ON THE STRUCTURE OF CERTAIN FACTORIZABLE GROUPS. II

DANIEL GORENSTEIN AND I. N. HERSTEIN

1. In [3], we have shown that in a finite AB-group G in which A and B are cyclic and A is its own normalizer, the commutator subgroup T of G is cyclic and $G=AT$ with $A\cap T=1$. This result can be used to determine the structure of arbitrary AB-groups in which A and B are cyclic.

If A is a subgroup of a group G, define the subgroup $N^i(A)$ of G inductively by the formula $N^i(A)=N_G(N^{i-1}(A))$, and denote by $N^*(A)$ the upper bound of the subgroups $N^i(A)$. Using this notation, we shall prove the following theorem concerning AB-groups:

THEOREM A. *Let G be a finite group of the form AB, where A and B are cyclic subgroups of G. Then G contains a unique cyclic normal subgroup T such that $G=N^*(A)T$ and $N^*(A)\cap T=1$. Moreover, if $N^*(A)=AB^*$ with $B^*\subset B$, then B^* and T commute elementwise.*

2. We begin with several lemmas:

LEMMA 1. *Let $G=AB$, with A and B cyclic, and assume that some subgroup B' of B is normal in G. Let $\overline{G}=G/B'=\overline{A}\overline{B}$, where $\overline{A}$, $\overline{B}$ are the images of A, B in $\overline{G}$. Then $N_G^*(A)B'$ is the complete inverse image of $N_{\overline{G}}^*(\overline{A})$ in G.*

PROOF. Let $B_0\subset B'$ with $o(B_0)=p$. Since B' is cyclic, B_0 is normal in G. If $B_0<B'$, set $\tilde{G}=G/B_0=\tilde{A}\tilde{B}$, and let $\tilde{B}'$ be the image of B' in $\tilde{G}$. Since $\overline{G}\cong\tilde{G}/\tilde{B}'$, it follows by induction on the order of G that the inverse image of $N_{\overline{G}}^*(\overline{A})$ in $\tilde{G}$ is $N_{\tilde{G}}^*(\tilde{A})\tilde{B}'$. Hence to prove the lemma, it suffices to show that $N(_{\tilde{G}}^*\tilde{A})^{-1}=N_G^*(A)B_0$. Thus without loss of generality we may assume $o(B')=p$.

Let $A=(a)$, $B=(b)$ and $B'=(b^r)$. It is clearly sufficient to prove by induction on i that if $b^u\in N^i(\overline{A})^{-1}$, then $b^u\in N^j(A)B'$ for some j. Now for some integer λ with $0<\lambda<p$, we have

$$(1) \qquad ab^ra^{-1} = b^{r\lambda}.$$

We treat the cases $\lambda=1$ and $\lambda>1$ separately. If $\lambda=1$, $B'\subset N(A)$. Now if $b^u\in N^i(\overline{A})^{-1}$, $\bar{b}^u\in N^i(\overline{A})$ and hence $\bar{b}^u\bar{a}\bar{b}^{-u}\in N^{i-1}(\overline{A})$. By induction $b^uab^{-u}\in N^j(A)B'$. If $j=0$, $b^uab^{-u}\in N^1(A)$ and consequently $b^u\in N^2(A)=N^2(A)B'$. If $j>0$, $N^j(A)B'=N^j(A)$, and so $b^u\in N^{j+1}(A)=N^{j+1}(A)B'$.

Received by the editors May 4, 1959.

If $\lambda>1$, it follows as above that $b^u ab^{-u}\in N^j(A)B'$. If $N^j(A)=AB_j$ and $B_j=(b^s)$, we have

$$b^u ab^{-u} = a^\alpha b^{s\beta} b^{r\gamma} \text{ for suitable integers } \alpha,\ \beta,\ \gamma. \tag{2}$$

Since $(\lambda - 1, p) = 1$, we can find an integer δ such that $\gamma + \delta\lambda \equiv \delta \pmod{p}$. We then have

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

whence $b^{u+r\delta}\in N^j(A)$. Thus $b^u\in N^j(A)B'$, and the lemma is proved.

