ON THE STRUCTURE OF CERTAIN FACTORIZABLE GROUPS, I

DANIEL GORENSTEIN[1] AND I. N. HERSTEIN

1. A considerable amount is known about the structure of finite factorizable groups—that is, groups G which can be represented in the form AB, where A and B are subgroups of G. Such groups are known to be solvable under a variety of assumptions on the subgroups A and B. If A and B are both Abelian, Ito [6] has shown that G is actually metabelian. If A and B are both cyclic, it is easy to see that either a subgroup of A or a subgroup of B must be normal in G (Douglas [1]).

Our investigations into the structure of finite groups of the form ABA, A, B being cyclic, [4; 5] have included AB groups as a special case. For our further work on this subject, it has been necessary to determine the precise structure of an AB group in which A is its own normalizer. Our results are contained in the following theorem.

THEOREM A. *Let G be a finite group of the form AB, where A and B are cyclic subgroups of G, and A is its own normalizer in G. Then G contains a unique cyclic normal subgroup T such that $G=AT$ and $A\cap T=1$. Moreover, T is the commutator subgroup of G and G is metacyclic.*

In the final section we shall give an example of a group satisfying the conditions of the theorem in which B itself is not normal. This example[2] will simultaneously resolve a question which Douglas raised in his paper [2] on AB groups in which A and B are cyclic and $A\cap B=1$. If A_1, B_1 are the maximal subgroups of A, B respectively which are normal in G, Douglas called the normal subgroup $N=\{A_1, B_1\}$ the *nucleus* of G. Since G/N is a group satisfying the same conditions as G, he constructed by induction a chain of groups $G=G_0, G_1, \cdots, G_r=1$, where $G_{i+1}=G_i/N_i$, N_i being the nucleus of G_i; and he then defined the integer r to be the *type* of G (with respect to the subgroups A, B). Thus if B is normal in G, G is of type $\leqq 2$ (with respect to A, B). Douglas raised the question of whether there exist AB groups of arbitrarily high type.

Received by the editors February 2, 1959.

[1] A portion of this research was done at the 1957 Summer Mathematical Conference at Bowdoin College, under contract to the Electronics Research Directorate, Air Force Cambridge Research Center, Air Research and Development Command, contract number AF 19(604)-2226.

[2] This example is given in [3].

Our example will show that there do exist groups of the form AB, with A, B cyclic, $A\cap B=1$, and in addition, with A its own normalizer, which are of arbitrarily high type with respect to A, B. However, Theorem A shows that any such group is of type 2 with respect to the subgroups A and T.

2. The proof of Theorem A is by induction on the order of G. We assume throughout that $A=(a)$ is of order h, $B=(b)$ is of order k.

We first dispose of the uniqueness of T. In fact, if $G=AT$, T normal in G, $A\cap T=1$ (T not necessarily assumed cyclic), then $T=[G,G]$. Since G/T is Abelian, $T\supseteq[G,G]$. On the other hand, since $N(A)=A$, a induces an automorphism ϕ on T leaving only the identity element fixed, and hence every element of T has a representation in the form $t^{-1}\phi(t)=t^{-1}ata^{-1}$, and so is in $[G,G]$.

We first consider the case in which a subgroup of A is normal in G. If $A\cap B=1$, let A_1 be any subgroup of A, normal in G; while if $A\cap B\neq 1$, set $A_1=A\cap B$. $A_1=(a^r)$ for some $r\mid h$. Let $\overline{G}=G/A_1=\overline{A}\,\overline{B}$, where $\overline{A}=(\bar{a})$, $\overline{B}=(\bar{b})$ are the residues of A, B in $\overline{G}$, and $\overline{B}$ has order m. In both cases we clearly have $\overline{A}\cap\overline{B}=1$, so that by induction $\overline{G}=\overline{A}\,\overline{T}$, where $\overline{T}=(\bar{t})$ is cyclic, normal in $\overline{G}$, and $\overline{A}\cap\overline{T}=1$. Since $o(\overline{G})=rm$, $o(\overline{T})=m$.

