

THE SIMILARITY BETWEEN THE PROPERTIES OF IDEALS IN COMMUTATIVE RINGS AND THE PROPERTIES OF NORMAL SUBGROUPS OF GROUPS

EUGENE SCHENKMAN¹

Introduction. The object of this note is to point out a striking similarity between the properties of the set of normal subgroups of a group with ascending chain condition for normal subgroups and the properties of ideals of a commutative Noetherian ring. In particular it will be seen that a normal subgroup equal to its commutator subgroup is the intersection of pairwise complementary subgroups (analogue of pairwise "relatively prime" ideals). And any normal subgroup modulo which the whole group is semisimple, is the intersection of such subgroups which are irreducible.

The theory is based on making the analogy in the following way: sum of ideals corresponds to the product of normal subgroups; product of ideals corresponds to the commutator of the normal subgroups; and the residual quotient of ideals has an analogue introduced here. The concepts prime ideal, irreducible ideal, and radical of an ideal have analogues for normal subgroups as will be pointed out. For the ideal theory one can consult Northcott [3] or van der Waerden [4].

Preliminaries. In what follows G will denote a group, E the subgroup consisting of the identity element alone, and A and B will denote normal subgroups of G . Then $[A, B]$ will denote the subgroup generated by the commutators $[a, b] = aba^{-1}b^{-1}$ where a is in A and b in B ; a^b will denote the conjugate bab^{-1} of a . AB will denote the group generated by A and B , $A \cap B$ their intersection. $[A, A] = A^{(1)}$ will be the derived group of A ; and for $n > 1$ $A^{(n)}$ will be the derived group of $A^{(n-1)}$.

DEFINITION. The residual quotient of A by B , denoted by $A:B$, will be defined to be the set of elements g of G such that for all b in B $[g, b]$ will be in A . It is clear that $A:B$ contains A since A is normal. Modulo A , $A:B$ is the centralizer of B ; and hence $A:B$ is a normal subgroup of G .

Presented to the Society, January 30, 1958; received by the editors December 16, 1957.

¹ The author is indebted to Professors Butts, Jacob, Kundert and Wade for an interesting seminar in algebraic geometry; to Professor Koch and the referee for improving the statement of the last proposition; and to the National Science Foundation for financial support.

Some of the elementary properties of normal subgroups are listed here.

- (1) $AB = BA$.
- (2) $(AB)C = A(BC)$.
- (3) $[A, B] = [B, A]$ is normal in G .
- (4) $[A, BC] = [A, B][A, C]$.
- (5) $A \subseteq AB$.
- (6) $[A, B] \subseteq A \cap B$.
- (7) $(A \cap B)/[A, B]$ is Abelian.
- (8) $[[AB]C] \subseteq [[B, C]A][[CA]B]$.
- (9) If $(A \cap B \cap C)$ is its own derived group then $A \cap B \cap C = [[A, B]C] = [[B, C]A] = [[C, A]B]$.
- (10) $[(A \cap B), AB] \subseteq [AB]$.
- (11) $[(A : B), B] \subseteq A$.
- (12) $A \subseteq [A : B]$.
- (13) $(\bigcap A_i) : B = \bigcap (A_i : B)$.
- (14) $A : (B_1 B_2 \cdots B_n) = A : B_1 \cap \cdots \cap A : B_n$.
- (15) $A : B = A : AB$.

PROOF. (3) follows from the fact that $[a, b] = [b, a]^{-1}$.

It is clear that the right side of (4) is contained in the left side. On the other hand for a in A , b in B , c in C we have $[a, bc] = [a, b][a, c]^b$ and hence the generators of the left side of (4) are contained in the right side. (6) depends on the fact that $[a, b] = a(a^{-1})^b = b^a b^{-1}$. (8) is the theorem on page 64 of [5]. (9) follows from (6) and (7).

The other statements are direct consequences of the definitions.

Radical groups. In what follows we shall assume the maximum condition for normal subgroups; that is, if A is normal in G then G/A has a finite principal series.

DEFINITION. P is an *irreducible normal subgroup* of G if it is not the intersection of two normal subgroups of G each properly containing P .

DEFINITION. If A is normal in G then the *radical of A* , denoted by $\text{Rad } A$, is defined to be the group union of all normal subgroups K of G such that for some n_k , $K^{(n_k)}$ is contained in A . If A is its own radical then A will be called a radical group or simply a radical.