LEMMA 2. *Let $G=AB$, with A and B cyclic. Then G contains a cyclic subgroup T, invariant under A, such that $G=N^*(A)T$ and $N^*(A)\cap T=1$.*

PROOF. Either a subgroup of A or a subgroup of B is normal in G (Douglas [1]). Let A_1 be the maximal subgroup of A normal in G, and assume first that $A_1\neq 1$. If $\overline{G}=G/A_1=\overline{A}\overline{B}$, we may assume by induction that $\overline{G}=N^*(\overline{A})\overline{T}$, where $N^*(\overline{A})\cap\overline{T}=1$, $\overline{T}$ is cyclic and invariant under $\overline{A}$. Clearly $N^*(A)=N^*(\overline{A})^{-1}$. If $T_0=\overline{T}^{-1}$, $G=N^*(A)T_0$ where $N^*(A)\cap T_0=A_1$ and T_0 is A-invariant.

If we let $G_0=AT_0=AB_0$ with $B_0\subset B$, it follows from our conditions that $N_{G_0}(A)=A$. The proof of Theorem A of [3] now implies that if $T=[G_0, G_0]$, then $T\subset T_0$, with T cyclic, $G_0=AT$ and $A\cap T=1$. It follows at once that $G=N^*(A)T$ with $N^*(A)\cap T=1$, T cyclic and invariant under A.

If $A_1=1$, we consider a minimal subgroup B' of B which is normal in G; and this time we set $\overline{G}=G/B'=\overline{A}\overline{B}$. By induction $\overline{G}=N^*(\overline{A})\overline{T}$, where $\overline{T}$ is cyclic, $\overline{A}$-invariant, and $N^*(\overline{A})\cap\overline{T}=1$. If $T_0=\overline{T}^{-1}$, it follows from Lemma 1 that $G=N^*(\overline{A})^{-1}T_0=N^*(A)B'T_0=N^*(A)T_0$, where $N^*(A)\cap T_0=B'$. Using the notation of Lemma 1, we consider the cases $\lambda=1$ and $\lambda>1$ separately.

If $\lambda=1$, set $G_0=AT_0$ and $\overline{G}_0=\overline{A}\overline{T}$. By Theorem A of [3], $\overline{T}=[\overline{G}_0, \overline{G}_0]$. Hence we can find a commutator t in T_0, which maps on a generator $\bar{t}$ of $\overline{T}$. Let $o(\overline{T})=m$ and suppose, if possible, that t has order mp. Since $o(T_0)=mp$, it follows that $T_0=(t)$, and consequently $T_0=[G_0, G_0]$. If $ata^{-1}=t^\sigma$, $[G_0, G_0]=(t^{\sigma-1})$, and hence $(\sigma-1, mp)=1$. But $t^m\in B'$ and, since $\lambda=1$, B' is in the center of G. Thus $t^m=at^m a^{-1}=t^{m\sigma}$, whence $p\mid(\sigma-1)$, a contradiction.

If $(t)=[G_0, G_0]$, we set $T=(t)$. Since $o(T)=m$, $T\cap B'=1$. Furthermore T is normal in G_0. We conclude at once that $G=N^*(A)T$, $N^*(A)\cap T=1$, T cyclic and invariant under A.

On the other hand, if $(t)<[G_0, G_0]$, we must have $T_0=[G_0, G_0]$. Since G_0 is an AB-group, its commutator subgroup T_0 is abelian (Ito

[4]). Now $o(T_0)=mp$ and we have just shown that T_0 contains no commutator of order mp. Therefore $p|m$.

Since T_0 is normal in G_0 and is generated by t and b^r, we have

$$ata^{-1} = t^\sigma b^{r\beta} \qquad \text{for suitable } \sigma, \beta. \tag{3}$$

It follows that $(\bar{t}^{\sigma-1})=[\overline{G}_0, \overline{G}_0]$ and hence that $(\sigma-1, m)=1$. Since $p|m$, there exists an integer α such that $\beta+\alpha\equiv\alpha\sigma \pmod p$. Consequently $a(tb^{r\alpha})a^{-1}=t^\sigma b^{r\beta}b^{r\alpha}=t^\sigma b^{r\alpha\sigma}=(tb^{r\alpha})^\sigma$. It follows that the subgroup $T=(tb^{r\alpha})$ is invariant under A. Since $o(T)=m$, $T\cap B'=1$, and we conclude at once that $G=N^*(A)T$, $N^*(A)\cap T=1$, T cyclic and invariant under A.