If t is a representative of $\bar{t}$ in G, our conditions imply

(1) $ta^rt^{-1}=a^{r\gamma}$ and $ata^{-1}=t^\beta a^{r\alpha}$ for suitable integers α, β, γ.

First of all, suppose $(\beta-1,\ m)=c$; then (1) yields $\bar{a}\bar{t}^{m/c}\bar{a}^{-1}=\bar{t}^{\beta m/c}$; whence $\bar{t}^{-m/c}\bar{a}\bar{t}^{m/c}=\bar{a}$. Hence $\bar{t}^{m/c}\in N(\overline{A})\cap\overline{T}=\overline{A}\cap\overline{T}=1$, and so $c=1$. Thus

$$(\beta-1,\ m)=1. \tag{2}$$

Now conjugating (1) by a leads to

$$ata^{-1}a^rata^{-1}=a^{r\gamma},\quad\text{whence}\quad t^\beta a^{r\alpha}a^ra^{-r\alpha}t^{-\beta}=a^{r\gamma}.$$

Thus $a^{r\gamma^\beta}=a^{r\gamma}$, and so $\gamma^{\beta-1}\equiv 1 \pmod{h/r}$. On the other hand, $t^ma^rt^{-m}=a^r$ since t^m is in A_1. But by (1) $t^ma^rt^{-m}=a^{r\gamma^m}$, and so $\gamma^m\equiv 1 \pmod{h/r}$. It follows at once from (2) that $\gamma\equiv 1 \pmod{h/r}$, and hence $ta^rt^{-1}=a^r$.

Let $t^m=a^\delta$. Then $a^\delta=at^ma^{-1}=t^{\beta m}a^{r\alpha m}=a^{\delta\beta+r\alpha m}$, whence

$$\delta(\beta-1)\equiv-\alpha m \pmod{h/r}. \tag{3}$$

By (2) there exist integers i and j such that $1=i(\beta-1)+jm$, whence by (3), $\alpha=\alpha i(\beta-1)+\alpha jm\equiv(\alpha i-\delta j)(\beta-1) \pmod{h/r}$. Thus there exists an integer ϵ such that

$$\epsilon(\beta-1)\equiv\alpha \pmod{h/r}. \tag{4}$$

We shall now show that the element $x = ta^{r\epsilon}$ generates a cyclic normal subgroup T' of G. It suffices to show that T' is invariant under conjugation by t and a. Clearly $txt^{-1} = x$. On the other hand,

$$axa^{-1} = t^{\beta}a^{r\alpha+r\epsilon} = t^{\beta}a^{r\epsilon\beta} = x^{\beta}, \tag{5}$$

using (4).

Since a, t generate G, so do a and x; and hence $G = AT'$. Since $\bar{x} = \bar{t}$, no power of x less than m is in A, and $x^m \in A_1$. Then $x^m = a^{r\nu}$ for some integer ν and x has order mq for some integer q. If $q = 1$, $x^m = 1$, and the desired conclusion $A \cap T' = 1$ follows. If $q > 1$, we proceed as follows: using (5) we obtain $x^m = x^{m\beta}$, which together with (2), implies

$$q \mid (\beta - 1) \quad \text{and} \quad (q, m) = 1. \tag{6}$$

We can therefore find an integer w such that $wm \equiv 1 \pmod{q}$. Setting $y = xa^{-r\nu w}$, we find that $y^m = x^m a^{-r\nu wm} = a^{r\nu(1-wm)} = 1$. Moreover, $aya^{-1}, = x^{\beta}a^{-r\nu w} = x^{\beta}a^{-r\nu w\beta} = y^{\beta}$. Thus y generates a cyclic normal subgroup T of G of order m such that $G = AT$ and $A \cap T = 1$. This completes the proof in the case that a subgroup of A is normal in G.

