On Metabelian Groups ...

Fite William Benjamin

ON METABELIAN GROUPS*

BY

WILLIAM BENJAMIN FITE

Introduction.

The concept of an isomorphism between two groups was introduced by JORDAN in 1868. In the Comptes Rendus of that year, vol. 66, p. 836, he defined an α, 1 isomorphism. Ten years later this concept was generalized to that of an α, β isomorphism by CAPELLI in the Giornali di Matematiche, vol. 16, 1878, p. 33.

Every simple isomorphism of a group with itself may be looked upon as a substitution that replaces each operator of the group by the operator that corresponds to it in this isomorphism. It was first observed by HÖLDER† and MOORE‡ that the totality of these substitutions forms a group. This group is called the group of isomorphisms of the given group.

An isomorphism of a group with itself produced by making every operator of G correspond to its transform with respect to some operator of G is called a cogredient isomorphism. To the totality of cogredient isomorphisms of G corresponds an invariant subgroup of the group of isomorphisms of G. This subgroup is called the group of cogredient isomorphisms of G.§

We define a *Metabelian Group* as *a group whose group of cogredient isomorphisms is abelian.*

The group of cogredient isomorphisms of a group G is simply isomorphic with the quotient group of G with respect to the subgroup formed by the invariant operators of G.‖ If G is metabelian this quotient group is abelian, and therefore the commutators¶ of G are invariant. Conversely, if the commutators of G are invariant, G is metabelian.** Hence we could define a metabelian group as *a group whose commutators are invariant.*

* Presented to the Society August 25, December 28, 1899, and February 23, 1901, under various titles. Received for publication February 3, 1902.

† HÖLDER, Mathematische Annalen, vol. 43 (1893), p. 314.

‡ MOORE, Bulletin of the American Mathematical Society, vol. 1 (1894), p. 61.

§ HÖLDER, loc. cit., p. 314.

‖ This is given implicitly by HÖLDER, loc. cit., pp. 329, 330.

¶ DEDEKIND, Mathematische Annalen, vol. 48 (1897), p. 553.

** MILLER, Bulletin of the American Mathematical Society, vol. 4 (1898), pp. 137 135.

It follows from the definition that every subgroup (and likewise every quotient group) of a metabelian group is either metabelian or abelian.

Let G' be the group of cogredient isomorphisms of a group G, and G'' that of G', and so on.† Then if the series G, G', G'', $\cdots$ ends with identity, G is the direct product of groups of orders $p_1^{a_1}, p_2^{a_2}, \cdots, p_n^{a_n}$ respectively, where $p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ is the order of G and $p_1, p_2, \cdots, p_n$ are distinct primes‡. Conversely, if G is the direct product of groups of orders $p_1^{a_1}, p_2^{a_2}, \cdots, p_n^{a_n}$ respectively, it is evident that we shall arrive at identity by forming these successive groups of cogredient isomorphisms.§ In particular, a metabelian group of order $p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ is the direct product of groups of orders $p_1^{a_1}, p_2^{a_2}, \cdots, p_n^{a_n}$ respectively.

We shall designate by G' the group of cogredient isomorphisms of the group G. Whenever we speak of the operators of G corresponding to the operators of G' we shall suppose that G and G' are arranged in an $\alpha, 1$ isomorphism, the α invariant operators of G corresponding to identity of G'.

A brief summary of the different sections follows.

In section 1 it is shown that certain abelian groups cannot be groups of cogredient isomorphisms. In addition, some limitations on the order of the group of cogredient isomorphisms under certain conditions are given, together with some theorems on the order of the operators of the group of cogredient isomorphisms. There is also a theorem on the order of an abelian subgroup that is always contained in a metabelian group of order p^m, where p is a prime.

The question of the order of the product of two operators of a metabelian group is considered in section 2.

In the second edition of his *Algebra*, vol. 2, p. 133, Weber states, without proof, that the product of two commutators is not necessarily a commutator. It is the object of section 3 to show that there are certain metabelian groups whose commutator subgroups contain operators that are not commutators.

