamma^{-1}\alpha\gamma$ is also finitary and Φ is a normal subgroup of Γ.

We close this section by giving the definitions of congruence subgroups of Γ. For each positive integer m we define the subset $\Gamma(m)$ of Γ to consist of all elements $\alpha \in \Gamma$ such that $x\alpha - x \in mA$ for all $x \in A$. Then $\Gamma(m)$ is a normal subgroup of Γ. This becomes clear at once if one writes $x\alpha\alpha' - x = (x\alpha - x)\alpha' - (x\alpha' - x)$ and $x\gamma^{-1}\alpha\gamma - x = \left(x\gamma^{-1}\alpha - x\gamma^{-1}\right)\gamma$ and observes that mA is characteristic in A. These subgroups $\Gamma(m)$ are called congruence subgroups of Γ; of course $\Gamma(1) = \Gamma$.

4. Finitary normal subgroups

In this section we determine all the normal subgroups of Φ. Each of these normal subgroups of Φ is normal in Γ also; we call these the finitary normal subgroups of Γ. We first define one normal subgroup of Φ by means of the "determinant" of a finitary automorphism. Let $\varphi \in \Phi$ and let $X = \left\{x_i \mid i \in Z^+\right\}$ be a basis of A with respect to φ so that $x_i\varphi = \sum_{j=1}^{n} c_{ij}x_j$, $1 \le i, j \le n$, $x_i\varphi = x_i$ for $i > n$, n being some positive integer. As we have pointed out in Section 3, φ can be represented by the matrix $C_{n\times n}$ with coefficients c_{ij}. Since φ maps $\langle x_1, x_2, \ldots, x_n\rangle$ onto itself and C has integral coefficients, $\det C = \pm 1$. The same automorphism φ can also be represented by some other finite matrix say, E, with respect to some other basis of A. We now show that $\det C = \det E$, so that the determinant of a finitary matrix representing an element of Φ is independent of the choice of a basis of A to which C corresponds.

LEMMA 4.1. *Let* α, β *be two elements of* Φ *and let* $A = H \oplus K = H' \oplus K'$ *be two decompositions of* A *corresponding to* α *and* β *respectively. Then we can write* $A = L \oplus M$ *where* $M \le K \cap K'$ *and* $L\alpha = L\beta = L$, L *has finite rank and contains both* H *and* H'.

Proof. By 2.4 $K \cap K'$ is a direct summand of A, and has finite codimension; and by 2.5 $K \cap K'$ is a direct summand in both K and K'. Thus we can write $A = H \oplus K_1' \oplus K \cap K' = H' \oplus K_2' \oplus K \cap K'$, where $K_1' < K$, $K_2' < K'$ and both K_1' and K_2' have finite rank. Let $H^* = \langle H \cup H' \cup K_1' \cup K_2'\rangle$, then H^* has finite rank. Also, $H^*\alpha = H^*\beta = H^*$; for, let $h^* \in H^*$. Then $h^* = h + k$, $h \in H$, $k \in K$ and $h^*\alpha = h\alpha + k\alpha = h\alpha + k$. Now $k = h^* - h \in H^*$ and $h\alpha \in H$ gives that $h^*\alpha \in H^*$. Thus $H^*\alpha = H^*$. Similarly $H^*\beta = H^*$, so that H^* is invariant under both α and β. It follows from 2.2.1 that there is a least direct summand L of A containing H^*, and L has finite rank. By 2.3 $L\alpha = L\beta = L$. Finally, by 2.6 we get $A = L \oplus M$, M contained in $K \cap K'$, as a decomposition of A with the required properties.

LEMMA 4.2. *If* φ *is represented by two finite matrices* A *and* B

https://doi.org/10.1017/S0004972700046670 Published online by Cambridge University Press

with respect to different bases, then $\det A = \det B$.

Proof. Let φ be represented by the matrices $A_{m\times m}$ and $B_{n\times n}$ corresponding to the bases $X = \left\{x_i \mid i \in Z^+\right\}$ and $X' = \left\{x_i' \mid i \in Z^+\right\}$ respectively. Then we can write $A = H \oplus K = H' \oplus K'$ where $H = \langle x_i \mid 1 \le i \le m\rangle$, $K = \langle x_i \mid i > m\rangle$, $H' = \langle x_i' \mid 1 \le i \le n\rangle$, $K' = \langle x_i' \mid i > n\rangle$, $H\varphi = H$, $H'\varphi = H'$, and φ is the identity on both K and K' . By Lemma 4.1 we can write $A = L \oplus M$ where L contains both H and H' , $L\varphi = L$ and M is contained in $K \cap K'$. Also both H and H' are direct summands in L and we can write $L = H \oplus K_1 = H' \oplus K_2$ where $K_1 < K$ and $K_2 < K'$. Thus if r is the rank of L , we can choose two bases of L as $Y = \{x_i, y_j \mid i = 1, 2, \ldots, m , j = 1, 2, \ldots, r-m\}$ and $Y' = \{x_i', y_j' \mid i = 1, 2, \ldots, n , j = 1, 2, \ldots, r-n\}$. Corresponding to these bases, φ will be represented by the matrices $A' = A_{m\times m} \dot{+} I_{r-m}$ and $B' = B_{n\times n} \dot{+} I_{r-n}$ respectively, where we have of course, $\det A' = \det A$ and $\det B' = \det B$. But now the matrices A' and B' represent the same automorphism of the free abelian group L of finite rank; hence A' and B' are conjugate, $B' = T^{-1}A'T$ for some invertible $(r\times r)$-matrix T , and so $\det A' = \det B'$, that is $\det A = \det B$.

