

Groups with finitely many non-normal subgroups

By

N. S. HEKSTER and H. W. LENSTRA, JR.

1. Introduction. In this paper we describe all groups that have only finitely many non-normal subgroups. Examples of such groups are, of course, groups that do not have any non-normal subgroups at all. It is well-known that the latter groups can be completely described, as follows.

Theorem 1. *Let G be a group. Then all subgroups of G are normal if and only if G satisfies one of the following two conditions:*

- (i) G is abelian;
- (ii) there exist groups A, B such that
 - (a) $G \cong A \times Q \times B$, where Q denotes the quaternion group of order 8;
 - (b) A is an abelian group with the property that every $x \in A$ has finite odd order;
 - (c) B is an abelian group with $x^2 = 1$ for all $x \in B$.

For the proof, see [1, Theorem 12.5.4]. A group G is called *hamiltonian* if it satisfies condition (ii) of Theorem 1.

For a prime number p , denote by C_{p^∞} a multiplicatively written group that is isomorphic to the group of complex roots of unity of p -power order. Our main result is as follows.

Theorem 2. *Let G be a group. Then the number of non-normal subgroups of G is finite if and only if G satisfies one of the following three conditions:*

- (i) G is abelian or hamiltonian;
- (ii) G is finite;
- (iii) there exist a prime number p and groups A, B such that
 - (a) $G \cong A \times B$;
 - (b) A is a finite group of order not divisible by p , and it is abelian or hamiltonian;
 - (c) B has a normal subgroup C , contained in the centre of B , for which B/C is a finite abelian p -group and $C \cong C_{p^\infty}$.

For the proof we refer to Section 4.

We can give a formula for the number of non-normal subgroups of the groups occurring in Theorem 2 (iii). Let G, p, A, B, C be as in Theorem 2 (iii). By $[\cdot, \cdot]$ we denote the map $B/C \times B/C \rightarrow C$ that is induced by the map $B \times B \rightarrow C$ sending (g, h) to $g^{-1}h^{-1}gh$. If J_1, J_2 are subgroups of B/C , then we denote by $[J_1, J_2]$ the subgroup of C generated by the image of $J_1 \times J_2$ under $[\cdot, \cdot]$. Finally, if D is a finite p -group, we write $l_p D$ for the number of factors p in the order of D ; so $l_p D = (\log \# D)/\log p$.

Proposition 3. *Let the notation be as just defined, and let k denote the number of subgroups of A . Then the number of non-normal subgroups of G equals*

$$k \cdot \sum_J (l_p [B/C, J] - l_p [J, J]) \cdot \# J,$$

where J ranges over the set of subgroups of B/C .

The proof is given in Section 2.

It is easy to see from Proposition 3 that a group G as in Theorem 2 (iii) does not have non-normal subgroups at all if and only if B is abelian; this also follows from Theorem 1.

The sum appearing in Proposition 3 is clearly divisible by p . Assuming that B is not abelian one can, more precisely, show the following. If C equals the centre of B , then the sum is congruent to $p \pmod{p^2}$, and at least $p(p + 1)$; and if C is properly contained in the centre of B , then the sum is congruent to $0 \pmod{p^2}$, and at least $p^2(p + 2)$. In particular, any infinite group that has non-normal subgroups at all has at least 6 of them; equality occurs only for the unique non-abelian group containing C_{2^∞} as a central subgroup of index 4.

Another consequence is the following. If the number of non-normal subgroups of a group is a prime number, or the square or the cube of a prime number, then the group is finite.

Let G be a group and σ an automorphism of G . If H is a subgroup of G , we say that σ fixes H if $\sigma H = H$. The following result is needed in the proof of Theorem 2.

Proposition 4. *Let G be a group. Then the following two assertions are equivalent:*

- (i) *G is an infinite abelian group, and it has an automorphism that fixes almost all but not all subgroups of G ;*
- (ii) *there exist a prime number p and groups A, D such that*
 - (a) $G \cong A \times C_{p^\infty} \times D$;
 - (b) A is a finite abelian group of order not divisible by p ;
 - (c) D is a non-trivial finite abelian p -group.