The number of metabelian groups whose order is a given power of a prime and whose invariant operators form cyclic groups is determined in section 4. It is shown that this number depends only on the different orders of the independent generators of the groups of cogredient isomorphisms and is independent of the number of these generators.

In section 5 a similar, but somewhat more limited, investigation is made concerning metabelian groups whose order is a given power of a prime and whose invariant operators form a subgroup that is the direct product of two cyclic groups of unequal orders, the commutator subgroup being contained in that one of these cyclic subgroups which is of the greater order.

† Cf. AHRENS, Leipziger Berichte, Mathematische-Physiche Klasse, vol. 49 (1897), pp. 616–626.

‡ BURNSIDE, *Theory of Groups of Finite Order*, 1897, p. 115.

§ LOEWY, Mathematische Annalen, vol. 55 (1901), pp. 68, 69.

Section 6 contains a discussion of groups that have metabelian groups of cogredient isomorphisms. It is shown that there are certain metabelian groups that cannot be groups of cogredient isomorphisms. Some of the theorems of this section are similar to those of section 1. An application of the results of this section is made to groups of orders p^5 and p^6, where p is a prime.

I am indebted to Professor Miller for helpful suggestions and criticisms in the preparation of this paper.

§ 1. *Abelian groups of cogredient isomorphisms.*

It is known that G' cannot be cyclic nor the direct product of two cyclic groups of different orders, and that if it is abelian it has no operator of order greater than the order of the subgroup formed by the invariant operators of G.*

Let H denote the subgroup formed by the invariant operators of G. Suppose that G' is abelian with the independent generators $A'_1, A'_2, \cdots$ of orders $a'_1, a'_2, \cdots$ respectively. Let $A_1, A_2, \cdots$ be operators of G that correspond respectively to $A'_1, A'_2, \cdots$. Since G' is abelian, we have

$$A_j^{-1}A_1A_j = h_jA_1 \qquad (j=2, 3, \cdots),$$

where the h_j are operators of H. From this we get

$$A_j^{-1}A_1^{a'_j}A_j = h_j^{a'_j}A_1^{a'_j} = A_1^{a'_j}.$$

If now G is of order p^m, where p is a prime, and we denote by a'_n the greatest of the orders $a'_2, a'_3, \cdots$, then $A_1^{a'_n}$ is commutative with every operator of G and is accordingly contained in H. But this is possible only if a'_1 is equal to, or less than, a'_n. Therefore if G is metabelian of order p^m, G' must have at least two independent generators of the highest order.

Now a metabelian group G of order $p_1^{a_1}p_2^{a_2}\cdots p_n^{a_n}$, where $p_1, p_2, \cdots, p_n$ are distinct primes, is the direct product of groups of orders $p_1^{a_1}, p_2^{a_2}, \cdots, p_n^{a_n}$ respectively (see introduction), and G' is the direct product of the groups of cogredient isomorphisms of the respective factor groups.† Let $A'_1, A'_2, \cdots, A'_n$ be operators of the highest order in the groups of cogredient isomorphisms of the respective factor groups. Let these highest orders be $p_1^{a'_1}, p_2^{a'_2}, \cdots, p_n^{a'_n}$ respectively. From what has just been proved it follows that there are operators $B'_1, B'_2, \cdots, B'_n$ in these groups of cogredient isomorphisms of orders

$$p_1^{a'_1}, p_2^{a'_2}, \cdots, p_n^{a'_n}$$

respectively that are independent of $A'_1, A'_2, \cdots, A'_n$. Therefore

$$A'_1A'_2\cdots A'_n \quad \text{and} \quad B'_1B'_2\cdots B'_n$$

* MILLER, Comptes Rendus de l'Académie des Sciences, vol. 128 (1899), p. 229.