Now we may speak of *the* determinant of a finitary automorphism, and an argument similar to the one just presented shows that $\det(\alpha\beta) = \det\alpha\det\beta$ whenever α and β are finitary. Thus we obtain:

THEOREM 4.3. *The finitary automorphisms with determinant* $+1$ *form a maximal normal subgroup,* Φ^+ *say, of* Φ . *Moreover* Φ^+ *is normal in* Γ .

Proof. Only the last part still needs proof. But if $\alpha \in \Phi$ and if X is a basis of A corresponding to α , then $X\gamma$ is a basis corresponding to $\gamma^{-1}\alpha\gamma$ for any $\gamma \in \Gamma$, and the matrix representing α with respect to the basis X also represents $\gamma^{-1}\alpha\gamma$ with respect to the basis $X\gamma$. Hence $\det\alpha = \det(\gamma^{-1}\alpha\gamma)$ for all $\gamma \in \Gamma$, which completes the proof.

The rest of this section is devoted to showing that the normal subgroups $\Phi(m) = \Phi \cap \Gamma(m)$ for all $m \in Z^+$, Φ^+ and $\Gamma(2) \cap \Phi^+$ are in fact the only normal subgroups of Φ , and therefore also the only normal subgroups of Γ contained in Φ . We also describe the lattice formed by these subgroups.

We shall write $I + me_{ij}$ for a square matrix (of any degree) which has diagonal entries equal to 1 , the entry in the place (i, j) with $i \neq j$ equal to m , all other entries zero.

LEMMA 4.4 ([1]). *Let $C \in GL_n[Z]$, $n > 2$ and let the greatest common divisor of the set $\{c_{ii}-c_{jj}, c_{ij} \mid i \neq j\}$ be m . The least normal subgroup of $GL_n[Z]$ (or of $SL_n[Z]$ if $\det C = 1$) containing C contains the matrix $I + me_{12}$.*

In fact such a normal subgroup of $GL_n[Z]$, or of $SL_n[Z]$, then contains all the matrices of the type $I + me_{ij}$, $i \neq j$. Moreover one has the following fact.

LEMMA 4.5 ([5]). *For $n > 2$ the least normal subgroup of $SL_n[Z]$ containing $I + me_{21}$ is the normal subgroup consisting of all matrices which are congruent to the identity matrix modulo m .*

THEOREM 4.6.

(i) If $m > 2$, $\Phi(m) = \Phi \cap \Gamma(m) \leq \Phi^+$;

(ii) the groups $\Phi(m)$ for all m , Φ^+ and $\Phi(2)^+ = \Phi(2) \cap \Phi^+$ are the only normal subgroups of Φ ;

(iii) $\Phi(p)$ and $\Phi(2)^+$ are precisely all the maximal normal subgroups of Φ^+ , where p ranges over the odd primes ;

(iv) Φ^+ and $\Phi(2)$ are the only two maximal normal subgroups of Φ .

Proof. *(i)* Let $\varphi \in \Phi(m)$, $m > 2$. Let the finite matrix A represent φ. As $A - I \equiv 0 \mod m$, the g.c.d.$\{a_{ii}-1, a_{ij} \mid i \neq j\} = k$ is greater than 2, and $\det A \equiv 1 \mod k$. Moreover $\det A$ cannot be -1 since $k > 2$; consequently $\det\varphi$ can only be $+1$, whence $\Phi(m) \leq \Phi^+$.

(ii) First we show that if $\varphi \in \Phi(m)$, $m \geq 1$, but $\varphi \notin \Phi(n)$ for $n > m$ then $\varphi^\Phi \geq \Phi(m) \cap \Phi^+$. Let $\mu \in \Phi(m) \cap \Phi^+$. Then there is a decomposition $A = L \oplus M$ such that both φ and μ are the identity on M and map L onto itself, and L has finite rank. We can assume that $r(L) = l$ is sufficiently large so that there is a basis X_1 of L such that at least one element of X_1 is mapped onto itself by φ. Let $A_{l\times l}$ and $B_{l\times l}$ be two matrices representing φ and μ respectively corresponding to X_1. By the definition of φ, $A \equiv I \mod m$ and m is the greatest such integer. Since at least one diagonal element of A is equal to 1, A satisfies the assumptions of Lemma 4.4. Therefore, by Lemmas 4.4 and 4.5, the normal closure of A in $GL_n[Z]$ contains B which implies that φ^Φ contains μ.