The same is true if both in (i) and in (ii) (b) “abelian” is replaced by “hamiltonian”.

The proof is given in Section 3.

2. Proof of Proposition 3. Let the notation be as in Proposition 3.

Any subgroup of G equals a subgroup of A times a subgroup of B , so the proof of Proposition 3 immediately reduces to the case that $G = B$, which we now assume. We write $\bar{G} = G/C$.

Let H be a subgroup of G , and \bar{H} its image in \bar{G} . Clearly we have $[\bar{H}, \bar{H}] \subset H \cap C$, and H is normal in G if and only if $[\bar{G}, \bar{H}] \subset H \cap C$.

It follows that the number of non-normal subgroups of G equals $\sum_{J,D} n_{J,D}$, where the sum ranges over all pairs of subgroups $J \subset \bar{G}, D \subset C$ for which $[J, J] \subset D, [\bar{G}, J] \not\subset D$, and where $n_{J,D}$ is the number of subgroups H of G with $\bar{H} = J$ and $H \cap C = D$.

For each J , the number of possible D equals $l_p[\bar{G}, J] - l_p[J, J]$. Now fix J and D . Since D is characteristic in C it is normal in G . Hence $n_{J,D}$ equals the number of subgroups of G/D that map isomorphically to J under the natural map $G/D \rightarrow G/C$. Since D contains $[J, J]$, the inverse image of J in G/D is abelian. From $C/D \cong C_{p^\infty}$ it follows that this inverse image is isomorphic to $C_{p^\infty} \times J$. Thus $n_{J,D}$ is the number of subgroups of $C_{p^\infty} \times J$ mapping isomorphically to J , and this number equals $\# \text{Hom}(J, C_{p^\infty}) = \# J$.

We conclude that $\sum_{J,D} n_{J,D} = \sum_{J,D} \# J = \sum_J (l_p[\bar{G}, J] - l_p[J, J]) \cdot \# J$, as required. This proves Proposition 3.

3. Proof of Proposition 4.

Lemma 5. *Let G be an infinite group, and suppose that G is written as the union of a finite set and a finite collection of subgroups. Then the finite set can be omitted from this union.*

Proof. This is an immediate consequence of a lemma of B. H. Neumann, which asserts the following. If a group is written as the union of finitely many cosets of subgroups, then the cosets occurring in that union belonging to subgroups of infinite index can be omitted. For a proof of this lemma, see [2, (4.4); 3, Lemma 4.17]. This proves Lemma 5.

Lemma 6. *Let G be a group and σ an automorphism of G that fixes almost all subgroups of G . Then σ fixes every infinite subgroup of G .*

Proof. Let $H \subset G$ be an infinite subgroup. For every $x \in H - \sigma H$, the subgroup $\langle x \rangle$ generated by x clearly belongs to the finite collection of subgroups C of G with $\sigma C \neq C$. Since for every C there are only finitely many $x \in G$ with $C = \langle x \rangle$, it follows that $H - \sigma H$ is finite. Lemma 5 now implies that $H \cap \sigma H = H$, so H is contained in σH . (This can also be seen without Lemma 5.) Likewise H is contained in $\sigma^{-1}H$, so $H = \sigma H$, as required. This proves Lemma 6.

Lemma 7. *Let G be an abelian group that has an element of infinite order, and σ an automorphism of G that fixes almost all subgroups of G . Then σ fixes all subgroups of G .*

Proof. Let T be the subgroup of G consisting of all elements of finite order. By Lemma 6, one has $\sigma x = x^{\pm 1}$ for every $x \in G - T$. Since G/T is not the union of two proper subgroups the sign is independent of x . But $G - T$ generates G , so either σ is the identity on G or σ maps each $x \in G$ to x^{-1} . This implies Lemma 7.

