# GROUPS $\{S, T\}$ WHOSE COMMUTATOR SUBGROUPS ARE ABELIAN*

BY
H. R. BRAHANA

The groups generated by $S$ and $T$ satisfying the relations $S^3=T^2=(ST)^6=1$ were classified by Professor Miller.† The fact that makes these groups particularly easy to manage is that the commutator subgroups are abelian. It has been noted‡ that, with the exception of the tetrahedral group and the dihedral group of order 6, the only groups generated by an operator $S$ of order 3 and an operator $T$ of order 2 whose commutator subgroups are abelian are those considered by Miller. The groups which we shall consider are generated by $S$ and $T$ which satisfy the relations

$$S^p = T^2 = 1$$

where $p$ is a prime, and have abelian commutator subgroups. The groups generated by two operators of order two are the well known dihedral groups. In view of this fact and of Miller's paper we may assume that $p$ is a prime greater than 3.

1. Using the notation we have used before§ we let $\sigma_i=TS^{-i}TS^i$, $i=1, 2, \cdots, p-1$. We note that $T$ transforms $\sigma_i$ into its inverse and that $S$ transforms $\sigma_i$ into $\sigma_1^{-1}\sigma_{i+1}$. The group generated by the $\sigma$'s is therefore invariant; it is contained in the commutator subgroup $H$, and we shall show that it coincides with $H$.

Any operator of $\{S, T\}$ may be written in one of the forms

(1.1) $\sigma$,

(1.2) $\sigma T$,

(1.3) $\sigma \cdot TS^i$,

(1.4) $\sigma \cdot S^i$,

where $\sigma$ is an operator of the group $\{\sigma_1, \sigma_2, \cdots, \sigma_{p-1}\}$. For, multiplication on the right by $S$ puts (1.1) and (1.2) into (1.4) and (1.3) respectively, and either leaves the latter two in their present forms or puts one or both of them into

* Presented to the Society, August 31, 1932; received by the editors July 28, 1932.

† Quarterly Journal, vol. 33 (1901), pp. 76–79.

‡ American Journal of Mathematics, vol. 50 (1928), p. 347. The two groups of orders 6 and 12 should be excepted in that paper too.

§ Cf. the last reference.

(1.2) and (1.1) respectively. Multiplication on the right by $T$ interchanges the first two and interchanges the last two, for $\sigma \cdot TS^iT = \sigma TS^iTS^{-i} \cdot S^i = \sigma\sigma_i \cdot S^i$ and $\sigma S^iT = \sigma S^iTS^{-i}T \cdot TS^i = \sigma\sigma_{-i}^{-1} \cdot TS^i$.

Now let $Q = \sigma T^{a_0}S^{a_1}$ and $R = \sigma' \cdot T^{b_0}S^{b_1}$, where $\sigma$ and $\sigma'$ are two operators of $\{\sigma_1, \sigma_2, \cdots, \sigma_{p-1}\}$, $a_0$ and $b_0$ are either or both 0 or 1, and $a_1$ and $b_1$ are integers less than $p$, be any two operators of $\{S, T\}$. Their commutator $Q^{-1}R^{-1}QR$ may be reduced as follows:

$$
\begin{aligned}
\Sigma &= Q^{-1}R^{-1}QR \\
&= S^{-a_1}T^{a_0}\sigma^{-1} \cdot S^{-b_1}T^{b_0}\sigma'^{-1} \cdot \sigma T^{a_0}S^{a_1} \cdot \sigma' T^{b_0}S^{b_1} \\
&= S^{-a_1}T^{a_0}S^{-b_1}\sigma'' T^{b_0}\sigma'^{-1} \cdot \sigma T^{a_0}S^{a_1} \cdot \sigma' T^{b_0}S^{b_1}, \text{ where } \sigma'' = S^{b_1}\sigma^{-1}S^{-b_1}, \\
&= S^{-a_1}T^{a_0}S^{-b_1}T^{b_0}\sigma''' T^{a_0}S^{a_1} \cdot \sigma' T^{b_0}S^{b_1}, \text{ where } \sigma''' = \sigma''^{-1}\sigma'^{-1}\sigma, \\
&= S^{-a_1}T^{a_0}S^{-b_1}T^{b_0} \cdot T^{a_0}S^{a_1}\sigma^{iv}T^{b_0}S^{b_1}, \text{ where } \sigma^{iv} = S^{-a_1}T^{a_0}\sigma'''T^{a_0}S^{a_1} \cdot \sigma';
\end{aligned}
$$

$$
(1.5)\quad \Sigma = S^{-a_1}T^{a_0}S^{-b_1}T^{b_0} \cdot T^{a_0}S^{a_1}T^{b_0}S^{b_1} \cdot \sigma^v, \text{ where } \sigma^v = S^{-b_1}T^{b_0}\sigma^{iv}T^{b_0}S^{b_1}.
$$