REMARK 1. When A is a normal subgroup of a group G such that G/A has a finite principal series then for some n , $(\text{Rad } A)^{(n)}$ is contained in A .

REMARK 2. It should be observed that $\text{Rad } A$ is the complete inverse image under the natural map from G to G/A of the radical of G/A in the sense of Fitting [1]; and that the radical of Fitting corre-

sponds to $\text{Rad } E$ as defined above. It is also clear that G modulo a radical is semisimple.

REMARK 3. $\text{Rad } [A, B] = \text{Rad } (A \cap B) = \text{Rad } A \cap \text{Rad } B$. The first equality follows from (6) and (7) above. The second one is a direct consequence of the definitions.

DEFINITION. P is a *prime normal subgroup* of G or P is prime in G if $[A, B] \subseteq P$ implies that either $A \subseteq P$ or $B \subseteq P$.

REMARK 4. P is prime if and only if it is an irreducible radical. For it is clear that if P is prime then it is a radical and it is irreducible. On the other hand if P is an irreducible radical such that $[C, D]$ is contained in P ; then $[CP, DP]$ is contained in P . But $CP \cap DP$ contains P and is Abelian modulo $[CP, DP]$. Since P is a radical $CP \cap DP = P$; since P is irreducible either CP or DP is equal P and hence either C or D is contained in P whence it follows that P is prime.

REMARK 5. P is prime if and only if G/P has a unique minimal normal non-Abelian subgroup.

REMARK 6. If P is prime then $P:A$ is G or P according as A is or is not contained in P . This follows from the definitions with (11) and (12).

REMARK 7. Let \bar{c} and \bar{d} denote conjugate classes of elements of G and let $[\bar{c}, \bar{d}]$ and $\bar{c}\bar{d}$ denote the union of all the classes containing $[c, d]$ and cd respectively, for c in \bar{c} and d in \bar{d} . Then P is prime in G if and only if when the elements of $[\bar{c}, \bar{d}]$ are in P it follows either that those of \bar{c} or those of \bar{d} are in P .

REMARK 8. If A_1, \dots, A_n are normal subgroups of G such that $[\dots [A_1, A_2] \dots A_n]$ is contained in the prime P then for some i between 1 and n , A_i is in P . If $\bar{c}_1, \dots, \bar{c}_n$ are conjugate classes such that the elements of $[\dots [\bar{c}_1\bar{c}_2] \dots \bar{c}_n]$ are in P then for some i the elements of \bar{c}_i are in P .

PROPOSITION. *If A is a normal subgroup of G contained in the set theoretic union of the primes P_1, \dots, P_n , then A is contained in one of them.*

PROOF. We shall prove that if A is contained in none of the primes P_i for $i=1, \dots, n$ then there is a conjugate class of elements contained in A but not in any of the primes P_i . For $n=1$ this assertion is clear. If we assume that the assertion is true for $n-1$ primes then for each i there is a class \bar{c}_i in A whose elements are not contained in $P_1, \dots, P_{i-1}, P_{i+1}, \dots, P_n$. It is clear we need only to consider the case where the elements of \bar{c}_i are in P_i for all i since otherwise the proposition follows. Then let $\bar{c} = \prod_{i=1}^n [\dots [\bar{c}_1, \bar{c}_2] \dots \bar{c}_{i-1}] \bar{c}_{i+1} \dots \bar{c}_n$.

The elements of the j th factor of this product do not all belong to P_j by the previous remark but the elements of all the other factors are in P_j . It follows that for each j we can pick an appropriate class as factor in the above product so that the product contains a class in none of the P_i as was to be shown.

For further results concerning the case where a group is covered by a union of groups one can be referred to the work of Neumann [2].

We shall need the following lemma.

LEMMA. *If A is a radical normal subgroup of G such that G/A has a finite principal series, and if A is the intersection of B and C then A is the intersection of any normal subgroups B' and C' where B'/B and C'/C are solvable.*

PROOF. Let $K = B' \cap C'$. If $K \neq A$ then K contains a subgroup H such that H/A is simple non-Abelian since A is a radical. But H must be in B since otherwise HB/B would not be solvable contrary to the fact that B'/B is solvable. Similarly H must be in C , and hence H is in $B \cap C$ contrary to the fact that $B \cap C = A$ is properly contained in H .

COROLLARY. *If A is a radical such that $A = Q_1 \cap \dots \cap Q_n$ then $A = \text{Rad } Q_1 \cap \dots \cap \text{Rad } Q_n$.*

If $A = B_1 \cap \dots \cap B_n$ where no B_i can be omitted then we shall say that we have a minimal decomposition of A .