† MILLER, Bulletin of the American Mathematical Society, vol. 5 (1899), p. 294.

are two independent generators of G' of the highest order $p_1^{\alpha'_1}p_2^{\alpha'_2}\cdots p_n^{\alpha'_n}$, and the order of every other independent generator of G' is a divisor of $p_1^{\alpha'_1}p_2^{\alpha'_2}\cdots p_n^{\alpha'_n}$. We have proved therefore

THEOREM I.—*The group of cogredient isomorphisms of a group G cannot be the direct product of cyclic groups whose orders are such that any one of them is not a divisor of at least one of the others.*

Now a'_1 is the least common multiple of the orders of $h_2, h_3, \cdots$. But these operators (the commutators formed by A_1 and all the operators of G) form an abelian group, and in any abelian group the least common multiple of the orders of any operators is the order of some operator.* Therefore a'_1 is the order of a commutator of G. This result can be stated as follows:

THEOREM II.—*The order of every operator of the group of cogredient isomorphisms of a metabelian group G is the order of a commutator of G.*

If G' is abelian the order of H is divisible by every prime factor of the order of G, and therefore if the order of G were not divisible by the cube of a prime, G' would be cyclic. Hence, *no group whose order is not divisible by the cube of a prime can be metabelian.*

The least common multiple of the orders of any operators of a group G that is the direct product of groups whose orders are respectively powers of distinct primes is the order of some operator of G.† In particular, this is true of metabelian groups.

THEOREM III.—*If G is a metabelian group of order g and contains an abelian subgroup of order* $g/p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$, *where* $p_1, p_2, \cdots, p_n$ *are distinct primes, the order of every operator of G′ is a divisor of* $p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$.

For, let G_1 denote the abelian subgroup of G of order $g/p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$ and G'_1 the subgroup of G' that corresponds to G_1. It may be assumed that G_1 contains H. If A_1 is any operator of G_1 that is not contained in H, it is commutative with at least $g/p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$ operators of G and therefore the number of its conjugates in G is a divisor of $p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$. The number of commutators of G formed by A_1 and all the operators of G is therefore a divisor of $p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$. These commutators form a group. Therefore the order of the operator of G'_1 that corresponds to A_1, that is, the order of any operator of G'_1, is a divisor of $p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$.

If A_2 is any operator of G that is not contained in G_1, then some power of A_2 of the form

$$A_2^{p_1^{\alpha'_1}p_2^{\alpha'_2}\cdots p_n^{\alpha'_n}},$$

where $\alpha'_1 \overline{\overline{<}} \alpha_1$, $\alpha'_2 \overline{\overline{<}} \alpha_2$, $\cdots$, $\alpha'_n \overline{\overline{<}} \alpha_n$, is contained in G_1, since G_1, whose order is $g/p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$, and A_2 generate a subgroup of G. But if

* FROBENIUS and STICKELBERGER, Crelle's Journal, vol. 86 (1879), p. 234.

† The proof of this is similar to that given by FROBENIUS and STICKELBERGER, loc. cit., for abelian groups.

$$A_2^{p_1^{\alpha'_1}p_2^{\alpha'_2}\cdots p_n^{\alpha'_n}} = A_1$$

then A_1 is commutative with at least $g/p_1^{\alpha_1-\alpha'_1}p_2^{\alpha_2-\alpha'_2}\cdots p_n^{\alpha_n-\alpha'_n}$ operators of G and the number of its conjugates in G is a divisor of $p_1^{\alpha_1-\alpha'_1}p_2^{\alpha_2-\alpha'_2}\cdots p_n^{\alpha_n-\alpha'_n}$. The order of the corresponding operator of G' is therefore a divisor of

$$p_1^{\alpha_1-\alpha'_1}p_2^{\alpha_2-\alpha'_2}\cdots p_n^{\alpha_n-\alpha'_n}.$$

Hence the order of every operator of G' is a divisor of $p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$, and the theorem is proved.