It follows from this that if $\varphi \in \Phi(m)$, $m > 2$ and $\varphi \notin \Phi(n)$, $n > m$, then $\varphi^\Phi = \Phi(m)$. Similarly, if $\varphi \in \Phi^+$ and is not in any proper normal subgroup of Φ^+ then $\varphi^\Phi = \varphi^{\Phi^+} = \Phi^+$; and likewise if φ is in Φ but not in any proper normal subgroup of Φ then $\varphi^\Phi = \Phi$. And lastly if $\varphi \in \Phi(2)^+$ and $\Phi(2)^+$ is the smallest normal subgroup of Φ with this property, then $\varphi^\Phi = \Phi(2)^+$. A similar result holds if we replace $\Phi(2)^+$ by $\Phi(2)$.

Now for every φ in Φ there is a greatest integer m such that $\varphi \in \Phi(m)$. Hence the above arguments allow us to deduce that the only proper normal subgroups of Φ are Φ^+, $\Phi(2)$, $\Phi(2)^+ = \Phi(2) \cap \Phi^+$ and $\Phi(m)$, $m > 2$.

(iii) Consider the least normal subgroup of Φ^+ containing $\Phi(p)$, p being an odd prime, and an element μ which is not in $\Phi(p)$. Then

μ^{Φ^+} contains an element ψ which can with respect to a suitable basis X of A be represented by the matrix $I + me_{ij}$, where m is not divisible by p . Let φ be the automorphism represented by the matrix $I + pe_{ij}$ in the basis X ; then $\varphi \in \Phi(p)$. Since $(p, m) = 1$, there exist integers r, s such that $pr + ms = 1$ and so $\varphi^r\psi^s$ is represented by the matrix $I + (pr+ms)e_{ij} = I + e_{ij}$. But then the normal closure of $\varphi^r\psi^s$ in Φ^+ is the whole of Φ^+ by *(ii)* above, whence $\Phi(p)$ is maximal normal in Φ^+ . The case of $\Phi(2)^+$ can be dealt with likewise. That $\Phi(2)^+$ and $\Phi(p)$ are the only maximal normal subgroups of Φ^+ follows from the fact that $\Phi(m) \geq \Phi(n)$ if and only if m divides n .

(iv) We have already shown in Theorem 4.3 that Φ^+ is maximal normal in Φ . As regards $\Phi(2)$, the same arguments as in the proof of *(iii)* above show that if $\mu \notin \Phi(2)$ then the least normal subgroup Θ of Φ containing both $\Phi(2)$ and μ contains Φ^+ . But $\Phi(2)$ also contains elements having determinant -1 , and that makes $\Theta = \Phi$.

COROLLARY 4.7. *Every normal subgroup of* Φ *is the normal closure of a single element of* Φ .

We conclude this section by pointing out that if m and n are two integers greater than 2 then $\Phi(m) \cap \Phi(n) = \Phi(r)$ where r is the least common multiple of m and n , and $\Phi(m).\Phi(n) = \Phi(s)$ where s is the greatest common divisor of m and n . When $m = 2$, some distinction of cases is necessary. For instance, for any odd prime p , $\Phi(2) \cap \Phi(p) = \Phi(2p) = \Phi(2)^+ \cap \Phi(p)$ but $\Phi(2).\Phi(p) = \Phi$ while $\Phi(2)^+.\Phi(p) = \Phi^+$. These remarks suffice to get a picture of the lattice formed by the normal subgroups of Φ .

5. An intersection property

As we have mentioned in the introduction, Φ has got the property that, modulo the centre, it intersects every normal subgroup of Γ non-trivially. We give a proof of this fact here. Moreover, any

https://doi.org/10.1017/S0004972700046670 Published online by Cambridge University Press

prescribed normal subgroup of Φ can be obtained as the intersection of Φ with some normal subgroup of Γ as will be indicated at the end of this section by an example.

THEOREM 5.1. *Φ intersects every other normal subgroup of Γ non-trivially modulo the centre of Γ.*

Proof.*) We first point out that the centralizer of Φ in Γ is just the centre $Z(\Gamma) = \langle -1 \rangle$ of Γ, where -1 is the automorphism of A that maps every element of A onto its inverse. Let Θ be another normal subgroup of Γ not contained in Φ. If $\Theta \cap \Phi = \{\iota\}$, then every element of Φ commutes with every element of Θ so that Θ is contained in the centralizer of Φ. Hence Θ is contained in the centre of Γ. The theorem follows.