Now if $a_0$ and $b_0$ are both zero, the right side of (1.5) is $\sigma^v$.

If $a_0 = b_0 = 1$, (1.5) becomes $\sigma_{a_1}^{-1}\sigma_{b_1}\sigma^v$.
If $a_0 = 0$, $b_0 = 1$, it becomes $\sigma_{a_1+b_1}^{-1} \cdot \sigma_{b_1}\sigma^v$.
If $a_0 = 1$, $b_0 = 0$, it becomes $\sigma_{a_1}^{-1}\sigma_{a_1+b_1} \cdot \sigma^v$.

So in any case $\Sigma$ is an operator of $\{\sigma_1, \sigma_2, \cdots, \sigma_{p-1}\}$.

In the above we have not assumed that $H$ was abelian nor that the order of $S$ was prime. Hence,

(1.6) *In any group $\{S, T\}$ the commutator subgroup is generated by commutators of $T$ and powers of $S$.*

2. We now assume that $H$ is abelian and that the order of $S$ is a prime number $p$. Since $T\sigma_iT = \sigma_i^{-1}$ it follows that $T$ is in $H$ only if $H$ is of order $2^m$ and type 1, 1, $\cdots$. Conversely, if $H$ is abelian, of order $2^m$, and type 1, 1, $\cdots$, $T$ is permutable with every operator of $H$, in which case $T$ may or may not be in $H$ as we shall see in a later section. We shall suppose hereafter, except where the contrary is explicitly stated, that $T$ is not in $H$.

If $S$ is in $H$ the group $\{S, T\}$ is generalized dihedral, being generated by an abelian group $H$ and an operator $T$ which transforms every operator of $H$ into its inverse. In fact $\{S, T\}$ must be the dihedral group of order $2p$. These two types of group are special and admit of special treatment. We shall then assume that neither $S$ nor $T$ is in $H$.

The quotient group of $\{S, T\}$ with respect to $H$ is necessarily abelian. It is generated by two operators of orders $p$ and 2 corresponding to $S$ and $T$ and therefore it must be cyclic and of order $2p$. The operator $(ST)^{2p}$ written

in terms of commutators* is

$$(ST)^{2p} = \sigma_{p-1}^{-1}\sigma_{p-2}^{-1}\sigma_{p-3}\sigma_{p-4}\cdots\sigma_1\sigma_{p-1}^{-1}\sigma_{p-2}^{-1}\sigma_{p-3}\cdots\sigma_1^{-1}.$$

Since $H$ is abelian this is identity. Hence,

(2.1) *If the abelian commutator subgroup contains neither $S$ nor $T$, then $(ST)$ is of order $2p$.*

3. We proceed to an examination of the $p-1$ $\sigma$'s which generate $H$. We note first a relation which has been used before:

$$\begin{aligned} S^{-1}\sigma_i S &= S^{-1}\cdot TS^{-i}TS^i\cdot S = S^{-1}TST\cdot TS^{-(i+1)}TS^{i+1} \\ &= \sigma_1^{-1}\sigma_{i+1}. \end{aligned} \tag{3.1}$$

In the same way we may obtain

$$S^{-k}\sigma_i S^k = \sigma_k^{-1}\cdot\sigma_{i+k}, \tag{3.2}$$

where $i$ and $k$ may take on all the values $0, 1, 2, \cdots, p-1$, and $i+k$ is reduced modulo $p$.