Lemma 8. *Let G be an abelian group that contains a subgroup of the form $C_{p^\infty} \times C_{p^\infty}$, where p is a prime number. Let σ be an automorphism of G that fixes almost all subgroups of G . Then σ fixes all subgroups of G .*

Proof. By Lemma 6, it suffices to prove that $\sigma H = H$ for every finite subgroup H of G . We may clearly assume that H is cyclic. Then it is easy to see that there exist subgroups C_1 and C_2 of $C_{p^\infty} \times C_{p^\infty}$, both isomorphic to C_{p^∞} , such that $C_1 \supset H \cap (C_{p^\infty} \times C_{p^\infty})$ and $C_1 \cap C_2 = \{1\}$. The infinite subgroups $C_1 H, C_2 H$ of G are fixed by σ , by Lemma 6, so the same is true for $(C_1 H) \cap (C_2 H) = H$. This proves Lemma 8.

We now prove Proposition 4. We treat the “abelian” and the “hamiltonian” case simultaneously.

To prove that (ii) implies (i), let $G = A \times C_{p^\infty} \times D$ as in Proposition 4(ii). It is clear that G is an infinite group that is abelian or hamiltonian, as the case may be. Let ϕ be any non-trivial homomorphism $D \rightarrow C_{p^\infty}$. We prove that the automorphism σ of G given by $\sigma(a, c, d) = (a, c\phi(d), d)$ fixes almost all but not all subgroups of G .

If $d \in D$ is such that $\phi(d) \neq 1$, then clearly the subgroup of G generated by $(1, 1, d)$ is not fixed by σ . It remains to prove that σ fixes almost all subgroups of G . Let p^n be the exponent of D . Since C_{p^∞} has only finitely many elements of order at most p^{2n} , almost any subgroup H of G has an element (a, c, d) with order $(c) > p^{2n}$. Taking the p^n -th power, we see that any such H also contains an element $(1, c', 1)$ with $c' \notin \phi D$. Then $\{1\} \times \phi D \times \{1\} \subset \langle (1, c', 1) \rangle \subset H$, and since σ acts modulo $\{1\} \times \phi D \times \{1\}$ as the identity this implies that σ fixes H . This proves that (ii) implies (i).

To prove that (i) implies (ii), let G be an infinite abelian or hamiltonian group, and let σ be an automorphism of G that fixes almost all but not all subgroups of G .

For a prime number l , let G_l be the subset of G consisting of all elements of finite l -power order. Since G is abelian or hamiltonian, each G_l is a subgroup of G , and it is clearly fixed by σ . Using Lemma 7 we see that G may be identified with the direct sum of all G_l . For any set π of primes, let G_π be the direct sum of all G_l with $l \in \pi$.

Let π be a set of primes, and π' its complement, so that $G = G_\pi \times G_{\pi'}$. Each subgroup of G is the direct sum of a subgroup of G_π and a subgroup of $G_{\pi'}$. It follows that at least one of $G_\pi, G_{\pi'}$ has a subgroup that is not fixed by σ ; say this is $H \subset G_\pi$. Then $H \times G_{\pi'}$ is not fixed by σ , so Lemma 6 implies that $G_{\pi'}$ is finite.

This proves that, for any set π of primes, one of $G_\pi, G_{\pi'}$ has a subgroup not fixed by σ and the other one is finite.

If G_l is non-trivial for infinitely many l , then we can choose π such that both π and π' contain infinitely many such l , contradicting what we just proved. It follows that almost all G_l are trivial. Likewise we obtain a contradiction if G_l is infinite for two distinct primes l . Hence there exists a unique prime p such that G_p is infinite, and this G_p has a subgroup not fixed by σ . For this prime the group $A = G_{\{p\}}$ is finite, it is either abelian or hamiltonian, and we have $G = A \times G_p$.

