Chapter 10
Some Special Subgroups

In this section, we introduce the notion of commutator subgroup or derived subgroup of a group. This subgroup is important because it is the smallest normal subgroup such that the quotient group of the original group by this subgroup is abelian. Also, we study other special subgroup of a group called the maximum subgroup.

10.1 Commutators and Derived Subgroups

Let G be a group, and let $a, b \in G$. The *commutator* of a and b is $[a, b] = a^{-1}b^{-1}ab$.

"Commutator" is a good word to use: because $[a, b]$ is a kind of measure as to how near a to b come to commuting, $[a, b]$ being the identity element of G if and only if $ab = ba$. For any $a, b, c \in G$, we denote $[a, b, c] = \big[[a, b], c\big]$ and $b^a = a^{-1}ba$.

Theorem 10.1 *Let G be a group. For every $a, b, c \in G$, the following hold:*

(1) $[ab, c] = [a, c]^b[b, c]$;

(2) $[a, bc] = [a, c][a, b]^c$;

(3) $[a, b^{-1}, c]^b[b, c^{-1}, a]^c[c, a^{-1}, b]^a = 1$.

Proof (1) We can write

$$\begin{aligned}[ab, c] &= (ab)^{-1}c^{-1}abc = b^{-1}a^{-1}c^{-1}abc \\ &= b^{-1}(a^{-1}c^{-1}ac)b(b^{-1}c^{-1}bc) = [a, c]^b[b, c].\end{aligned}$$

(2) We have

$$\begin{aligned}[a, bc]\ a^{-1}(bc)^{-1}abc &= a^{-1}c^{-1}b^{-1}abc \\ &= (a^{-1}c^{-1}ac)c^{-1}(a^{-1}b^{-1}ab)c = [a, c][a, b]^c.\end{aligned}$$

B. Davvaz, *A First Course in Group Theory*,
https://doi.org/10.1007/978-981-16-6365-9_10

(3) We can write

$$\begin{aligned}[a, b^{-1}, c]^b &= b^{-1}\big[[a, b^{-1}], c\big]b = b^{-1}[a^{-1}bab^{-1}, c]b \\ &= b^{-1}(ba^{-1}b^{-1}ac^{-1}a^{-1}bab^{-1}c)b = (a^{-1}b^{-1}ac^{-1}a^{-1})(bab^{-1}cb) \\ &= (aca^{-1}ba)^{-1}(bab^{-1}cb).\end{aligned}$$

Hence, we have

$$[a, b^{-1}, c]^b = (aca^{-1}ba)^{-1}(bab^{-1}cb). \tag{10.1}$$

Similarly, we obtain

$$[b, c^{-1}, a]^c = (bab^{-1}cb)^{-1}(cbc^{-1}ac) \tag{10.2}$$

and

$$[c, a^{-1}, b]^a = (cbc^{-1}ac)^{-1}(aca^{-1}ba). \tag{10.3}$$

Now, by (10.1)–(10.3), the results follows. ■

It is perfectly natural to look at the set of all commutators in a group G. This subset may not form a subgroup of G, so we move to the next best thing.

Definition 10.2 Let G be a group. The subgroup generated by the set $\{[a, b] \mid a, b \in G\}$ is called the *commutator subgroup* or *derived subgroup* of G. It is denoted by G' or $G^{(1)}$ or $[G, G]$.

A group G is called *perfect* if $G = G'$.