If in (3.2) we take $i$ to be 1 and allow $k$ to take on the values $1, 2, \cdots, p-1$ we get the set of $p$ conjugates of $\sigma_1$ under $S$. This set generates a group which contains $\sigma_i$ for every $i$. Hence we have

(3.3) *The group $H$ is generated by the set of conjugates of $\sigma_1$ under $S$.*

The $p-1$ $\sigma$'s generate $H$, (1.6), and consequently $H$ can have no more than $p-1$ independent generators. There must then be a relation connecting the $p$ conjugates of $\sigma_1$ under $S$. There may be a relation connecting a smaller number of these conjugates. If there is a relation connecting the first $m+1$ conjugates under $S$, viz. $\sigma_1, \sigma_1^{-1}\sigma_2, \sigma_2^{-1}\sigma_3, \cdots, \sigma_m^{-1}\sigma_{m+1}$, then $\sigma_{m+1}$ is in the group generated by the first $m$ $\sigma$'s. By (3.1) $\sigma_{m+2}$ can be expressed in terms of the preceding $\sigma$'s and hence in terms of the first $m$ $\sigma$'s. Therefore,

(3.4) *If $m+1$ is the smallest number of successive conjugates of $\sigma_1$ under $S$ so that the last one may be expressed in terms of the preceding ones, then $H$ has $m$ independent generators.*

The $p$ conjugates of $\sigma_1$ which by (3.3) generate $H$ are of course of the same order, the order of $\sigma_1$; we shall show also that the $p-1$ $\sigma$'s are of the same order.

Let the order of $\sigma_i$ be $n_i$. If in (3.2) we let $i=p-k$ we have

$$S^{-k}\sigma_{p-k}S^k = \sigma_k^{-1}\cdot\sigma_p = \sigma_k^{-1}. \tag{3.5}$$

This implies that $n_k=n_{p-k}$. If in (3.1) we let $i=1$, we have $S^{-1}\sigma_1^n S$

* Cf. the reference given in the third footnote in this paper.

$=\sigma_1^{-n}\sigma_2\sigma_1^{n}$. When $n=n_1$ this gives $\sigma_2\sigma_1^{n_1}=1$, and therefore $n_2$ is a divisor of $n_1$. Similarly, allowing $i$ in (3.1) to take on successively the values 2, 3, $\cdots$ it follows that $n_i$ is a divisor of $n_1$.

If in (3.2) we let $k=2$, and let $i$ take on successively the values 2, 4, 6, $\cdots$, $p-1$, we see in the same manner as above that $n_4$, $n_6$, $\cdots$, $n_{p-1}$ are divisors of $n_2$. By (3.5) we see that $n_{p-1}=n_1$, and since $n_2$ divides $n_1$ and $n_{p-1}=n_1$ divides $n_2$, it follows that $n_1=n_2=n_{p-1}=n_{p-2}$.

If in (3.2) we let $k=3$, and allow $i$ to take on the values 3, 6, $\cdots$, we find that $n_6$, $n_9$, $\cdots$ are divisors of $n_3$. One of the numbers $p-1$ and $p-2$ is divisible by 3 and therefore $n_1=n_{p-1}=n_{p-2}$ divides $n_3$, and $n_3=n_1$.

This induction may be completed by showing in the same manner that if $n_i=n_1$, for $i=1, 2, \cdots, k$, then $n_{k+1}=n_1$. Hence

(3.6) *If the order of $S$ is a prime and $H$ is abelian, the $\sigma$'s are all of the same order.*

4. In order to investigate the group $H$ it is convenient to consider the orders of the operators in the co-set $HS$. The order of $\sigma_i S$ may be obtained as follows:

$$(4.1)\qquad \begin{aligned}(\sigma_i S)^p &= \sigma_i S\cdot\sigma_i S\cdot\sigma_i S\cdots\sigma_i S\cdot\sigma_i S\\ &= S^p\cdot S^{-p}\sigma_i S^p\cdot S^{-(p-1)}\sigma_i S^{p-1}\cdots S^{-2}\sigma_i S^2\cdot S^{-1}\sigma_i S.\end{aligned}$$

By application of (3.2) this becomes

$$(\sigma_i S)^p = S^p\cdot\sigma_i\cdot\overset{-1}{\sigma_{p-1}}\sigma_{i+p-1}\cdot\cdots\cdot\sigma_2^{-1}\sigma_{i+2}\cdot\sigma_1^{-1}\sigma_{i+1}.$$