The following example also is due to Professor B.H. Neumann.

LEMMA 5.2. *There exists an automorphism $\alpha \in \Gamma$ which is not finitary, but the intersection $\alpha^{\Gamma} \cap \Phi$ contains an automorphism of determinant -1.*

Proof. Consider the integral matrix

$$W = \begin{bmatrix} 1 & 0 & 0 \\ 0 & w & 0 \\ 0 & 0 & w^2 \end{bmatrix},$$

where 1 and 0 are to be interpreted as the corresponding 2×2-matrices, and $w = \begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix}$, so that $w^3 = 1$ and $w^2 + w + 1 = 0$. Thus W is of degree 6 and determinant 1. Now take

$$Q = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

with the same interpretation of 0 and 1 so that

$$W + W^{Q} + W^{Q^2} = 0 \quad (\text{where } X^{Y} = Y^{-1}XY) .$$

*) This simple proof is due to Professor B.H. Neumann. It replaces our proof which was based on Brenner's [1] arguments.

Next put

$$P = \begin{bmatrix} 0 & W \\ 0 & 0 \end{bmatrix} \quad \text{and} \quad T = \begin{bmatrix} Q & 0 \\ 0 & Q \end{bmatrix}$$

where 0 is the zero matrix of degree 6. Then one checks that

$$P + P^T + P^{T^2} = PP^T + P^TP^{T^2} + PP^{T^2} = PP^TP^{T^2} = 0$$

hence

$$(5.2.1) \qquad (I+2P)\left(I+2P^T\right)\left(I+2P^{T^2}\right) = I .$$

Now define the infinite invertible matrix A by

$$A = D \dotplus \sum_{i \in Z^+} \dotplus P_i ,$$

where $P_i = I + 2P$ for all i, D is any invertible matrix of finite degree which in this example is chosen so that $D \equiv I \bmod 2$ and $\det D = -1$. Then for every integer $s > 2$ one has $D \not\equiv I \bmod s$. Now A represents, with respect to some fixed basis, an automorphism, α say, which belongs to $\Gamma(2)$, but not to $\Gamma(s)$ when $s > 2$, and α is not finitary. Let $C = E \dotplus \sum_{i \in Z^+} \dotplus T_i$, where $T_i = T$ for all i and E is any invertible matrix of the same size as D, and let γ be the automorphism represented by C in the same basis. Then $\alpha\alpha^\gamma\alpha^{\gamma^2}$ can be represented by the product $AA^CA^{C^2} = DD^ED^{E^2} \dotplus I$ where I is the infinite identity matrix because of (5.2.1). Thus $\beta = \alpha\alpha^\gamma\alpha^{\gamma^2}$ is finitary and it clearly has determinant -1, because D has determinant -1.

This completes the proof of the lemma.

It is now easy to see, and will merely be stated, that in fact $\alpha^\Gamma \cap \Phi = \Phi(2)$, that by using the freedom of choice left in D and E, α can be so chosen that the intersection is the whole of Φ, and that a similar construction will produce non-finitary elements of Γ whose normal closure intersects Φ precisely in Φ^+, $\Phi(2)^+$ or $\Phi(m)$ for

https://doi.org/10.1017/S0004972700046670 Published online by Cambridge University Press

every $m > 2$.

6. A first generalization of congruence subgroups

We introduce now those normal subgroups which contain the congruence subgroups of Γ lying in Φ , that is, the subgroups $\Phi(m)$, and are contained in the larger congruence subgroups $\Gamma(m)$ of Γ . These subgroups are defined in terms of direct decompositions of A or in terms of descending chains of subgroups of A and are of various types. This section and the next one is devoted to the study of such normal subgroups. The main results concern the number of such normal subgroups.

Let $m \geq 1$, $q \geq 1$ be integers.

DEFINITION 6.1. Let $\Lambda(m, q)$ be the subset of Γ such that $\lambda \in \Lambda(m, q)$ if and only if there exists a decomposition of A , namely $A = H \oplus K$, where H has finite rank, such that $h\lambda - h \in mA$ for all $h \in H$ and $k\lambda - k \in mqA$, for all $k \in K$.

Obviously for $q = 1$ we simply obtain the subgroup $\Gamma(m)$ itself and $\Lambda(1, 1) = \Gamma$. When for an automorphism λ of this kind we speak of "a decomposition of A associated with λ" , we shall always tacitly assume the properties specified in this definition. Similarly in later definitions of other types of automorphisms that are defined in terms of direct decompositions of A or subgroup chains of A , a decomposition (or a descending chain) associated with the automorphism in question will always mean the one that has the properties specified in the particular definition.