3. We now consider the case in which no subgroup of A, and hence in which some subgroup of B is normal in G. In particular $A \cap B = 1$. Let $B_1 = (b^r)$ be a minimal subgroup of B which is normal in G. We may assume $r \mid k$, and hence k/r is a prime p. Let $\overline{G} = G/B_1 = \overline{A}\,\overline{B}$, where $\overline{A} = (\bar{a})$, $\overline{B} = (\bar{b})$ are the residues of A, B, in $\overline{G}$. Clearly $\overline{A} \cap \overline{B} = 1$.

Let $\overline{B}_0 = N(\overline{A}) \cap \overline{B}$; $\overline{B}_0 = (\bar{b}^s)$ with $s \mid r$. In G we have the relations

$$a^{-1}b^r a = b^{r\lambda} \quad \text{and} \quad b^s a b^{-s} = a^{\alpha}b^{r\beta} \quad \text{for suitable integers } \lambda, \alpha, \beta. \tag{7}$$

Since $N(A) = A$, (7) implies

$$(\lambda - 1, p) = 1. \tag{8}$$

Hence there exists an integer γ such that

$$\gamma(\lambda - 1) \equiv -\beta \pmod{p}. \tag{9}$$

Using (7) and (9), we now have

$$a^{-1}b^{s+r\gamma}a = (a^{-1}b^s a)(a^{-1}b^{r\gamma}a) = (a^{\alpha-1}b^{s+r\beta})(b^{r\gamma\lambda}) = a^{\alpha-1}b^{s+r\gamma}$$

whence

$$b^{s+r\gamma}ab^{-s-r\gamma} = a^{\alpha}. \tag{10}$$

Since $N(A) = A$ and $A \cap B = 1$, $b^{s+r\gamma} = 1$, whence $\bar{b}^s = 1$ and

$$N(\overline{A}) = \overline{A}.$$

Hence by induction $\overline{G} = \overline{A}\,\overline{T}$, $\overline{T}$ cyclic, normal in $\overline{G}$, $\overline{A} \cap \overline{T} = 1$. If T

denotes the inverse image of $\overline{T}$ in G, $G=AT$, T normal in G, metacyclic and $A\cap T=1$. By the uniqueness part of our argument, $T=[G, G]$ and hence by Ito's result, T is Abelian.

Thus to prove T is cyclic, it suffices to prove that each Sylow subgroup of T is cyclic. Let Q be the q-Sylow subgroup of T for some $q \mid o(T)$. Then $AQ=AB_q$ for some subgroup $B_q \subset B$. If $Q<T$, $AQ<G$, and the cyclicity of Q follows by induction on the order of G. We may therefore assume T is of prime power order. Since $B_1 \subset T$ and $o(B_1)=p$, T is a p-group.

If $\overline{T}=(\bar{t})$ and t is a representative of $\bar{t}$ in G, T is generated by t and b^r satisfying $tb^rt^{-1}=b^{r\sigma}$. Since b^r has order p, and t has order a power of p, $\sigma \equiv 1 \pmod{p}$ and T is Abelian. If T is not elementary Abelian, the elements of order dividing p in T form a proper subgroup of T, which by induction will be cyclic, and this will imply T is cyclic.

Hence we may assume T is elementary Abelian of type (p, p), so that $k=p^2$, $r=p$. Let $t=a^ib^j$. Since $A\cap T=1$ and $b^p \in T$, $j \not\equiv 0 \pmod{p}$. Since T is Abelian,

$$(a^ib^j)b^p(a^ib^j)^{-1} = b^p, \tag{11}$$

whence

$$a^{-i}b^pa^i = b^p. \tag{12}$$

Since T is normal, and is generated by t and b^p,

$$a^{-i}ta^i = t^\alpha b^{p\beta} \qquad \text{for some integers } \alpha, \beta \tag{13}$$

Hence in $\overline{G}$, we have $\bar{a}^{-i}\bar{t}\bar{a}^i=\bar{t}^\alpha$, so that

$$1 = \bar{b}^{jp} = (\bar{a}^{-i}\bar{t})^p = \bar{t}^{\alpha+\alpha^2+\cdots+\alpha^p}\bar{a}^{-ip}.$$