The $\sigma$'s with negative exponents are $\sigma_1, \sigma_2, \cdots, \sigma_{p-1}$. Those with positive exponents are $p$ in number including $\sigma_{i+p-i}=\sigma_p=1$. The remaining $p-1$ are $\sigma_1, \sigma_2, \cdots, \sigma_{p-1}$. Hence we have

$$(4.2)\qquad (\sigma_i S)^p = 1.$$

If we take the $p$th power of any operator of $HS$ we have

$$(4.3)\qquad (\overset{\alpha_1}{\sigma_1}\overset{\alpha_2}{\sigma_2}\cdots\overset{\alpha_{p-1}}{\sigma_{p-1}}S)^p = (\overset{\alpha_2}{\sigma_2}\overset{\alpha_3}{\sigma_3}\cdots\overset{\alpha_{p-1}}{\sigma_{p-1}}S)^p.$$

This is obtained by moving $\sigma_1^{\alpha_1}$ past successive $S$'s by means of (3.1) in the form $\sigma_i S=S\cdot\sigma_1^{-1}\sigma_{i+1}$. By repeated application of (4.3) we reduce the $p$th power of any element of $HS$ to (4.2) and hence obtain

(4.4) *Every operator in the co-set $HS$ is of order $p$.*

From this theorem we may draw many important conclusions concerning $H$ and $S$. We note first

(4.5) *Any operator of $H$ which is permutable with $S$ is of order $p$.*

From (4.5) and the fact that $T$ transforms every operator of $H$ into its inverse follows

(4.6) *The central of* $\{S, T\}$ *is identity.*

If $H$ contains operators of order $p$ then $\{\sigma_1\}$ contains operators of order $p$. If an operator of order $p$ in $\{\sigma_1\}$ is not invariant under $S$ the cyclic group generated by it is not invariant and contains no invariant operator except identity. Its conjugates generate a group of order $p^m$, $m \leqq p-1$, and type 1, 1, $\cdots$. This group contains $1+p+p^2+\cdots+p^{m-1}$ subgroups and at least one of them is invariant under $S$.

5. $H$ is the direct product of its Sylow subgroups, and each of its Sylow subgroups is invariant under $S$. Let the order of $H$ be $p^a p_1^{a_1} p_2^{a_2} p_3^{a_3} \cdots$, where the $p$'s are distinct primes. Then by (4.5) none of the Sylow subgroups corresponding to $p_i$, $i=1, 2, 3, \cdots$, can contain invariant operators. Hence

(5.1) *If the order of* $H$ *is* $p^a p_1^{a_1} p_2^{a_2} \cdots$, *where the* $p$*'s are distinct primes, each of the numbers* $p_i^{a_i}$ *is congruent to* 1, mod $p$.

If the residue of $p_i$, mod $p$, belongs to the exponent $p-1$, then the number $a_i$ must be at least $p-1$. The Sylow subgroup $H_{p_i}$ of order $p_i$ contains a characteristic subgroup composed of operators of order $p_i$ contained in subgroups generated by operators of highest order in $H_{p_i}$. When $p_i$ belongs to the exponent $p-1$ the order of this characteristic subgroup must be $p_i^{p-1}$, and therefore $H_{p_i}$ must contain $p-1$ independent generators of highest order.

If $\alpha_i$ is used to denote the exponent to which $p_i$ belongs, mod $p$, then $\alpha_i$ is a divisor of $p-1$. Replacing the exponent $p-1$ in the preceding paragraph by $\alpha_i$ we have the result that the number of independent generators of highest order of $H_{p_i}$ is a multiple of $\alpha_i$. Continuing the argument we observe that $H_{p_i}$ contains a characteristic subgroup generated by operators of order $p_i$ contained in cyclic subgroups of next to highest order in $H_{p_i}$. The order of this subgroup must also be a multiple of $p_i^{\alpha_i}$, and the number of independent generators of $H_{p_i}$ of next to highest order must be a multiple of $\alpha_i$. This argument may be continued to give

(5.2) *The number of independent generators of* $H_{p_i}$ *of each order for which there is one is a multiple of* $\alpha_i$, *the exponent to which* $p_i$ *belongs modulo* $p$.