We now first prove that G_p is abelian. If this is not the case, then we have $p = 2$ and $G_p \cong Q \times B$, where B is an abelian group of exponent 2. In this group, two elements generate the same subgroup if and only if they are conjugate. Hence the hypothesis that σ fixes almost all subgroups implies that G_p is the union of a finite set F and $\bigcup_{\phi} \{x \in G_p : \sigma x = \phi x\}$, with ϕ ranging over the inner automorphisms of G_p . Since there are only finitely many ϕ 's, Lemma 5 implies that the finite set F can be omitted from the union. Hence $\sigma \langle x \rangle = \langle x \rangle$ for every $x \in G_p$, so $\sigma H = H$ for every subgroup

H of G_p , which is a contradiction. This proves that G_p is abelian. In particular, A is abelian if and only if G is abelian, and A is hamiltonian if and only if G is hamiltonian.

For a non-negative integer m , denote by $G(m)$ the subgroup of all elements of G_p of order dividing p^m . We prove that each $G(m)$ is finite. Suppose that this is not the case. Then we can choose m so large that $G(m)$ is infinite and contains an element x with $\sigma \langle x \rangle \neq \langle x \rangle$. The hypothesis that σ fixes almost all subgroups of G implies that $G(m)$ is the union of a finite set F and $\bigcup_a \{x \in G(m) : \sigma x = x^a\}$, with a ranging over the integers mod p^m that are not divisible by p . Lemma 5 now implies that the finite set F can be omitted from the union. Hence $\sigma \langle x \rangle = \langle x \rangle$ for every $x \in G(m)$, contradicting the choice of m . This proves that all $G(m)$ are finite.

For each m , let $C(m)$ be the subgroup $\bigcap_{n \geq 0} G(m+n)p^n$ of $G(m)$. Since $G(m)$ is finite, we have $C(m) = G(m+n)p^n$ for all n exceeding a bound depending on m . This implies that $C(m+1)p = C(m)$ for all m , which readily yields that the set $C = \bigcup_m C(m)$ is a subgroup of G_p that is isomorphic to the direct sum of t copies of C_{p^∞} , for some non-negative integer t . Because C_{p^∞} is divisible we have $G_p \cong C \times D$ for some subgroup D of G_p . If n is such that $C(1) = G(1+n)p^n$, then $Dp^n = \{1\}$, so $D \subset G(n)$ and therefore D is finite. But G_p is infinite, so we must have $t > 0$. By Lemma 8 we have $t < 2$. Therefore $t = 1$, and $C \cong C_{p^\infty}$.

Since G_p has a subgroup not fixed by σ , not every subgroup of G_p is characteristic. Hence $G_p \neq C$, and D is non-trivial.

This proves Proposition 4.

4. Proof of Theorem 2. The *if*-part of Theorem 2 is clear in the cases (i) and (ii), and in case (iii) it suffices to refer to Proposition 3.

Before we prove the *only if*-part we derive a series of auxiliary results.

Lemma 9. *Let G be a group with only finitely many non-normal subgroups. Then every infinite subgroup of G is normal.*

Proof. This follows from Lemma 6, applied to inner automorphisms of G .

Lemma 10. *Let G be a group that has only finitely many non-normal subgroups, and p a prime number. Suppose that G contains a normal subgroup C isomorphic to C_{p^∞} for which G/C is a finite cyclic group. Then G is abelian.*

Proof. For almost all x in a generating coset of G modulo C the subgroup $\langle x \rangle$ is normal in G . Choose such an x . Then the natural map $C \rightarrow G/\langle x \rangle$ is surjective, so $G/\langle x \rangle$ is abelian. Therefore the commutator subgroup G' of G is contained in $\langle x \rangle$, so G' is finite. But G' is the homomorphic image $C^{x^{-1}}$ of C , so it is divisible as well. Hence $G' = \{1\}$. This proves Lemma 10.

Lemma 11. *Let G be a group that has only finitely many non-normal subgroups, and p a prime number. Suppose that G contains a subgroup C of finite index that is isomorphic to C_{p^∞} . Then C is contained in the centre of G .*

Proof. By Lemma 9 the subgroup C is normal. Now apply Lemma 10 to subgroups generated by C and a single element of G . This proves Lemma 11.