THEOREM 6.2. *$\Lambda(m, q)$ is a normal subgroup of Γ .*

The proof is just like that of Theorem 3.2 together with the remark on congruence subgroups following it.

We point out that, obviously, $\Lambda(m, q)$ could have equally well been defined as follows: $\lambda \in \Lambda(m, q)$ if and only if there is a subgroup K of A such that A/K is free abelian of finite rank and $a\lambda - a \in mA$ for all $a \in A$, but $k\lambda - k \in mqA$ for all $k \in K$. A little less obvious is that we could also require merely that A/K is finitely generated. Again, one might think of generalizing further by defining $\Lambda(m_1, m_2, \ldots, m_l)$, $l > 2$, to consist of all those automorphisms λ

such that there exists a direct decomposition $A = \oplus \sum_{i=1}^{l} H_i$, only H_l having infinite rank and $h_i\lambda - h_i \in m_1m_2 \ldots m_iA$ for all $h_i \in H_i$. But it is immediate from the definition that $\Lambda(m_1, m_2, \ldots, m_l) = \Lambda(m_1, m_l)$. However, the situation is different when we admit an infinite number of subgroups. Moreover here it is not clear, and in fact not known, whether the definitions based on a direct decomposition of A into summands of finite rank, or on an infinite descending chain with successive factors free abelian of finite rank, or with factors merely required to be finitely generated, lead to the same normal subgroups or not. We restrict ourselves to only one of these possibilities.

Let F be the set of all functions $f : Z^+ \to Z^+$ such that $f(i)$ properly divides $f(i+1)$ for each $i \in Z^+$. For a given function $f \in F$ we define a subset of Γ as follows:

DEFINITION 6.3. Let $f \in F$. Then $\Sigma(f)$ is the subset of Γ such that $\sigma \in \Sigma(f)$ if and only if there exists an infinite descending chain of subgroups of A , say $A = H_1 \geq H_2 \geq \ldots \geq H_i \geq \ldots$, such that H_i/H_{i+1} is free abelian of finite rank for each i and $h_i\sigma - h_i \in f(i)A$ for all $h_i \in H_i$.

THEOREM 6.4. *$\Sigma(f)$ is a normal subgroup of Γ .*

Proof. This uses again the same routine arguments as before. We merely remark that if σ, σ' are two elements of $\Sigma(f)$ and if $A = H_1 \geq H_2 \geq \ldots \geq H_i \geq \ldots$ and $A = H_1' \geq H_2' \geq \ldots \geq H_i' \geq \ldots$ are two descending chains of subgroups of A corresponding to them, then the chain $A = H_1 \cap H_1' \geq H_2 \cap H_2' \geq \ldots$ will do for $\sigma\sigma'$.

It follows from the definition that there can only be countably many normal subgroups of the type $\Lambda(m, q)$. However, of those of type $\Sigma(f)$ there are uncountably many, which fact we now proceed to prove. We shall write $m \| n$ if the integer m divides n or is equal to n .

LEMMA 6.5. *Let $f, g \in F$. Then $\Sigma(g) \leq \Sigma(f)$ if and only if there exists an infinite increasing sequence $(s_i)_i$ of positive integers such*

https://doi.org/10.1017/S0004972700046670 Published online by Cambridge University Press

that $f(i) \| g(s_i)$ *for all* i *, and* $s_1 = 1$.

Proof. (a) *The condition is sufficient:*

We assume that there exists an infinite increasing sequence $(s_i)_i$ of positive integers s_i such that $f(i) \| g(s_i)$, for all i , and $s_1 = 1$. Let $\sigma \in \Sigma(g)$ and let $A = H_1 \geq H_2 \geq \ldots \geq H_i \geq \ldots$ be a descending chain associated with σ . Then the chain $A = K_1 \geq K_2 \geq \ldots \geq K_i \geq \ldots$ where $K_i = H_{s_i}$, $K_1 = H_1$, has the property that $k_i\sigma - k_i \in g(s_i)A$, for all $k_i \in K_i$. Now since $f(i) \| g(s_i)$, for all i , we have $k_i\sigma - k_i \in f(i)A$, for all $k_i \in K_i$. By the definition of $\Sigma(f)$, $\sigma \in \Sigma(f)$. Hence $\Sigma(g) \leq \Sigma(f)$.

(b) *The condition is necessary:*

First, we note that for $\Sigma(g)$ being contained in $\Sigma(f)$ it is necessary that $f(1) \| g(1)$; for consider the element $\sigma \in \Sigma(g)$ defined with respect to a basis $X = \left\{x_i \mid i \in Z^+\right\}$ of A by $x_1\sigma = g(1)x_2 + x_1$, $x_i\sigma = x_i$ for all $i > 1$. For σ to belong also to $\Sigma(f)$, $x\sigma - x \in f(1)A$ must hold for all x , hence in particular for x_1 . Hence $g(1)x_2 \in f(1)A$ and so $f(1) \| g(1)$ as required.