Since $\overline{A}\cap\overline{T}=1$ and $\bar{t}^p=1$, $\alpha(\alpha^p-1)/(\alpha-1) \equiv 0 \pmod{p}$. Hence either $\alpha \equiv 0 \pmod{p}$ or $\alpha \equiv 1 \pmod{p}$. But $\alpha \equiv 0 \pmod{p}$ is clearly impossible, so that $\alpha \equiv 1 \pmod{p}$ and consequently $t^\alpha = t$. Thus

$$b^{jp} = t^pb^{p\beta(1+2+\cdots+p)}a^{-ip} = a^{-ip} \qquad \text{if } p \text{ is odd,}$$

and consequently $b^{jp} = 1$, contrary to the fact that $p \nmid j$ and b has order p^2.

On the other hand, if $p=2$, $k=4$, and (7) reduces to $a^{-1}b^2a=b^2$, so that $b^2 \in N(A)$, a contradiction. Thus G contains a cyclic normal subgroup T such that $G=AT$ and $A\cap T=1$.

4. The example we shall now construct depends upon two arithmetic identities, which are easily verified and which we state without proof:

$$4^{3^{n-1}} \equiv 1 \pmod{3^n}, \qquad 4^{3^{n-1}} \not\equiv 1 \pmod{3^{n+1}} \tag{14}$$

$$\frac{16^{3^{n-1}}-1}{16-1} \equiv 3^{n-1} \pmod{3^n}. \tag{15}$$

Define the metacyclic group G_n by the relations

$$a^h = 1, \quad t^k = 1, \quad ata^{-1} = t^{-4}, \quad \text{where} \quad h = 2\cdot 3^{n-1} \quad \text{and} \quad k = 3^n. \tag{16}$$

For (16) to define a group of order hk we must have

$$(-4)^h \equiv 1 \pmod{k},$$

which follows at once from (14).

If $A=(a)$, $T=(t)$, we have $G_n = AT$, T normal in G_n and cyclic, and $A\cap T=1$.

If $t^i \in N(A)$, $i\equiv -4i \pmod{k}$ and hence $k \mid i$, whence $t^i=1$. Thus A is its own normalizer in G_n.

Let $b=ta^2$ and put $B=(b)$. We shall now prove

THEOREM B. *G_n is of the form AB with $A\cap B=1$ and is of type $2n$ with respect to the subgroups A and B.*

PROOF. From (16) we obtain

$$b^i = (ta^2)^i = t^{(16^i-1)/(16-1)}\, a^{2i}. \tag{17}$$

Since a has order $2\cdot 3^{n-1}$, (15) and (17) imply

$$b^{3^{n-1}} = t^{3^{n-1}}, \qquad \text{whence } b \text{ has order} \qquad k = 3^n. \tag{18}$$

Moreover, no power of b is a power of a, for otherwise we would have $b^{3^j}=a^r$ for some $j<n$, whence by (17)

$$\frac{16^{3^j}-1}{16-1} \equiv 0 \pmod{3^n}$$

which would contradict (15) with $n-1$ replaced by j. Thus $A\cap B=1$ and consequently the set AB contains $hk=o(G_n)$ elements. Thus $G_n=AB$.

To prove G_n is of type $2n$ with respect to A, B, we proceed by induction. If $n=1$, $a^2=1$, $t=b$, and $aba^{-1}=b^{-1}$, so that G_1 is of type 2 with respect to A, B.

We now compute the nucleus N_n of G_n. For a^i to generate a normal subgroup of G, we must have $(-4)^i\equiv 1 \pmod{k}$ by (16). The multiplicative order of 4 (mod 3^n) is 3^{n-1}, and hence the multiplicative order of (-4) (mod 3^n) is $2\cdot 3^{n-1}$. Thus $2\cdot 3^{n-1} \mid i$ and hence no subgroup of A is normal in G_n.