6. The Sylow subgroup $H_{p_i}$ of $H$ is invariant under $H$, $S$, and $T$, and is therefore an invariant subgroup of $\{S, T\}$. The corresponding quotient group of $\{S, T\}$ is generated by two operators of orders $p$ and 2, and its commutator subgroup is abelian, being the quotient group of $H$ with respect to $H_{p_i}$. Moreover, any product of the $H_{p_i}$'s is invariant in $\{S, T\}$ and the corresponding quotient group is of the same type as $\{S, T\}$. Hence,

(6.1) *The existence of the group* $\{S, T\}$ *whose commutator subgroup is abelian and of order* $p^a p_1^{a_1} p_2^{a_2} \cdots$ *implies the existence of a group* $\{S', T'\}$ *whose commutator subgroup is abelian and of order* $p_i^{a_i}$ *for each* $i$.

From this theorem it follows that the question of the existence of a group $\{S, T\}$ with a given abelian group $H$ as a commutator subgroup must be concerned with the existence of groups $\{S, T\}$ whose commutator subgroups are Sylow subgroups of $H$. We shall show that the existence of $\{S, T\}$ follows from the existence of each of these groups whose commutator subgroups are prime power groups, thus proving the converse of (6.1).

Let $\{S', T'\}$ and $\{S'', T''\}$ be two groups whose abelian commutator subgroups $H'$ and $H''$ are of orders $p_1^{a_1}$ and $p_2^{a_2}$ respectively, where $p_1$ and $p_2$ are distinct primes, let $S'$ and $S''$ be of the same prime order $p$, and let $\sigma_1'$ and $\sigma_1''$ be commutators of the respective pairs of generators. Now let $H$ be the direct product of $H'$ and $H''$, and let $T$ be an operator of order 2 which transforms every operator of $H$ into its inverse. The group $\{H, T\}$ is generalized dihedral and its group of isomorphisms is abstractly the same as the holomorph of $H$.* The group of isomorphisms of $H$ is the direct product of the groups of isomorphisms of $H'$ and $H''$ and hence the holomorph of $H$ contains operators of order $p$. We wish to show that there is one such operator $S$ which with $T$ will generate a group having $H$ as a commutator subgroup. Let $S$ be an operator which transforms $H'$ and $H''$ as they are transformed by $S'$ and $S''$ respectively, and let $S^{-1}TS = T\sigma_1'\sigma_1''$. Then

$$\begin{aligned}
S^{-k}TS^k &= S^{-(k-1)}T\sigma_1'\sigma_1' S^{k-1} = S^{-(k-1)}TS^{k-1}\sigma_{k-1}^{\prime -1}\sigma_k'\sigma_{k-1}^{\prime\prime -1}\sigma_k'', \\
&= S^{-(k-1)}TS^{k-1}\Sigma_k, \text{ where } \Sigma_m = \sigma_{m-1}^{\prime -1}\sigma_m'\sigma_{m-1}^{\prime\prime -1}\sigma_m'', \\
&= S^{-(k-2)}TS^{k-2}\Sigma_{k-1}\Sigma_k, \\
&\quad \cdots\cdots\cdots\cdots \\
&= S^{-1}TS\Sigma_2 \cdots \Sigma_{k-1}\Sigma_k, \\
&= T\sigma_1'\sigma_1''\Sigma_2\Sigma_3 \cdots \Sigma_{k-1}\Sigma_k.
\end{aligned}$$

If $k = p$, we have

$$S^{-p}TS^p = T\sigma_1'\sigma_1''\Sigma_2\Sigma_3 \cdots \Sigma_{p-1}\Sigma_p.$$

Taking account of the definition of $\Sigma_m$ and of (4.1) and (4.2), we have $S^{-p}TS^p = T$. Since $S$ transforms $\{H, T\}$ according to an operator of order $p$ we may take $S$ to be of order $p$†. The group $\{S, T\}$ contains $\sigma_1'\sigma_1''$, and since the orders of $\sigma_1'$ and $\sigma_1''$ are relatively prime, contains both $\sigma_1'$ and $\sigma_1''$. The

* Miller, Blichfeldt, and Dickson, *Finite Groups*, p. 169.