Now we assume that $f(1) \| g(1)$ but there does not exist any sequence of integers satisfying the condition mentioned in the statement of the lemma. This means that for every infinite increasing sequence $(s_i)_i$ of positive integers there exists an integer i_0 such that $f(i_0) \nparallel g(s_{i_0})$. Let $(s_i)_i$ be the sequence such that $s_i = i$ for all i . Thus there exist integers t_1' and t_1 such that $f(t_1') \nparallel g(t_1)$. Next consider the sequence $(t_1+i)_i$. Again, we can find integers t_2' and t_2 such that $f(t_2') \nparallel g(t_2)$ where $t_2 \geq t_1 + 1$. According to our assumption this process will define inductively an increasing sequence $(t_i)_i$ of positive integers with a sequence $(t_i')_i$ of positive integers such that $f(t_i') \nparallel g(t_i)$, for all i , and the sequence $(t_i)_i$ is unbounded and strictly monotonically increasing, that is, $t_i \neq t_j$ if and only if $i \neq j$ (though any number of terms of the sequence $(t'_i)_i$ may be equal to each other).

We now prove that there is an integer k such that $f(i) \nparallel g(j)$ for all $i, j \geq k$. It is sufficient to prove that $f(k) \nparallel g(j)$ for $j \geq k$, because $f(i)$ is a multiple of $f(k)$ for all $i \geq k$. If the contrary is true then for every integer i we can find an integer $l'_i \geq i$ such that $f(i) \| g(l'_i)$. But since the integers i are increasing and unbounded, the sequence of integers l'_i are unbounded and so infinitely many of the l'_i must be distinct. Hence we have an infinite strictly increasing subsequence, $(l_i)_i$ say, such that $f(i) \| g(l_i)$ for all i, which together with $f(1) \| g(1)$ contradicts our basic assumption. And therefore, there exists an integer k such that $f(k) \nparallel g(j)$ for all $j \geq k$.

Let $\sigma \in \Sigma(g)$ be such that with respect to a basis $X = \{x_i \mid i \in Z^+\}$ of A, $x_1\sigma = x_1$, $x_j\sigma = x_j + g(j+k)x_{j-1}$ for all $j > 1$. Suppose that $\sigma \in \Sigma(f)$ so that there exists a descending chain of subgroups of A, namely $A = H_1 \geq H_2 \geq \ldots \geq H_i \geq \ldots$, such that $h_i\sigma - h_i \in f(i)A$ for all $h_i \in H_i$, and for each i, H_i/H_{i+1} has finite rank. Let $s > k$ and consider A/H_s; this has finite rank. Now $x_j\sigma - x_j = g(j+k)x_{j-1}$, for all $j > 1$, so $x_j\sigma - x_j \notin f(i)A$ for any $i > k$ because $f(i) \nparallel g(j)$ for any $i, j > k$. Thus $x_j \notin H_s$ for $j > 1$. We show that all the elements $x_j + H_s$, $j > 1$, are linearly independent in A/H_s. Since A/H_s is free abelian, it is sufficient to prove that if $x = \sum_{i>1} a_ix_i$ is any finite linear combination such that $\text{g.c.d.}\{a_i \mid i > 1\} = 1$, then $x \notin H_s$. Consider $x\sigma - x = \sum_{i>1} a_i(x_i\sigma - x_i) = \sum_{i>1} a_ig(i+k)x_{i-1}$. Now since $\text{g.c.d.}\{a_i \mid i > 1\} = 1$, either $x\sigma - x$ is a primitive element or $x\sigma - x = mx'$ where x' is a primitive element of A and m divides

https://doi.org/10.1017/S0004972700046670 Published online by Cambridge University Press

$g(j)$ for some $j > k$. Since $s > k$, $f(s)\nmid g(j)$ for any j and so $f(s)\nmid m$. Hence $x\sigma - x \notin f(s)A$, but $h_s\sigma - h_s \in f(s)A$ for all $h_s \in H_s$, hence $x \notin H_s$. Thus, as we asserted, the infinitely many elements $x_i + H_s$, $i > 1$ are linearly independent in the factor group A/H_s and so A/H_s cannot have finite rank. This is a contradiction. Hence σ cannot be in $\Sigma(f)$ and the condition of Lemma 6.5 is necessary also.