If G_1 is a maximum abelian subgroup of G, the order of G'_1 is divisible by $p_1p_2\cdots p_n$ and contains no other prime factors besides $p_1, p_2, \cdots, p_n$. If now the order of G_1 is $g/p_1p_2\cdots p_n$, G' has an operator of order $p_1p_2\cdots p_n$ that is not in G'_1 and that with G'_1 generates G'. If A_3 is an operator of G that corresponds to this operator of G', A_3 is not commutative with any operator of G_1 that is not in H. The commutators formed by A_3 and two operators A_1 and A_2 of G_1 that correspond to different operators of G'_1 are distinct. The number of commutators of G is therefore equal to the order of G'_1. If the order of G is $g = g_1p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$, where g_1 is not divisible by $p_1, p_2, \cdots, p_n$, and if G' is of order $p_1^{\alpha'_1}p_2^{\alpha'_2}\cdots p_n^{\alpha'_n}$, then the number of commutators of G is

$$p_1^{\alpha'_1-1}p_2^{\alpha'_2-1}\cdots p_n^{\alpha'_n-1}.$$

The order of H is $g_1p_1^{\alpha_1-\alpha'_1}p_2^{\alpha_2-\alpha'_2}\cdots p_n^{\alpha_n-\alpha'_n}$. Therefore

$$\alpha_i - \alpha'_i \geqq \alpha'_i - 1; \qquad \alpha'_i \leqq \tfrac{1}{2}(\alpha_i + 1) \qquad (i = 1, 2, \cdots, n).$$

We have therefore

THEOREM IV.—*If G is a metabelian group of order $g = g_1p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$, where $p_1, p_2, \cdots, p_n$ are distinct primes and g_1 is not divisible by $p_1, p_2, \cdots, p_n$, and if G has a maximum abelian subgroup of order $g/p_1p_2\cdots p_n$, then G' is of order $p_1^{\alpha'_1}p_2^{\alpha'_2}\cdots p_n^{\alpha'_n}$, where*

$$1 < \alpha'_i \leqq \tfrac{1}{2}(\alpha_i + 1) \qquad (i = 1, 2, \cdots, n).$$

Suppose that G has a maximum abelian subgroup of order

$$g_1p_1^{\alpha_1-\alpha'_1}p_2^{\alpha_2-\alpha'_2}\cdots p_n^{\alpha_n-\alpha'_n}$$

and that G' is of order $p_1^{\alpha_1-1}p_2^{\alpha_2-1}\cdots p_n^{\alpha_n-1}$. Consider the subgroup P' of G' of order $p_i^{\alpha_i-1}$ $(i = 1, 2, \cdots, n)$. Let P'_1 be the subgroup of P' that is contained in G'_1. Now if any operator of G that corresponds to an operator of P'_1 is commutative with every operator of G that corresponds to an operator of P' it is contained in H. Also, an operator of G that corresponds to an operator of P' not in P'_1 cannot be commutative with every operator of G that corresponds to an operator of P'_1. Now P'_1, considered as a substitution group on the operators of the subgroup of G that corresponds to P', is of degree

$$g_1p_1p_2\cdots p_i^{\alpha_i}\cdots p_n - g_1p_1p_2\cdots p_i^{\alpha_i-\alpha_i'}\cdots p_n$$

and has

$$g_1p_1p_2\cdots p_i^{\alpha_i-1}\cdots p_n - g_1p_1p_2\cdots p_i^{\alpha_i-\alpha_i'-1}\cdots p_n$$

systems of intransitivity. The total number of letters in P_1' (considered as a substitution group) is therefore *

$$p_i^{\alpha_i-\alpha_i'-1}(g_1p_1p_2\cdots p_i^{\alpha_i}\cdots p_n - g_1p_1p_2\cdots p_i^{\alpha_i-\alpha_i'}\cdots p_n - g_1p_1p_2\cdots p_i^{\alpha_i-1}\cdots p_n + g_1p_1p_2\cdots p_i^{\alpha_i-\alpha_i'-1}\cdots p_n).$$