Theorem 10.3 *If G is a group, then $G' \trianglelefteq G$ and G/G' is abelian.*

Proof For every $a, b, g \in G$, we have

$$\begin{aligned}[a^g, b^g] &= [g^{-1}ag, g^{-1}bg] = (g^{-1}ag)^{-1}(g^{-1}bg)^{-1}(g^{-1}ag)(g^{-1}bg) \\ &= (g^{-1}a^{-1}g)(g^{-1}b^{-1}g)(g^{-1}ag)(g^{-1}bg) \\ &= g^{-1}(a^{-1}b^{-1}ab)g = g^{-1}[a, b]g = [a, b]^g.\end{aligned}$$

So, we obtain $[a, b]^g = [a^g, b^g]$. Now let $x \in G'$ be an arbitrary element. Then, we can write $x = \prod_{i=1}^{n} [a_i, b_i]$, where $a_i, b_i \in G$ for all $1 \leq i \leq n$. Therefore, we have

$$g^{-1}xg = \Big(\prod_{i=1}^{n}[a_i, b_i]\Big)^g = \prod_{i=1}^{n}[a_i, b_i]^g = \prod_{i=1}^{n}[a_i^g, b_i^g] \in G'.$$

This shows that $G' \trianglelefteq G$.

Now, let aG' and bG' be arbitrary elements of G/G'. Since $a^{-1}b^{-1}ab \in G'$, it follows that $abG' = \big(a^{-1}b^{-1}\big)^{-1}G'$, or equivalently $aG'bG' = bG'aG'$, and so G/G' is abelian. ■

Theorem 10.4 *Let G be a group and N be a normal subgroup of G. Then, G/N is abelian if and only if $G' \leq N$.*

Proof Suppose that G/N is abelian. Then, for every $a, b \in G$, we have $aNbN = bNaN$. This implies that $abN = baN$, or equivalently $a^{-1}b^{-1}ab \in N$. Since N contains every commutator $[a, b]$, it follows that $G' \leq N$.

Conversely, let $G' \leq N$, and assume that aN and bN are arbitrary elements of G/N. Since $a^{-1}b^{-1}ab \in G'$, it follows that $a^{-1}b^{-1}ab \in N$. Hence, we have $abN = baN$. This means that $aNbN = bNaN$, and so we conclude that G/N is abelian. ■

Definition 10.5 A group G is called *metabelian* if there exists a normal subgroup N of G such that both N and G/N are abelian.

Theorem 10.6 *A group G is metabelian if and only if $G'' = \{e\}$.*

Proof Let G be a metabelian group; we show that $G'' = \{e\}$. Since G is metabelian, it has a normal abelian subgroup N, and G/N is abelian. Thus, by Theorem 10.4, $G' \leq N$. Since N is abelian, it follows that G' is abelian, and so $G'' = \{e\}$.

Conversely, suppose that $G'' = \{e\}$. We show that G is metabelian. It is clear that if G is abelian, then G is metabelian. So, we have only to consider the case where G is not abelian, and hence $G' \neq \{e\}$. Thus, assume that G is not abelian. By Theorem 10.3, we know that G' is a normal subgroup of G. Let $a, b \in G'$. We know that $aba^{-1}b^{-1} = e$ since $G'' = \{e\}$ and so we have that $ab = ba$. Thus, arbitrary elements $a, b \in G'$ commute, and so $G' \neq \{e\}$ is a normal abelian subgroup of G. Again, by Theorem 10.3, G/G' is abelian, and so G is metabelian. ■

Theorem 10.7 *Let G be a group such that G' is a subset of the center of G. Then, $[a, bc] = [a, b][a, c]$, for all $a, b, c \in G$.*

Proof We can write

$$\begin{aligned}[a, bc] &= a^{-1}(bc)^{-1}abc = a^{-1}c^{-1}(ac)(c^{-1}a^{-1})b^{-1}abc \\ &= (a^{-1}c^{-1}ac)c^{-1}(a^{-1}b^{-1}ab)c = [a, c]c^{-1}[a, b]c.\end{aligned}$$

Since $[a, b] \in G'$ and $G' \subseteq Z(G)$, it follows that $[a, b] \in Z(G)$. So, we conclude that $[a, b]c = c[a, b]$. Consequently, we get $[a, bc] = [a, c][a, b] = [a, b][a, c]$. This completes the proof. ■

More generally, for subgroups H and K of a group G, we denote $[H, K]$ the subgroup of G generated by the set $\{[h, k] \mid h \in H \text{ and } k \in K\}$.