If $\lambda>1$, we set $T=[G_0, G_0]$. Since $T\subset T_0$, $N^*(A)\cap T\subset B'$. Suppose, if possible, that $B'\subset N^*(A)$, and let d be the least integer such that $B'\subset N^d(A)$. By definition of $N^d(A)$, $b^ra^{-1}b^{-r}\in N^{d-1}(A)$, and hence $ab^ra^{-1}b^{-r}=b^{r(\lambda-1)}\in N^{d-1}(A)$. Since $(\lambda-1, p)=1$, it follows that $b^r\in N^{d-1}(A)$, a contradiction. Thus $B'\cap N^*(A)=1$, and consequently $N^*(A)\cap T=1$. On the other hand, by Theorem A of [3], T is cyclic and $G_0=AT$. We conclude that in all cases G contains a cyclic subgroup T, invariant under A, such that $G=N^*(A)T$ and $N^*(A)\cap T=1$.

LEMMA 3. *Let $G=AB=N^*(A)T$ with $N^*(A)\cap T=1$, where T is cyclic and A-invariant and assume that $A\cap B=1$. If $N^*(A)=AB^*$ and $AT=AB_0$ with B^*, $B_0\subset B$, then $(o(B^*), o(B_0))=1$, $B=B^*\times B_0$, and $o(T)=o(B_0)$.*

PROOF. $G=N^*(A)T=(AB^*)T=(AB^*)(AT)=(AB^*)(AB_0)=A(B^*B_0)$. Since $A\cap B=1$, it follows that $B=B^*B_0$. On the other hand, $N^*(A)\cap T=1$, $N^*(A)\cap AT=A$, and hence $N^*(A)\cap B_0\subset A\cap B_0=1$. Thus $B^*\cap B_0=1$, whence $B=B^*\times B_0$. Since B^* and B_0 are subgroups of the cyclic group B, it also follows that $(o(B^*), o(B_0))=1$.

Finally let $T=(t)$, where $t=a^sb^r$ and let $o(T)=m$. Since $AT=AB_0$, it follows as in the proof of Theorem 10 of [2] that T consists of the elements $a^{sj}b^{rj}$, and since $A\cap B=1$, these elements must be distinct for $j=1, 2, \cdots, m$ and $a^{sm}b^{rm}=1$. Hence $b^{rm}=1$ and so $o(B_0)|m$. On the other hand, if $o(B_0)=n<m$, $a^nb^{rn}=a^{sn}\in A\cap T=1$, whence $a^{sn}b^{rn}=a^{sm}b^{rm}$, a contradiction. Thus $o(B_0)=o(T)$, as asserted.

LEMMA 4. *T is uniquely determined by the conditions $G=AB=N^*(A)T$ with $N^*(A)\cap T=1$, T cyclic and A-invariant.*

PROOF. Suppose T, T' are two subgroups of G satisfying the conditions of the lemma. Let $G_0=AT$ and $G_0'=AT'$. Since $A\cap T=1$,

$N_{G_0}(A)=A$, whence by Theorem A of [3], $T=[G_0, G_0]$, and similarly $T'=[G_0', G_0']$. Hence to prove the lemma, it clearly suffices to show that $G_0=G_0'$.

If $A\cap B\neq 1$, the equality of G_0 and G_0' follows readily by induction by considering $\overline{G}=G/A\cap B$; hence without loss of generality we may assume that $A\cap B=1$. If $G_0=AB_0$ and $G_0'=AB_0'$, it follows from Lemma 3 that $B=B^*\times B_0$ and $B=B^*\times B_0'$. Hence $o(B_0)=o(B_0')$. But B, being cyclic, has a unique subgroup of any given order. Thus $B_0=B_0'$ and $G_0=G_0'$.