THEOREM. *Every radical A of a group G such that G/A has a finite principal series has a unique minimal decomposition as an intersection of primes.*

PROOF. If A is irreducible then it is a prime. Otherwise let $A = B \cap C$ where by the above corollary B and C can be assumed to be radicals. But then by an induction argument on the length of the principal series from A to G , we can assume that B and C have decompositions as intersections of primes; hence A has such also.

Now suppose A has two minimal decompositions into primes, $A = P_1 \cap \dots \cap P_n = R_1 \cap \dots \cap R_m$; then either $m = n$ and the P 's comprise the same set of groups as the R 's or else it is possible to pick a P_i or R_j which is contained in no other group from either set. For definiteness suppose it to be P_1 . Then by (13) and Remark 6 $A : P_1 = P_1 : P_1 \cap \dots \cap P_n : P_1 = G \cap P_2 \cap \dots \cap P_n = P_2 \cap \dots \cap P_n$. On the other hand $A : P_1 = R_1 : P_1 \cap \dots \cap R_m : P_1 = R_1 \cap \dots \cap R_m = A = P_1 \cap \dots \cap P_n$ and we have a contradiction since the decompositions were assumed to be minimal. We are forced to conclude that the minimal decomposition is unique.

The primes determined by the above theorem will be called the primes of A .

REMARK 9. If P is a prime containing a radical A with primes P_1, \dots, P_n then P contains one of the P_i . For $[\dots [P_1, P_2] \dots P_n] \subseteq P_1 \cap P_2 \cap \dots \cap P_n = A \subseteq P$ and hence the assertion follows from Remark 8.

REMARK 10. If A is a radical with primes P_i for $i = 1, \dots, n$ then $A : B = A$ if and only if B is contained in no P_i . For $A = P_1 \cap \dots \cap P_n$ and $(P_1 \cap \dots \cap P_n) : B = P_1 : B \cap \dots \cap P_n : B$ by (13); this, by Remark 6, is equal to $P_1 \cap \dots \cap P_n = A$ if and only if B is contained in no P_i .

When $A : B = A$ we shall say that B is relatively prime to A .

REMARK 11. If both A and B are radicals with minimal decompositions $A = P_1 \cap \dots \cap P_n$, $B = R_1 \cap \dots \cap R_m$ then $A : B = A$ if and only if no R_j is contained in a P_i . This follows from Remarks 9 and 10.

REMARK 12. One might define a primary group Q to be such that if $[A, B] \subseteq Q$ then for some n either $A^{(n)}$ or $B^{(n)}$ is contained in Q . It then follows that if Q is a subgroup of a prime P such that P/Q is solvable, then Q is primary. On the other hand the analogy to ideal theory breaks down here, for it is not true that if Q is primary then $\text{Rad } Q$ is a prime as the following example illustrates. Let H be isomorphic to the group of 2 by 2 matrices of determinant one over a field of 5 elements. Then H has a center Z containing an element z of order 2 and H/Z is simple. If K is the direct product of H and H' where H' is another such group with center element z' of order 2, let $G = K/(zz')$. Then it can be checked that the identity E of G is primary but $\text{Rad } E$ is not prime since it is not irreducible.

Subgroups equal to their derived groups.

DEFINITION. Two normal subgroups A and B of a group G will be called complementary if $G = AB$. In this case we say each is a complement of the other.

REMARK 13. If A and B are complementary subgroups of a group G equal to its derived group; and if A' and B' are normal in G such that A/A' and B/B' are solvable then A' and B' are complementary. For $AB/A'B'$ must be solvable and then since $G = G^{(1)}$, $G = AB = A'B'$.

REMARK 14. If $G = G^{(1)}$ and if A is a complement of B and also of C , then A is also a complement of $[B, C]$ and $B \cap C$. For $AB = G$ and $AC = G$. But because of (4) and (6), $G = G^{(1)} = [AB, AC] \subseteq A[B, C] \subseteq A(B \cap C)$.

REMARK 15. If A is a radical and if A and B are complementary in G then B is relatively prime to A . For B cannot be contained in any

of the primes of A since then $G=AB$ would be also contained in a proper subgroup of G . Remark 10 is then applicable.