Theorem 10.8 *If G is a group and H, K are subgroups of G, then*

(1) $[H, K] = [K, H]$;
(2) $[H, K] \trianglelefteq H \vee K$.

Proof (1) Let $[h, k]$ be an arbitrary commutator in $[H, K]$. Then, we have

$$[h, k] = h^{-1}k^{-1}hk = \left(k^{-1}h^{-1}kh\right)^{-1} = [k, h]^{-1}.$$

Since $[K, H] \leq G$ and $[k, h] \in [K, H]$, it follows that $[k, h]^{-1} \in [K, H]$. This implies that $[h, k] \in [K, H]$. So, we have $[H, K] \subseteq [K, H]$. In a similar way, we obtain $[K, H] \subseteq [H, K]$. Therefore, we conclude that $[H, K] = [K, H]$.

(2) Since $H \vee K$ is the subgroup generated by $H \cup K$, it follows that $[h, k] \in H \vee K$, for all $h \in H$ and $k \in K$. This shows that $[H, K]$ is a subgroup of $H \vee K$. Now, let $[h, k]$ be an arbitrary commutator in $[H, K]$ and $x \in H$. Then, by Theorem 10.1 (1), we have $[hx, k] = [h, k]^x[x, k]$, and so $[h, k]^x = [hx, k][x, k]^{-1}$. Since $[hx, k]$ and $[x, k]^{-1}$ belong to $[H, K]$, it follows that $[h, k]^x \in [H, K]$. Also, let $y \in K$, then by Theorem 10.1 (2), we can write $[h, ky] = [h, y][h, k]^y$, and hence $[h, k]^y = [h, y]^{-1}[h, ky]$. Since $[h, y]^{-1}$ and $[h, ky]$ lies in $[H, K]$, it follows that $[h, k]^y \in [H, K]$. Therefore, we conclude that $[H, K] \trianglelefteq H \vee K$. ■

Theorem 10.9 *If G is a group and H, K are normal subgroups of G, then $[H, K] \leq H \cap K$.*

Proof Suppose that $h \in H$ and $k \in K$ are arbitrary. Since $H \trianglelefteq G$, it follows that $h^{-1}(k^{-1}hk) \in H$. Similarly, since $K \trianglelefteq G$, it follows that $(h^{-1}k^{-1}h)k \in K$. Thus, we obtain $[h, k] \in H \cap K$. Consequently, we have $[H, K] \leq H \cap K$. ■

Theorem 10.10 *If H, K, and N are normal subgroups of a group G, then $[HK, N] = [H, N][K, N]$.*

Proof Assume that $a \in H$, $b \in K$ and $c \in N$. Then, by Theorem 10.1 (1), we can write

$$[ab, c] = [a, b]^b[b, c] = [a^b, c^b][b, c]. \tag{10.4}$$

Since H and N are normal subgroups of G, it follows that $[a^b, c^b] \in [H, N]$. On the other hand, we have $[b, c] \in [K, N]$. Now, by (10.4), we conclude that $[HK, N] \subseteq [H, N][K, N]$.

Conversely, since H and K are subgroups of HK, it follows that

$$[H, N] \subseteq [HK, N] \text{ and } [K, N] \subseteq [HK, N].$$

Consequently, we get $[H, N][K, N] \subseteq [HK, N]$, and this completes the proof. ■

Exercises

1. Let G be a group and H be a cyclic subgroup of G. If $G' \leq H$, show that $H \trianglelefteq G$.
2. For any group G, show that G' is the subset of all "*long commutators*":

$$G' = \{a_1 a_2 \dots a_n a_1^{-1} a_2^{-1} \dots a_n^{-1} \mid a_i \in G \text{ and } n \geq 2\}.$$