Now any operator of G that corresponds to an operator of P_1' has p_i conjugates and is commutative with $g_1p_1p_2\cdots p_i^{\alpha_i-1}\cdots p_n$ operators of that subgroup of G that corresponds to P'. Therefore the total number of letters in P_1' is

$$(p_i^{\alpha_i-\alpha_i'-1}-1)(g_1p_1p_2\cdots p_i^{\alpha_i}\cdots p_n - g_1p_1p_2\cdots p_i^{\alpha_i-1}\cdots p_n),$$

and we have

$$p_i^{\alpha_i-\alpha_i'-1}(g_1p_1p_2\cdots p_i^{\alpha_i}\cdots p_n - g_1p_1p_2\cdots p_i^{\alpha_i-\alpha_i'}\cdots p_n - g_1p_1p_2\cdots p_i^{\alpha_i-1}\cdots p_n + g_1p_1p_2\cdots p_i^{\alpha_i-\alpha_i'-1}\cdots p_n)$$
$$= (p_i^{\alpha_i-\alpha_i'-1}-1)(g_1p_1p_2\cdots p_i^{\alpha_i}\cdots p_n - g_1p_1p_2\cdots p_i^{\alpha_i-1}\cdots p_n).$$

Therefore

$$\alpha_i' = \tfrac{1}{2}(\alpha_i - 1).$$

Hence:

THEOREM V. *If G is a metabelian group of order $g = g_1p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$, where $p_1, p_2, \cdots, p_n$ are distinct primes and g_1 is not divisible by $p_1, p_2, \cdots, p_n$, and if G has a maximum abelian subgroup of order $g_1p_1^{\alpha_1-\alpha_1'}p_2^{\alpha_2-\alpha_2'}\cdots p_n^{\alpha_n-\alpha_n'}$, its group of cogredient isomorphisms cannot be of order $p_1^{\alpha_1-1}p_2^{\alpha_2-1}\cdots p_n^{\alpha_n-1}$ unless $\alpha_i' = \frac{1}{2}(\alpha_i - 1)$ $(i = 1, 2, \cdots, n)$.*

If G is any group of order p^m, where p is a prime, it is known that it has an abelian subgroup of order p^γ, if

$$\frac{\gamma(\gamma-1)}{2} < m. \dagger$$

If now G is a metabelian group, the minimum value of m in order that G necessarily contain an abelian subgroup of order p^γ is less than this value when $\gamma > 3$, as is shown in the following

THEOREM VI.—*If G is a metabelian group of order p^m, where p is a prime it contains an abelian subgroup of order p^γ if*

$$m > \frac{(\gamma+3)(\gamma-1)}{4}.$$

*FROBENIUS, Crelle's Journal, vol. 101 (1887), p. 287.

† MILLER, Messenger of Mathematics, vol. 27 (1897-8), p. 120.

Suppose that G contains p^a invariant operators and that its commutator subgroup is of order p^β. Let A_1 be a non-invariant operator of G. It has no more than p^β conjugates and is therefore invariant in a G_1 of order $p^{m-\beta}$ that has at least p^{a+1} invariant operators. Any non-invariant operator A_2 of G_1 is invariant in a G_2 of order $p^{m-2\beta}$ that has at least p^{a+2} invariant operators. By continuing this process, we see that $G_{\gamma-a-1}$ of order $p^{m-(\gamma-a-1)\beta}$ contains $p^{\gamma-1}$ invariant operators, if $m-(\gamma-\alpha-1)\beta>\gamma-1$. In this case $G_{\gamma-a-1}$ contains an abelian subgroup of order p^γ. But $m-(\gamma-\alpha-1)\beta>\gamma-1$, if $m>\frac{1}{4}(\gamma+3)(\gamma-1)$, since $\beta \gtreqless \alpha$.