3. Proof of Theorem A. In view of Lemmas 2 and 4 it suffices to prove that T commutes elementwise with B^*, for this will clearly imply that T is normal in G. In this section we treat the case $A\cap B=1$.

Let d be the least integer such that $N^{d+1}(A)=N^d(A)$, so that $N^*(A)=N^d(A)$. Let $N^i(A)=AB_i$ with $B_i=(b^{r_i})\subset B$, $i=1, 2, \cdots, d$. Then $B_1<B_2< \cdots <B_d$ and $B_d=B^*$. We may assume $r_i | r_{i-1}$, $i=2, 3, \cdots, d$. $N^{i-1}(A)$ is normal in $N^i(A)$ since $N^i(A)=N_G(N^{i-1}(A))$. Furthermore let $G_0=AT=AB_0$ with $B_0=(b^r)\subset B$ and $o(B_0)=m$. Then $T=(t)$, where $t=a^sb^r$ for some integer s.

If $s=0$, $T=B_0$, and it is obvious that T and B^* commute elementwise. Hence we may suppose $s\neq 0$ and without loss of generality that $s|h$, where $h=o(A)$. First of all, if $h<sm$, $a^hb^{rh/s}=b^{rh/s}\in T$, and generates a subgroup T_0, which is clearly invariant under B and hence is normal in G. It follows at once by considering G/T_0 and using induction on the order of G, that

$$b^{r_d}tb^{-r_d} = tb^{r(h/s)\beta} \qquad \text{for some integer } \beta. \tag{4}$$

If n denotes the order of B^*, we conclude at once from (4) that $t=b^{r_dn}tb^{-r_dn}=tb^{r(h/s)\beta n}$, whence

$$r(h/s)\beta n \equiv 0 \pmod{m}. \tag{5}$$

Since $(n, m)=1$ by Lemma 3,

$$r(h/s)\beta \equiv 0 \pmod{m} \quad \text{and} \quad b^{r_d}tb^{-r_d} = t, \text{ as desired.}$$

We may therefore assume that $h=sm$. For $i=1, 2, \cdots, d$ we have

$$b^{r_i}ab^{-r_i} = a^{u_{i-1}}b^{r_{i-1}v_{i-1}} \text{ for suitable integers } u_{i-1}, v_{i-1}, \text{ where } r_0 = 0. \tag{6}$$

Let G_i' be the commutator subgroup of $G_i=N^i(A)T$. We know that $T=(t)$ is the commutator subgroup of $G_0=AT$. Since $N^{i-1}(A)$ is normal in $N^i(A)$, and $G_i=N^i(A)B_0$, G_{i-1} is normal in G_i. It follows readily by induction that G_i' is generated by the elements a^{u_0-1},

$a^{u_1-1}b^{r_1v_1}, \cdots, a^{u_{i-1}-1}b^{r_{i-1}v_{i-1}}, t$. Furthermore G_i' is abelian since G_i is an AB-group for each i.

To prove that B^* and T commute elementwise, we have only to show that $b^{r_i}tb^{-r_i}=t$ on the assumption that $b^{r_{i-1}}tb^{-r_{i-1}}=t$. Now from the form of G_i', we have

$$b^{r_i}tb^{-r_i} = xt^\gamma \quad \text{where} \quad x \in N^{i-1}(A) \quad \text{and} \quad xt = tx. \tag{7}$$