   Hint: $(aba^{-1}b^{-1})(cdc^{-1}d^{-1}) = a(ba^{-1})b^{-1}c(dc^{-1})d^{-1}a^{-1}(ab^{-1})bc^{-1}(cd^{-1})d$.
3. Let G be a group and suppose that H and K are subgroups of G. Prove that
   (1) $H \trianglelefteq G$ if and only if $[H, G] \leq H$;
   (2) If K is a subgroup of H and $K \trianglelefteq G$, then $[H, G] \leq K$ if and only if $H/K \leq Z\big(G/K\big)$.
4. Let $G = HK$, where H and K are abelian subgroups of G. Prove that G' is abelian.
5. Let N be a normal subgroup of a group G such that $N \cap G' = \{e\}$. Show that $N \leq Z(G)$.
6. If H is a subgroup of a metabelian group G, prove that H is metabelian.

10.2 Derived Subgroups of Some Special Groups

In this section, we investigate the derived subgroups of symmetric groups, alternating groups, quaternion group, general linear groups, special linear groups, and dihedral groups.

Lemma 10.11 *Let $n \geq 5$ and $N \trianglelefteq A_n$. If N contains a cycle of length 3, then $N = A_n$.*

Proof Suppose that $(x\ y\ z) \in N$. By Theorem 5.43, each permutation in A_n is a product of cycles of length 3. Hence, it suffices to prove that every cycle of length 3 lies in N. Assume that $(a\ b\ c) \in S_n$ is an arbitrary cycle. Take $\sigma \in S_n$ such that $x\sigma = a$, $y\sigma = b$ and $z\sigma = c$. Then, we have $\sigma^{-1}(x\ y\ z)\sigma = (a\ b\ c)$.

If $\sigma \in A_n$, then $(a\ b\ c) \in N$, because $N \trianglelefteq A_n$.

If $\sigma \notin A_n$, then σ is an odd permutation. Since $n \geq 5$, we can consider r and s distinct from x, y, and z. So, we have $(r\ s)\sigma \in A_n$. Consequently, we have $\big((r\ s)\sigma\big)^{-1}(x\ y\ z)(r\ s)\sigma \in N$, or equivalently $\sigma^{-1}(r\ s)(x\ y\ z)(r\ s)\sigma \in N$. Since $(r\ s)$ and $(x\ y\ z)$ are disjoint cycles, it follows that $\sigma^{-1}(x\ y\ z)\sigma \in N$. This shows that $(a\ b\ c) \in N$. ■

Theorem 10.12 *For all $n \geq 2$, $S_n' = A_n$.*

Proof Let $n \geq 2$ and suppose that σ and τ are two arbitrary permutations in S_n. Let $\sigma = \sigma_1\sigma_2 \dots \sigma_r$ and $\tau = \tau_1\tau_2 \dots \tau_s$, where σ_i's and τ_i's are transpositions. Then, we have

$$[\sigma, \tau] = \sigma^{-1}\tau^{-1}\sigma\tau = \sigma_r \dots \sigma_2\sigma_1\tau_s \dots \tau_2\tau_1\sigma_1\sigma_2 \dots \sigma_r\tau_1\tau_2 \dots \tau_s.$$

Hence, $[\sigma, \tau]$ is a product of $2(r + s)$ transpositions, and so it is an even permutation. This shows that $[\sigma, \tau] \in A_n$. Therefore, we conclude that $S'_n \leq A_n$.

Now, in order to show that $A_n = S'_n$, we consider the following cases:

Case 1: $n = 2$. In this case, clearly, we have $S'_n = A_2 = \{id\}$.

Case 2: $n = 3$. We have $A_3 = \{id,\ (1\,2\,3),\ (1\,3\,2)\}$. Since there are permutations in S_3 that don't commute, it follows that the derived subgroup is not just $\{id\}$. Hence, it must be all of A_3.

Case 3: $n = 4$. For distinct $i, j, k \in \{1,\ 2,\ 3,\ 4\}$, we have

$$[(i\ j), (i\ k)] = (i\ j)(i\ k)(i\ j)(i\ k) = (i\ j\ k)^2 = (i\ k\ j),$$

that is, every cycle of length 3 belongs to derived subgroup. Therefore, we conclude that $S'_4 = A_4$.