§ 2. *The order of the product of two operators of a metabelian group.*

Let A and B be any two operators of a metabelian group G, so that

$$A^{-1}BA=hB, \qquad A^{-1}B^xA=h^xB^x,$$

where x is any integer. Then

$$(AB)^x=h^{\frac{1}{2}x(x-1)}A^xB^x.$$

Suppose that A and B are of orders α and β respectively, and let μ be the least common multiple of α and β. Then

$$(AB)^\mu=h^{\frac{1}{2}\mu(\mu-1)}A^\mu B^\mu=h^{\frac{1}{2}\mu(\mu-1)}.$$

Now the order of h is a divisor of both α and β. Therefore if α and β are both odd, or if they contain the factor 2 to different powers,

$$(AB)^\mu=1.$$

But if α and β contain the factor 2 to the same power, we cannot conclude that

$$(AB)^\mu=1.$$

In this case, however,

$$(AB)^{2\mu}=1.$$

The operators $A\equiv bd$, $B\equiv ab\cdot cd\cdot efg$ of the group $(abcd)_8(efg)cyc$ * may be cited as two operators of a metabelian group the order of whose product is twice the least common multiple of their orders.

Let γ be the order of $C=AB$, and let p^a, p^b, p^c be the highest powers of p (any prime) contained in α, β, γ respectively. Then since $BC^{-1}=A^{-1}$ and $C^{-1}A=B^{-1}$, it follows from the preceding that of the numbers a, b, c two are equal and the third one less than, or equal to, the other two, except that in the case $p=2$ the third one may be one greater than the value of the other two.

Hence:

* For this notation see CAYLEY, Quarterly Journal of Mathematics, vol. 25 (1890-1), p. 76.

THEOREM I.—*If G is a metabelian group, the order γ of the product of any two of its operators A and B of orders α and β respectively must be a divisor of the least common multiple of α and β, except that when α and β contain the same power of 2 as a factor, γ is a divisor of twice the least common multiple of α and β. Also γ must be a multiple of the least common multiple of α' and β', where $\alpha = \delta\alpha'$, $\beta = \delta\beta'$, δ being the product of the powers of all the prime factors that occur to the same power in α and β, except that, when one of the numbers α, β contains the factor 2 to a power one higher than the other one does, γ is a multiple of one-half the least common multiple of α' and β'.*

COROLLARY.—*If α and β are relatively prime, $\alpha\beta$ is the order of AB.*

This follows from the fact that in this case A and B are commutative.

COROLLARY.—*If G is a metabelian group of order p^m, where p is an odd prime, the order of the product of any two of its operators A and B, of orders p^{n_1} and p^{n_2} respectively $(n_1 > n_2)$, is p^{n_1}. If $p = 2$, the order of AB must be 2^{n_1}, except that it may be 2^{n_2} when $n_1 = n_2 + 1$.*

If G is an abelian group, the order of AB is a multiple of the least common multiple of α' and β', and a divisor of the least common multiple of α and β. Two commutative operators A and B can be chosen so that the order of AB is any multiple of the least common multiple of α' and β' that is also a divisor of the least common multiple of α and β. For, take

$$A \equiv a_1 a_2 \cdots a_\delta \cdot b_1 b_2 \cdots b_{\delta'} \cdot c_1 c_2 \cdots c_{\alpha'},$$

where δ' is any divisor of δ, and

$$B \equiv a_\delta a_{\delta-1} \cdots a_2 a_1 \cdot d_1 d_2 \cdots d_{\beta'}.$$

The order of AB is δ' times the least common multiple of α' and β'.

THEOREM II.—*In a metabelian group G the order of the product of two operators that correspond respectively to two independent operators of G' is a multiple of the least common multiple of the orders of these operators of G'.*

This follows from the fact that the order of the product of two independent commutative operators is the least common multiple of the orders of the operators.