† American Journal of Mathematics, vol. 52 (1930), p. 919.

group generated by the conjugates of $\sigma_1'\sigma_1''$ under $S$ contains the conjugates of $\sigma_1'$ and $\sigma_1''$ under $S'$ and $S''$ respectively and so is $H$, which by (1.6) is the commutator subgroup of $\{S, T\}$. Hence we have

(6.2) *The existence of two groups* $\{S', T'\}$ *and* $\{S'', T''\}$ *whose abelian commutator subgroups are of orders relatively prime and with* $S'$ *and* $S''$ *of the same prime order* $p$, *implies the existence of a group* $\{S, T\}$ *with* $S$ *of order* $p$ *and a commutator subgroup which is the direct product of the commutator subgroups of the two given groups.*

7. We consider next the subgroups $\{S', T'\}$ which have abelian commutator subgroups and are generated by an operator of order $p$ and one of order 2. Let $S'=\sigma_{p-1}^{l}S$ and $T'=\sigma_1^{k}T$. Then

$$
\begin{aligned}
\sigma_1' &= T'S'^{-1}T'S' = \sigma_1^{k}TS^{-1}\sigma_{p-1}^{-l}\sigma_1^{k}T\sigma_{p-1}^{l}S \\
&= \sigma_1^{k}TS^{-1}T\sigma_1^{-k}\sigma_{p-1}^{2l}S \\
&= \sigma_1^{k}TS^{-1}TS\cdot\sigma_1^{k}\sigma_2^{-k}\sigma_1^{-2l} \\
&= \sigma_1^{2k-2l+1}\sigma_2^{-k}.
\end{aligned} \tag{7.1}
$$

Let the order of $\sigma_1$ be $m$. When $m$ is odd $k$ may be chosen to be $m$ and then $l$ may be chosen so that $1-2l$ is any number less than or equal to $m$. Then (7.1) becomes $\sigma_1'=\sigma_1^{m'}$, where $m'$ is any number; hence $l$ may be chosen so that $m'$ is any divisor of $m$. If $m$ is even then for any choice of $k$ the number $2k-2l+1$ is still odd and for proper choice of $k$ and $l$ will be any odd divisor of $m$; or $k$ may be chosen as any even number and then $l$ may be chosen so that $2k-2l+1$ is any odd number less than $m$. If in the latter case $k$ is taken to be the highest power of 2 contained in $m$ and $l$ chosen so that $2k-2l+1$ is the largest odd divisor of $m$, then $\sigma_1'$ will be of even order. Hence,

(7.2) *If the order of* $H$ *is* $p^{\alpha}2^{a_1}p_1^{a_2}\cdots$, *then* $\{S, T\}$ *contains subgroups* $\{S', T'\}$ *whose commutator subgroups* $H'$ *have the orders* $2^{a_1}p_2^{k_2a_2}p_3^{k_3a_3}\cdots$, *where the* $k$*'s are zeros or ones independently.*

8. In the preceding pages we have determined various conditions on $H$ which are necessary in order that $H$ be the abelian commutator subgroup of $\{S, T\}$. The last conditions are conditions on the order of $H$. We wish to inquire what conditions on $H$ may be sufficient to determine $H$ so that a group $\{S, T\}$ necessarily exists containing $H$ as a commutator subgroup.

We proceed to prove the following fundamental theorem:

(8.1) *Necessary and sufficient conditions that there exist a group* $\{S, T\}$ *generated by* $S$ *of order* $p$ *and* $T$ *of order* 2 *and containing a given abelian group*

*$H$ as a commutator subgroup are* (1) *that the group of isomorphisms of $H$ contain an operator $U$ of order $p$ whose powers transform an operator $s_1$ of $H$ into a set of generators, and* (2) *that the product of the operators in the set of conjugates under $U$ which contains $s_1$ be identity.*

The conditions are necessary because of (3.3) and (4.2). Conversely, the group of isomorphisms of $H$ contains an operator of order 2 which transforms every operator of $H$ into its inverse; let $T$ be an operator of order 2 which performs this transformation. Let $S$ be an operator which transforms $H$ according to $U$ and which transforms $T$ into $Ts_1$. The order of $S$ has not yet been determined, but if its $p$th power transforms $T$ into itself it will be possible to require further that $S$ be of order $p$*. We therefore determine $S^{-p}TS^p$.

$$S^{-k}TS^k = S^{-(k-1)}Ts_1S^{k-1} = S^{-(k-1)}TS^{k-1}\cdot S^{-(k-1)}s_1S^{k-1}.$$

If we denote the successive conjugates of $s_1$ under $U$ as follows:

$$U^{-k}s_1U^k = s_{k+1},$$

we have

$$S^{-p}TS^p = Ts_1s_2\cdots s_{p-1}s_p.$$

If $s_1s_2\cdots s_{p-1}s_p=1$, then $S^p$ is permutable with $T$ and $S$ may be taken to be of order $p$, which completes the proof of the converse.