THEOREM. *If G is a group equal to its derived group and if $A = A^{(1)}$ is a normal subgroup of G such that G/A has a finite principal series, then A is the intersection of pairwise complementary subgroups C_i such that $C_i = C_i^{(1)}$ and such that the C_i are not intersections of pairwise complementary subgroups.*

PROOF. If A is not an intersection of pairwise complementary subgroups there is nothing to prove. Otherwise A is the intersection of the complementary groups D and F which because of Remark 13 may be taken equal to their derived groups. The theorem now follows readily by an induction argument on the length of the principal series from G to A . For D and F are each intersections of complementary subgroups D_i and F_i equal to their derived groups and such that the D_i and the F_i equal to their derived groups and such that the D_i and the F_i are not intersections of pairwise complementary subgroups; and each D_i is complementary to each F_i since D is complementary to F and D_i contains D , F_i contains F .

Intersections of cosets. If for $i=1, \dots, n$, C_i are normal subgroups of G let their intersection be denoted by C and for $j=1, \dots, n$ let the intersection of all the C_i except C_j be denoted by B_j . Then it is clear that modulo C the group generated by the B_j is the direct product of the B_j . In case this direct product is equal to G we have the following situation.

PROPOSITION. *Using the notations above, the following statements are equivalent:*

- (i) $G = B_1B_2 \cdots B_n$,
- (ii) *for every set of elements a_1, \dots, a_n in G , $\bigcap_{i=1}^n a_iC_i$ is not vacuous.*

PROOF. Suppose $G = B_1B_2 \cdots B_n$ and suppose the a_iC_i are given. Then for each i , $G = C_iB_i$ and hence the coset a_iC_i can be represented as b_iC_i where b_i is in B_i . Then the element $b_1b_2 \cdots b_n$ is in all the given cosets. Thus, if $G = B_1B_2 \cdots B_n$, then $\bigcap_{i=1}^n a_iC_i$ is nonvacuous.

Now suppose that for arbitrary a_i in G , $\bigcap_{i=1}^n a_iC_i$ is not vacuous, and let g be arbitrary in G . Then $x = g \pmod{C_1}$ and $x = 1 \pmod{C_i}$ for $i=2, \dots, n$ have a common solution; that is $g = xc_i$ where x is in B_1 . But now an induction argument on the length of the principal series from G to C allows us to conclude that C_1 is contained in $B_2 \cdots B_n$. It follows that $G = B_1B_2 \cdots B_n$ as was to be shown.

REMARK 16. When $\bigcap_{i=1}^n a_iC_i$ contains the element x then it con-

tains precisely the whole coset xC . For the condition that x and y are in $\bigcap_{i=1}^n a_i C_i$ is that xy^{-1} is in C_i for each i or that y is in the coset xC .

REMARK 17. If the C_i are pairwise complementary normal subgroups of a group G such that $G = G^{(1)}$ and such that G/C has a finite principal series, and if a_i are arbitrary elements of G then the n congruences $x = a_i \pmod{C_i}$ have a common solution and all such common solutions make up precisely a coset of C . For in view of the proposition above and Remark 16 it will be enough to show that the B_i generate G . We do that as follows. There is a non-Abelian factor between G and C_2 since $G = G^{(1)}$; this factor must occur between C_1 and C since C_1 and C_2 are proper complementary subgroups of G . Then if $\bar{C}_i = \bigcap_{n=1}^{\infty} C_i^{(n)}$, \bar{C}_1 must contain C ; and by Remark 13 $\bar{C}_1, C_2, \dots, C_n$ are pairwise complementary. Then by Remark 14, $G = \bar{C}_1 B_1$ and an induction argument on n allows us to conclude that \bar{C}_1 is contained in $B_2 \dots B_n$ whence $G = B_1 B_2 \dots B_n$ as was to be shown.

This above is of course, the analogue of the Chinese Remainder Theorem.

BIBLIOGRAPHY

1. Hans Fitting, *Beitrage zur Theorie der Gruppen endlicher Ordnung*, Jber. Deutschen Math. Verein vol. 48 (1938) pp. 77-141.
2. B. H. Neumann, *Groups covered by finitely many cosets*, Publ. Math. Debrecen vol. 3 (1955) pp. 227-242.
3. D. G. Northcott, *Ideal theory*, London, Cambridge University Press, 1953.
4. B. L. van der Waerden, *Moderne algebra*, New York, Ungar, 1931.
5. Hans Zassenhaus, *Group theory*, New York, Chelsea, 1949.

LOUISIANA STATE UNIVERSITY