Lemma 12. *Let G be a group that has only finitely many non-normal subgroups, and p a prime number. Suppose that G contains a normal subgroup C that is isomorphic to C_{p^∞} for which G/C is a finite p -group. Then G/C is abelian.*

Proof. By Lemma 9 we can choose a positive integer m such that every non-normal subgroup of G has order less than p^m . Denote by $C(m)$ the unique subgroup of C of order p^m . Then every subgroup of G containing $C(m)$ is normal, so $G/C(m)$ is abelian or hamiltonian. But the orders of the elements of $G/C(m)$ are exactly all powers of p , so $G/C(m)$ is not hamiltonian. Therefore $G/C(m)$ is abelian, and it follows that G/C is abelian as well. This proves Lemma 12.

Lemma 13. *Let G be an infinite group that has only finitely many non-normal subgroups, and that is neither abelian nor hamiltonian. Then G has a normal subgroup F of finite index that is abelian or hamiltonian, and that contains a subgroup H that is non-normal in G .*

Proof. We construct a sequence of non-normal subgroups H_1, H_2, \dots , of G and a sequence of normal subgroups F_1, F_2, \dots , of finite index in G with $H_i \subset F_i$ in the following way.

Let H_1 be any non-normal subgroup of G , and F_1 its normalizer in G . All conjugates of H_1 are non-normal in G , so they are finite in number. Hence F_1 is of finite index in G , and by Lemma 9 it is normal.

Suppose, inductively, that H_i, F_i have been constructed. If F_i is abelian or hamiltonian, then the construction stops, and $F = F_i, H = H_i$ satisfy the conclusion of the lemma. If F_i is not abelian or hamiltonian, we let H_{i+1} be any non-normal subgroup of F_i , and F_{i+1} its normalizer in F_i . Then F_{i+1} is normal of finite index in G .

To prove that the process stops, it suffices to show that $H_i \neq H_j$ for $j > i$. But H_i is normal in F_i , whereas H_j is not even normal in the subgroup F_{j-1} of F_i . This proves Lemma 13.

We now prove the *only if*-part of Theorem 2.

Let G be a group that has only finitely many non-normal subgroups, and that is not as in (i) or (ii) of Theorem 2; i.e., G is infinite, and neither abelian nor hamiltonian. Let F, H be chosen as in Lemma 13, and let ϕ be an inner automorphism of G with $\phi H \neq H$. Then F is an infinite group that is abelian or hamiltonian, and the restriction of ϕ to F is an automorphism of F that fixes almost all but not all subgroups of F . Applying Proposition 4 to F we see that F has a subgroup C of finite index that is isomorphic to C_{p^∞} . Then C is of finite index in G , so by Lemma 9 each subgroup of G containing C is normal. Therefore G/C is abelian or hamiltonian, and we can write $G/C = A \times D$, where D is a finite p -group and A is a finite group of order not divisible by p that is abelian or hamiltonian. Also, C is contained in the centre of G , by Lemma 11.

Let E be the unique subgroup of G for which $A = E/C$, and let a be the order of A . Since C is uniquely divisible by a , the cohomology group $H^2(A, C)$ vanishes, so E can be identified with $A \times C$. From $A = \{x \in E : x^a = 1\}$ we see that A is characteristic in E ,

and therefore normal in G . The subgroup B of G with $D = B/C$ is also normal in G , and it follows that $G = A \times B$. Finally, applying Lemma 12 with B in the role of G we see that B/C is abelian.

This completes the proof of Theorem 2.

References

- [1] M. HALL, JR., The theory of groups. New York 1959.
- [2] B. H. NEUMANN, Groups covered by permutable subsets. J. London Math. Soc. **29**, 236–248 (1954).
- [3] D. J. S. ROBINSON, Finiteness conditions and generalized soluble groups, Part 1. *Ergeb. Math. Grenzgeb.* (2) **62**, Berlin-Heidelberg-New York 1972.

Eingegangen am 5. 9. 1988

Anschriften der Autoren:

N. S. Hekster
IBM The Netherlands
Paalbergweg 9–11
1105 AG Amsterdam
The Netherlands

H. W. Lenstra, Jr.
Department of Mathematics
University of California
Berkeley, California 94720
USA