Since the two conditions above are sufficient to ensure the existence of $\{S, T\}$ it follows that the conditions stated in the preceding theorems hold; in particular (4.5) holds. The question arises as to whether or not (2) can be replaced by (4.5). The product of the set of conjugates of $s_1$ is of course invariant under $U$. If (4.5) holds and the order of $H$ is $q^n$, where $q$ is prime to $p$, this product must be identity. Hence,

(8.2) *If $H$ is abelian and of order $q^n$, where $q$ is prime to $p$, then condition* (1) *of* (8.1) *and* (4.5) *are necessary and sufficient that there exist a group $\{S, T\}$ having $H$ as a commutator subgroup.*

If the order of $H$ is $p$, it is obvious that condition (2) of (8.1) may not be replaced by (4.5), for the group of order $p^p$ and type 1, 1, $\cdots$ admits an automorphism $U$,

$$U^{-1}s_iU = s_{i+1},$$

such that $s_1$ and $U$ satisfy the given conditions. But since $H$ has $p$ independent generators it cannot be the commutator subgroup of any group $\{S, T\}$. The groups $H$ satisfying (1) of (8.1), (4.5), and having not more than $p-1$ inde-

* Cf. the second reference in §6.

pendent generators have been determined in another paper* and the groups in which we are interested will be found among them. They are of the two following categories:

(a) $H$ of order $p^{k_1 m+k_2(m-1)}$ with $k_1$ independent generators of order $p^m$ and $k_2$ of order $p^{m-1}$, where $k_1+k_2=p-1$ and $m \geqq 1$;

(b) $H$ of order $p^{k+2}$ and type 2, 1, 1, $\cdots$, where $k<p-2$.

In the case of the groups of the first category it is always possible to select $U$ so that conditions (1) and (2) of (8.1) hold. Let us suppose that $k_1=p-1$, so that $k_2=0$ and $H$ is of type $m, m, \cdots$. Let $s_1, s_2, \cdots, s_{p-1}$ be a set of independent generators of $H$, all necessarily of order $p^m$. Then the group of isomorphisms of $H$ contains an operator $U$ defined as follows:

$$
\begin{aligned}
U^{-1}s_iU &= s_{i+1}, \quad i = 1, 2, \cdots, p-2, \\
U^{-1}s_{p-1}U &= s_1^{-1}s_2^{-1}\cdots s_{p-1}^{-1}.
\end{aligned} \tag{8.3}
$$

It is obvious that the order of $U$ is $p$, and the product of the set of conjugates of $s_1$ under $U$ is identity.

The existence of a group $\{S, T\}$ for the $H$ just considered follows from (8.1). $H$ contains a subgroup $H'$ of order $p$ which is invariant in $\{S, T\}$. The quotient group of $\{S, T\}$ with respect to $H'$ is, by an argument similar to that used to establish (6.1), of the kind we are considering and its commutator subgroup is the quotient group of $H$ with respect to $H'$; it is of type $m, m, \cdots, m, m-1$. By taking successive quotient groups with respect to invariant subgroups of order $p$, we may obtain a group $\{\overline{S}, \overline{T}\}$ having any one of the groups of category (a) as a commutator subgroup.