THEOREM III.—*In a metabelian group G of order p^m, where p is a prime, the order of the product of two operators that correspond respectively to two operators of G' of different orders is equal to, or greater than, the greater of these orders.*

This follows from the fact that the order of the product of two commutative operators of orders $p_{n_1}^{n_1}$ and p^{n_2} respectively, where $n_1 > n_2$, is p^{n_1}.

THEOREM IV.—*If G is a metabelian group of order p^m, where p is an odd* *prime, the p^β power of all the operators form a group, p^β being the highest order of any commutator of G.*

For if $A^{p^\beta} = h_1$, and $B^{p^\beta} = h_2$, then

$$(AB)^{p^\beta} = h^{\frac{1}{2}p^\beta(p^\beta-1)} A^{p^\beta} B^{p^\beta} = h_1 h_2,$$

where $A^{-1}BA = hB$.

§ 3. *The commutators of a metabelian group.*

The commutator subgroup of a group is invariant in the group,* and in a group of order p^m an operator of order p cannot be transformed into one of its own powers, except the first.† Hence, *a group of order p^m, where p is a prime, is metabelian if its commutator subgroup is of order p.*

If the commutator subgroup of a group G of order p^m is of order p^a and contains a subgroup H_1 of order p^{a-1} that is invariant in G, then G/H_1 is metabelian, since its commutator subgroup is of order p.

Let G be a metabelian group whose group of cogredient isomorphisms is generated by three independent operators. Let A_1, A_2, A_3 be three operators of G that correspond respectively to the three generators A_1', A_2', A_3', of G'. If

$$A_2^{-1} A_1 A_2 = h_1 A_1, \qquad A_3^{-1} A_1 A_3 = h_2 A_1, \qquad A_3^{-1} A_2 A_3 = h_3 A_2,$$

then h_1, h_2, h_3 generate the commutator subgroup of G. We proceed to prove that every operator of this subgroup is a commutator.

This is done by showing that integral values of a_1, a_2, a_3, b_1, b_2, b_3 can be found that will satisfy the relation

$$(A_1^{a_1} A_2^{a_2} A_3^{a_3})^{-1} \cdot A_1^{b_1} A_2^{b_2} A_3^{b_3} \cdot (A_1^{a_1} A_2^{a_2} A_3^{a_3}) = h_1^{\alpha_1} h_2^{\alpha_2} h_3^{\alpha_3} A_1^{b_1} A_2^{b_2} A_3^{b_3}$$

for all integral values of α_1, α_2, α_3 taken modulo the orders of h_1, h_2, h_3 respectively.

Now

$$(A_1^{a_1} A_2^{a_2} A_3^{a_3})^{-1} \cdot A_1^{b_1} A_2^{b_2} A_3^{b_3} \cdot (A_1^{a_1} A_2^{a_2} A_3^{a_3})$$
$$= h_3^{a_3 b_2} h_2^{a_3 b_1} h_3^{-a_2 b_3} h_1^{a_2 b_1} h_2^{-a_1 b_3} h_1^{-a_1 b_2} A_1^{b_1} A_2^{b_2} A_3^{b_3}.$$

Hence the relation given above will be satisfied if the following equations are satisfied

$$a_2 b_1 - a_1 b_2 = \alpha_1, \qquad a_3 b_1 - a_1 b_3 = \alpha_2, \qquad a_3 b_2 - a_2 b_3 = \alpha_3.$$

But integral values of a_1, a_2, a_3, b_1, b_2, b_3 can always be found that satisfy these equations.

* MILLER, Quarterly Journal of Mathematics, vol. 28 (1896), p. 266. Cf. FROBENIUS, Berliner Sitzungsberichte, 1896, p. 1348.

† FROBENIUS, loc. cit., 1895, p. 982.

If h_1, h_2, h_3 are not all distinct, or if any of them equal identity, the conclusion still holds.