COROLLARY 6.6. *$\Sigma(g) \nsubseteq \Sigma(f)$ if and only if there exists an integer k such that $f(k)\nmid g(j)$ for all $j \geq k$.*

We now proceed to prove the main result of this section. First, we claim that the set F is uncountable. Let us assume on the contrary that the set F is countable, and let $f_1, f_2, \ldots, f_i, \ldots$ be an enumeration of all elements of F . Consider the function f which is defined as follows: $f(i) = f_1(2).f_2(3) \ldots f_i(i+1)$ for all i . f is a function from Z^+ into Z^+ which has the property that $f(i)$ divides $f(i+1)$ for all i , therefore $f \in F$. But, clearly, f is not equal to any of the functions f_i enumerated above because $f(i) \neq f_i(i)$ for all i . Hence the set F is uncountable. Then, we have

THEOREM 6.7. *There exists an uncountable subset F_1 of the set F such that $\Sigma(f) \neq \Sigma(g)$ if $f, g \in F_1$ and $f \neq g$.*

Proof. Let P^* be the set of all infinite subsets of the set of all primes. P^* is uncountable. Let P be an element of P^* and index the primes in P in some way, for example in order of magnitude, so that $P = \left\{p_i \mid i \in Z^+\right\}$. We construct a function $f_P : Z^+ \to Z^+$ such that for each i , $f_P(i) = p_1p_2 \ldots p_i$. Clearly, $f_P(i)$ divides $f_P(i+1)$ and so $f_P \in F$. Let Q be another element of P^* , $Q \neq P$, $Q = \left\{q_i \mid i \in Z^+\right\}$ and similarly define $f_Q : Z^+ \to Z^+$ such that $f_Q(i) = q_1q_2 \ldots q_i$ for all i . Since $P \neq Q$, we may assume without loss of generality that there is a prime in P which is not in Q ; let it be p_j , say, for some j . Then, $f_P(k)$ does not divide $f_Q(k)$ for any $k > j$ because p_j divides $f_P(k)$, for all $k > j$ but p_j does not appear as a factor of $f_Q(i)$ for any i . Then, by Corollary 6.6 $\Sigma(f_Q) \neq \Sigma(f_P)$. This completes the proof.

7. A second generalization of congruence subgroups

We further generalize the concept of congruence subgroups of Γ and define for each $f \in F$ normal subgroups of Γ which are contained in $\Sigma(f)$. Let $f^* : Z^+ \to R^+$ be a function from the set of positive integers into the set of positive reals, and let F^* be the set of all such functions.

DEFINITION 7.1. $\Sigma(f, f^*)$ is the subset of Γ such that $\sigma \in \Sigma(f, f^*)$ if and only if

(i) $\sigma \in \Sigma(f)$,

(ii) a descending chain $A = H_1 \geq H_2 \geq \ldots$ associated with σ by (i) can be so chosen that, if r_i is the rank of H_i/H_{i+1} , there exists a constant $c(\sigma)$ such that

$$r_i \leq c(\sigma)f^*(i) \text{ for all } i .$$

THEOREM 7.2. $\Sigma(f, f^*)$ *is a normal subgroup of* Γ .

Proof. Again most of the proof is routine. We only remark that for $c(\sigma\sigma')$, where $\sigma, \sigma' \in \Sigma(f, f^*)$, one may take $c(\sigma) + c(\sigma')$, as follows. If $A = H_1 \geq H_2 \geq \ldots$ and $A = H_1' \geq H_2' \geq \ldots$ are the chains associated with σ and σ' respectively, then take again $A = H_1 \cap H_1' \geq H_2 \cap H_2' \geq \ldots$ for $\sigma\sigma'$. Now $H_i \cap H_i'/H_{i+1} \cap H_{i+1}'$ is isomorphic to a subgroup of $H_i/H_{i+1} \oplus H_i'/H_{i+1}'$, so that for each i

$$r\left(H_i \cap H_i'/H_{i+1} \cap H_{i+1}'\right) \leq r\left(H_i/H_{i+1}\right) + r\left(H_i'/H_{i+1}'\right) \leq \left(c(\sigma)+c(\sigma')\right)f^*(i) .$$

As in the case of the normal subgroups of type $\Sigma(f)$, the number of those of type $\Sigma(f, f^*)$ is uncountable; in fact it is uncountable for every fixed f . We show more precisely that we can find for each real number α a normal subgroup N_α of Γ , $N_\alpha = \Sigma\left(f, f_\alpha^*\right)$ for fixed f , such that $N_\alpha > N_\beta$ whenever $\alpha > \beta$. This statement relies on the following theorem.

THEOREM 7.3. *Let* $f^*, g^* \in F^*$ *be such that* f^*, g^* *and the quotient* f^*/g^* *are monotonically increasing and unbounded. Then, for every* $f \in F$, $\Sigma(f, f^*)$ *properly contains* $\Sigma(f, g^*)$.

Proof. That $\Sigma(f, f^*)$ contains $\Sigma(f, g^*)$ is obvious. We only show that there is an element σ in $\Sigma(f, f^*)$ which does not belong to $\Sigma(f, g^*)$.