Since by assumption $A\cap B=1$, Lemma 3 implies $o(T)=o(B_0)$, whence $t^m=1$. It follows now from (7) that $x^m=1$. Suppose for some $j>1$, $x\in N^j(A)$, $x\notin N^{j-1}(A)$. Let β be the least integer such that $x^\beta\in N^{j-1}(A)$. Since $N^{j-1}(A)$ is normal in $N^j(A)$ $\beta\mid [N^j(A): N^{j-1}(A)]$ and hence $\beta\mid o(B^*)=n$. But clearly $\beta\mid m$ since $x^m=1$. Since $(n, m)=1$, $\beta=1$ and so $x\in N^{j-1}(A)$, a contradiction. Thus $x\in A$ and (7) takes the form

$$b^{r_i}tb^{-r_i} = a^\rho t^\gamma, \qquad a^\rho t = ta^\rho. \tag{8}$$

Now $t=a^sb^r$ and $t^\gamma=a^{s\sigma}b^{r\sigma}$ for some integer σ, whence $b^{r_i}a^sb^{-r_i} =a^{\rho+s\sigma}b^{r(\sigma-1)}$. But this implies $b^{r(\sigma-1)}\in N^{i-1}(A)\cap B_0=1$, so that $\sigma\equiv 1 \pmod m$. Since $a^{sm}=1$, we may assume $\sigma=\gamma=1$, and hence that

$$b^{r_i}a^sb^{-r_i} = a^{\rho+s}, \qquad b^{r_i}tb^{-r_i} = a^\rho t. \tag{9}$$

In particular, (9) implies that $s\mid\rho$.

Since T is normal in AT, we have finally

$$ata^{-1} = t^\lambda \qquad \text{for some integer } \lambda. \tag{10}$$

In view of (6)

$$(b^{r_i}a)t(b^{r_i}a)^{-1} = (a^{u_i-1}b^{r_i+r_{i-1}v_{i-1}})t(a^{u_i-1}b^{r_i+r_{i-1}v_{i-1}})^{-1}. \tag{11}$$

Using (9) and (10) and our assumption that $b^{r_{i-1}}$ commutes with t, we conclude readily from (11) that

$$a^{\rho\lambda}t^\lambda = a^\rho t^{\lambda^{u_i-1}}. \tag{12}$$

Since $A\cap T=1$, $\rho(\lambda-1)\equiv 0 \pmod h$. Since $h=ms$ and $s\mid\rho$, we obtain

$$\frac{\rho}{s}(\lambda - 1) \equiv 0 \pmod m. \tag{13}$$

But T is the commutator subgroup of AT, which implies $(\lambda-1, m) =1$; and it follows from (13) that $\rho\equiv 0 \pmod h$. Hence $b^{r_i}tb^{-r_i}=t$, as desired. We conclude that B^* and T commute elementwise.

4. Finally we treat the case $A\cap B\neq 1$. Let $\overline{G}=G/A\cap B=\overline{A}\overline{B}$

$=N^*(\bar{A})\bar{T}$, where $\bar{A}$, $\bar{B}$, $\bar{T}$ are the images of A, B, T, in $\bar{G}$. Clearly $\bar{T}$ is cyclic, invariant under $\bar{A}$, and $N^*(\bar{A})\cap\bar{T}=1$. If $N^*(\bar{A})=\bar{A}\bar{B}^*$ with $\bar{B}^*\subset\bar{B}$, let $n=o(\bar{B}^*)$; and let $m=o(\bar{T})$. Since $\bar{A}\cap\bar{B}=1$, it follows from the preceding section that $(n, m)=1$ and that $\bar{B}$ commutes elementwise with $\bar{T}$. Furthermore $N^*(\bar{A})^{-1}=N^*(A)(A\cap B)=N^*(A)$, and hence B^* is the inverse image of $\bar{B}^*$ in G. If $B^*=(b^rd)$, it follows that

$$b^{rd}tb^{-rd} = xt, \quad x \in A \cap B, \quad \text{and} \quad b^{rdn} \in A \cap B. \tag{14}$$

Since $A\cap B$ is in the center of G, $x^m=1$. On the other hand (14) yields $t=b^{rdn}tb^{-rdn}=x^nt$, whence $x^n=1$. Since $(n, m)=1$, we conclude that $x=1$; 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. D. Gorenstein, *Finite groups which admits an automorphism with few orbits*, Canad. J. Math. vol. 12 (1960) pp. 73–100.

3. D. Gorenstein and I. N. Herstein, *On the structure of certain factorizable groups*. I, Proc. Amer. Math. Soc. vol. 10 (1959) pp. 940–945.

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

Clark University and
Cornell University