The groups of category (b) do not admit of isomorphisms which with $H$ satisfy conditions (1) and (2) of (8.1). Let $H$ be of type 2, 1, 1, $\cdots$, and let $s_1$, an operator of $H$, be of order $p^2$. Then there exists an operator $U$ of order $p$ in the group of isomorphisms of $H$ which transforms $s_1$ into a set of generators.† Now $U^{-1}s_1U=s_1s_\alpha$, where $s_\alpha$ is some operator of $H$. Because of the type of $H$, $s_1^p$ must be invariant under $U$ and hence $s_\alpha$ is of order $p$ and may be taken to be $s_2$, one of a set of independent generators. We may then suppose the generators of $H$ to be chosen so that

$$
\begin{aligned}
U^{-1}s_1U &= s_1s_2, \\
U^{-1}s_iU &= s_{i+1}, \quad i = 2, 3, \cdots, k, \\
U^{-1}s_{k+1}U &= s_1^{a_p}s_2^{a_2}\cdots s_{k+1}^{a_{k+1}}.
\end{aligned} \tag{8.4}
$$

* *Prime-power abelian groups generated by a set of conjugates under a special automorphism*, to be published in the American Journal of Mathematics.

† Ibid., (5.64).

As was shown* in the paper referred to, the numbers $a_2, a_3, \cdots, a_{k+1}$ are completely determined by $k$. In considering successive conjugates of $s_1$ under $U$ we need only consider the powers of $s_1$ in these conjugates, as will be apparent at the conclusion. Each of the first $k+1$ conjugates contains $s_1$ to the first power. Successive ones thereafter have $s_1$ to the powers

$$(8.5)\qquad \begin{aligned} &1+ap,\\ &1+\left[1-\binom{r-1}{1}\right]ap,\\ &1+\left[1-\binom{r-1}{1}+\binom{r-1}{2}\right]ap, \end{aligned}$$

and so on, where $r=p-1-k$ and the numbers in the brackets are the binomial coefficients. The last one in the series (8.5) is

$$1+\left[1-\binom{r-1}{1}+\binom{r-1}{2}-\cdots+(-1)^{n-2}\binom{r-1}{r-2}\right]ap.$$

The sum of these numbers is readily obtained. We note first that

$$1-\binom{r-1}{1}+\binom{r-1}{2}-\cdots+(-1)^{i}\binom{r-1}{i}=(-1)^{i}\binom{r-2}{i}.$$

Then the coefficient of $ap$ in the sum will be

$$1-\binom{r-2}{1}+\binom{r-2}{2}-\cdots+(-1)^{r-2}\binom{r-2}{r-2},$$

which is $(1-1)^{n-2}=0$. Hence the sum is simply the sum of the $p$ numbers independent of $ap$, all of which are 1's. Therefore the product of the $p$ conjugates in the set which contains $s_1$, contains $s_1^p$, and cannot be identity† since the $s_i$'s are independent generators. Since any operator $U$ of order $p$ which transforms an operator $s_1$ of $H$ into a set of generators can be written in the form (8.4), and since the product of the set of conjugates of $s_1$ is not identity, it follows that no group $H$ of the second category is the commutator subgroup of a group $\{S, T\}$. We may then state the following theorem:

(8.6) *In order that there exist a group $\{S, T\}$ having a given abelian group $H$ of order $p^n$ as a commutator subgroup it is necessary and sufficient that* (1) $n=k_1m+k_2(m-1)$, (2) $k_1+k_2=p-1$, *and* (3) $H$ *have* $k_1$ *and* $k_2$ *independent generators of orders* $p^m$ *and* $p^{m-1}$ *respectively.*

* Ibid., (5.26).

† The product is exactly $s_1^p$, but it is not necessary to prove it here.

The corresponding theorem for the case where the order of $H$ is $q^n$, $q$ prime to $p$, is obtained from (8.2) and (3.2) of the paper referred to above.

(8.7) *In order that there exist a group* $\{S, T\}$ *having a given abelian group* $H$ *of order* $q^n$ *as a commutator subgroup, it is necessary and sufficient that* (1) $n = \alpha(k_1m_1+k_2m_2+\cdots+k_jm_j)$, *where* $\alpha$ *is the exponent to which* $q$ *belongs, mod* $p$, (2) $k_1+k_2+\cdots+k_j \leqq (p-1)/\alpha$, *and* (3) $H$ *have* $k_i\alpha$ *independent generators of order* $q^{m_i}$.

On the basis of a knowledge of the elementary part of the theory of abelian groups, theorems (6.2), (8.6), and (8.7) give a complete solution of the problem of the determination of the groups designated in the introduction.

UNIVERSITY OF ILLINOIS,
URBANA, ILL.