Now (18) implies that the subgroup $(b^{3^{n-1}})$ is normal in G_n. We shall prove that this subgroup is the nucleus N_n of G_n. From (15) and

(17), we have $b^{3^j} = t^{q3^j} a^{2\cdot 3^j}$, where $q \not\equiv 0 \pmod 3$, and hence

$$ab^{3^j}a^{-1} = t^{-4q3^j} a^{2\cdot 3^j}. \tag{19}$$

For (b^{3^j}) to be normal in G_n, we must have $ab^{3^j}a^{-1} = b^{\lambda 3^j} = t^r a^{2\lambda 3^j}$ for some integer r, whence by (19), $\lambda \equiv 1 \pmod{3^{n-1-j}}$, and hence, for some integer s, $b^{\lambda 3^j} = b^{s3^{n-1}+3^j} = t^{s3^{n-1}+q3^j} a^{2\cdot 3^j}$. We must therefore have

$$s\cdot 3^{n-1} + q3^j \equiv -4q3^j \pmod{3^n}.$$

Since $q \not\equiv 0 \pmod 3$, this is impossible if $j < n-1$. Thus $N_n = (b^{3^{n-1}})$, as asserted.

Let $\bar{G}_n = G_n/N_n = \bar{A}\bar{B}$, where $\bar{A} = (\bar{a})$, $\bar{B} = (\bar{b})$ are the residues of A, B in $\bar{G}_n$. If $\bar{t}$ is the residue of t in $\bar{G}_n$, $\bar{G}_n$ is defined by the relations

$$\bar{a}^h = 1, \quad \bar{t}^{k/3} = 1, \quad \bar{a}\bar{t}\bar{a}^{-1} = \bar{t}^{-4}, \quad \text{and} \quad \bar{b} = \bar{t}\bar{a}^2. \tag{20}$$

Clearly no subgroup of $\bar{B}$ is normal in $\bar{G}_n$, and hence its nucleus $\bar{N}_n$ is contained in $\bar{A}$. By a calculation similar to the preceding, one can show that $\bar{N}_n = (\bar{a}^{h/3})$.

Now let $\tilde{G}_n = \bar{G}_n/\bar{N}_n = \tilde{A}\tilde{B}$ where $\tilde{A} = (\tilde{a})$, $\tilde{B} = (\tilde{b})$, and $\tilde{t}$ are the residues of $\bar{A}$, $\bar{B}$, $\bar{t}$ in $\tilde{G}_n$. Consequently $\tilde{G}_n$ is defined by the relations

$$\tilde{a}^{h/3} = 1, \quad \tilde{t}^{k/3} = 1, \quad \tilde{a}\tilde{t}\tilde{a}^{-1} = \tilde{t}^{-4} \quad \text{and} \quad \tilde{b} = \tilde{t}\tilde{a}^2. \tag{21}$$

We see at once from these relations that $\tilde{G}_n \cong G_{n-1}$, and hence by induction $\tilde{G}_n$ is of type $2(n-1)$ with respect to A, B. It follows that G_n is of type $2n$ with respect to A, B, and the theorem is proved.

Bibliography

1. J. Douglas, *On finite groups with 2 independent generators* I, Proc. Nat. Acad. Sci. U.S.A. vol. 37 (1951) pp. 604–610.

2. ———, *On finite groups with 2 independent generators* IV, Proc. Nat. Acad. Sci. U.S.A. vol. 37 (1951) pp. 808–813.

3. D. Gorenstein, *On a problem of J. Douglas*, Project Document No. 10, Summer Mathematical Conference Reports, Bowdoin College, 1957.

4. ———, *Finite groups which admit an automorphism with few orbits*, to appear in the Canad. J. of Math.

5. D. Gorenstein, and I. N. Herstein, *A class of solvable groups*, Canad. J. Math. vol. 11 (1959) pp. 311–320.

6. N. Ito, *Products of abelian groups*, Math. Z. vol. 62 (1955) pp. 400–401.

Clark University and
Cornell University