Consider now a metabelian group G of order p^m whose group of cogredient isomorphisms is generated by four independent operators, A_1', A_2', A_3', A_4', and let A_1, A_2, A_3, A_4 be operators of G that correspond respectively to these generators of G'. Let

$$A_2^{-1}A_1A_2 = h_1A_1, \qquad A_3^{-1}A_1A_3 = h_2A_1, \qquad A_4^{-1}A_1A_4 = h_3A_1,$$
$$A_3^{-1}A_2A_3 = h_4A_2, \qquad A_4^{-1}A_2A_4 = h_5A_2, \qquad A_4^{-1}A_3A_4 = h_6A_3.$$

We assume that it is possible that the h_i $(i = 1, 2, \cdots, 6)$ be all different from identity and independent. We shall justify this assumption later.

Now the h_i $(i = 1, 2, \cdots, 6)$ generate the commutator subgroup of G; that is, every commutator is obtained from $A_1^{a_1}A_2^{a_2}A_3^{a_3}A_4^{a_4}$ and $A_1^{b_1}A_2^{b_2}A_3^{b_3}A_4^{b_4}$, where a_1, a_2, a_3, a_4, and also b_1, b_2, b_3, b_4 take all possible values modulo the orders of A_1', A_2', A_3', A_4' respectively.

We have

$$(A_1^{a_1}A_2^{a_2}A_3^{a_3}A_4^{a_4})^{-1}A_1^{b_1}A_2^{b_2}A_3^{b_3}A_4^{b_4}(A_1^{a_1}A_2^{a_2}A_3^{a_3}A_4^{a_4})$$
$$= h_1^{a_2b_1-a_1b_2}h_2^{a_3b_1-a_1b_3}h_3^{a_4b_1-a_1b_4}h_4^{a_3b_2-a_2b_3}h_5^{a_4b_2-a_2b_4}h_6^{a_4b_3-a_3b_4}A_1^{b_1}A_2^{b_2}A_3^{b_3}A_4^{b_4}.$$

If now p^{m_i} is the order of h_i, and k_i is an integer $(i = 1, 2, \cdots, 6)$, then $h_1^{\alpha_1}h_2^{\alpha_2}h_3^{\alpha_3}h_4^{\alpha_4}h_5^{\alpha_5}h_6^{\alpha_6}$ is an operator of the commutator subgroup of G that is not a commutator if integral values of a_i and b_j $(i, j = 1, 2, \cdots, 4)$ cannot be found to satisfy the following equations:

$$a_2b_1 - a_1b_2 = \alpha_1 + k_1p^{m_1}, \; a_3b_1 - a_1b_3 = \alpha_2 + k_2p^{m_2}, \; a_4b_1 - a_1b_4 = \alpha_3 + k_3p^{m_3},$$
$$a_3b_2 - a_2b_3 = \alpha_4 + k_4p^{m_4}, \; a_4b_2 - a_2b_4 = \alpha_5 + k_5p^{m_5}, \; a_4b_3 - a_3b_4 = \alpha_6 + k_6p^{m_6}.$$

Such integral values cannot be found to satisfy these equations for all values of α_i $(i = 1, 2, \cdots, 6)$; *e. g.*, for $\alpha_i = 1$. Therefore if a group exists that has the properties assumed, the commutator subgroup of this group contains operators that are not commutators. The group generated by the following operators is such a group: *

$$h_1 \equiv ac \cdot bd, \qquad h_2 \equiv eg \cdot fh, \qquad h_3 \equiv ik \cdot jl,$$
$$h_4 \equiv mo \cdot np, \qquad h_5 \equiv qs \cdot rt, \qquad h_6 \equiv uw \cdot vx,$$
$$A_1 \equiv ac \cdot eg \cdot ik, \qquad A_2 \equiv ab \cdot cd \cdot mo \cdot qs,$$
$$A_3 \equiv ef \cdot gh \cdot mn \cdot op \cdot uw, \qquad A_4 \equiv ij \cdot kl \cdot qr \cdot st \cdot uv \cdot wx.$$

* This group was constructed by Professor MILLER.