Since f^* is a positive, non-decreasing function, we can choose a constant c such that $cf^*(i) \geq 2$ for all i . Let $d_i = [cf^*(i)]$ be the integral part of $cf^*(i)$. Choose a basis $X = \{x_i \mid i \in Z^+\}$ and define an automorphism σ of A as follows:

$x_1\sigma = x_1$,

$x_j\sigma = x_j + f(1)x_{j-1}$ for all j such that $1 \leq j \leq d_1 + 1$,

then generally for each $i > 1$:

$$x_j\sigma = x_j + f(i)x_{j-1}$$

for all j such that

$$1 + d_1 + \ldots + d_{i-1} < j \leq 1 + d_1 + \ldots + d_{i-1} + d_i \, .$$

Clearly $\sigma \in \Sigma(f, f^*)$; a descending chain corresponding to σ is given by $H_1 = A$, $H_i = \{x_j \mid j > 1 + d_1 + \ldots + d_{i-1}\}$, and with $c(\sigma) = c$ all requirements are satisfied.

Now assume that σ belongs also to $\Sigma(f, g^*)$, so that there is a descending chain $A = K_1 \geq K_2 \geq \ldots$ corresponding to σ such that $k\sigma - k \in f(i)A$ for all $k \in K_i$ and $r(K_i/K_{i+1}) \leq c'(\sigma)g^*(i)$ for some real constant $c'(\sigma)$. From the definition of σ , the elements x_j for $1 < j \leq 1 + d_1 + \ldots + d_i$ do not belong to K_{i+1} . Now the same argument as at the end of the proof of Lemma 6.5 shows that the elements $x_j + K_{i+1}$ for $1 < j \leq 1 + d_1 + \ldots + d_i$ are linearly independent in A/K_{i+1} . Thus

$$r(A/K_{i+1}) \geq d_1 + d_2 + \ldots + d_i > c[f^*(1) + \ldots + f^*(i)] - i \, ,$$

where $c = c(\sigma)$. Now let $f^*(i)/g^*(i) = r(i)$, so that $r(i) < r(i+1)$ and $r(i) \to \infty$ as $i \to \infty$. Then, from the above

$$r\left(A/K_{i+1}\right) > c(\sigma)\left(r(1)g^*(1) + \ldots + r(i)g^*(i)\right) - i \ .$$

On the other hand, as $r\left(K_i/K_{i+1}\right) \leq c'(\sigma)g^*(i)$, we have

$$r\left(A/K_{i+1}\right) \leq c'(\sigma)\left(g^*(1) + \ldots + g^*(i)\right) \ .$$

Hence, writing $a(\lambda) = \left(c(\sigma)r(\lambda)-c'(\sigma)\right)g^*(\lambda) - 1$ for $\lambda \in Z^+$, we have for all i

$$\sum_{\lambda=1}^{i} a(\lambda) < 0 \ .$$

But $c(\sigma)$ and $c'(\sigma)$ are positive constants, and $r(\lambda)$ and $g^*(\lambda)$ tend to infinity, and so $a(\lambda) \to \infty$, contradicting the above inequality. Thus $\sigma \notin \Sigma(f, g^*)$ as required.

Theorem 7.3 provides us with many ways of constructing normal subgroup chains as described in the introduction. Put, for example, $g_\alpha^*(i) = i^{2^\alpha}$ for all i , where α is an arbitrary real number. Then whenever $\alpha > \beta$ we have $\Sigma\left(f, g_\alpha^*\right) > \Sigma\left(f, g_\beta^*\right)$ for an arbitrary fixed $f \in F$. Clearly other such functions could be used so that there are certainly infinitely many distinct such subgroup chains in each $\Sigma(f)$.

References

[1] J.L. Brenner, "The linear homogeneous group, III", *Ann. of Math.* 71 (1960), 210-223.

[2] L. Fuchs, *Abelian groups* (Pergamon Press, Oxford, London, Edinburgh, New York, Toronto, Sydney, Paris, Braunschweig, 3rd ed. 1960).

[3] Irving Kaplansky, *Infinite abelian groups* (The University of Michigan Press, Ann Arbor, 1954).

[4] George Maxwell, "Infinite general linear groups over rings", *Trans. Amer. Math. Soc.* 151 (1970), 371-375.

[5] Jens L. Mennicke, "Finite factor groups of the unimodular group", *Ann. of Math.* 81 (1965), 31-37.

[6] Alex Rosenberg, "The structure of the infinite general linear group", *Ann. of Math.* 68 (1958), 278-294.

[7] J. Schreier und S. Ulam, "Über die Permutationsgruppe der natürlichen Zahlenfolge", *Studia Math.* 4 (1933), 134-141.

Department of Mathematics,
The University of Karachi,
Karachi, Pakistan.