Case 4: $n \geq 5$. We know that S'_n is a normal subgroup of S_n. Moreover, we proved that $S'_n \leq A_n$. On the other hand, we have

$$[(1\,2), (2\,3)] = (1\,2)(2\,3)(1\,2)(2\,3) = (1\,2\,3) \in S'_n.$$

This means that S'_n contains a cycle of length 3, and so by Lemma 10.11, we deduce that $S'_n = A_n$. ■

Theorem 10.13 *We have*

(1) $A'_2 = A'_3 = \{id\}$;
(2) $A'_4 = \{id,\ (1\,2)(3\,4),\ (1\,3)(2\,4),\ (1\,4)(2\,3)\}$;
(3) $A'_n = A_n$, *for all* $n \geq 5$.

Proof (1) It is straightforward.

(2) Assume that $N = \{id,\ (1\,2)(3\,4),\ (1\,4)(2\,3),\ (1\,3)(2\,4)\}$. It can be checked that N is a normal subgroup of A_4. Since $|A_4/N| = 3$, it follows that A_4/N is abelian, and so by Theorem 10.4, we have $A'_4 \leq N$. Since A_4 is non-abelian, it follows that $A'_4 \neq \{id\}$. Hence, there exists a non-identity permutation $(a\ b)(c\ d)$ in A'_4. Since $A'_4 \trianglelefteq A_4$ and every product of disjoint transpositions are conjugate in A_4, we conclude that $A'_4 = N$.

(3) Since $A'_n \trianglelefteq A_n$, by Lemma 10.11, it is enough to prove that A'_n contains a cycle of length 3. Since $n \geq 5$, assume that $\sigma = (a\ c\ b)$ and $\tau = (b\ c)(d\ e)$. Then, we have $[\tau\ \sigma] = \tau^{-1}\sigma^{-1}\tau\sigma = (\tau^{-1}\sigma^{-1}\tau)\sigma$. Also, we have

$$\tau^{-1}\sigma^{-1}\tau = \tau^{-1}(a\ b\ c)\tau = (a\tau\ b\tau\ c\tau) = (a\ c\ b) = \sigma.$$

Consequently, we obtain $[\tau, \sigma] = \sigma^2 = (a\ b\ c)$ as desired. ■

Theorem 10.14 *If Q_8 is the quaternion group, then $Q_8' = \{1, 1\}$.*

Proof We know that $Q_8 = \{1, -1, I, -I, J, -J, K, -K\}$. The commutator subgroup contains the element

$$[I, J] = I^{-1}J^{-1}IJ = (-I)(-J)IJ = (IJ)(IJ) = K^2 = -1.$$

Similarly, $[J, K] = -1$ and $K, I] = -1$. On the other hand, 1 and -1 commute with all elements of Q_8, hence $[a, -1] = [a, 1] = 1$, for all $a \in Q_8$. Therefore, the commutator subgroup is the subgroup of Q_8 generated by -1 and 1, which is $Q_8' = \{1, 1\}$. ■

Theorem 10.15 *Let $\mathbb{F}$ be a field and $n \geq 2$ be an integer. Then,*

$$SL_n(\mathbb{F})' = GL_n(\mathbb{F})' = SL_n(\mathbb{F}),$$

except when $n = 2$ and $\mathbb{F}$ consists of 2 or 3 elements. Thus, $SL_n(\mathbb{F})$ is perfect (with the exceptions listed).

Proof Let A and B are two arbitrary matrices in $GL_n(\mathbb{F})$. Then, we have $A^{-1}B^{-1}AB \in GL_n(\mathbb{F})'$. Since

$$\det(A^{-1}B^{-1}AB) = \det(A^{-1})\det(B^{-1})\det(A)\det(B) = 1,$$

it follows that $A^{-1}B^{-1}AB \in SL_n(\mathbb{F})$. This yields that $GL_n(\mathbb{F})' \subseteq SL_n(\mathbb{F})$. On the other hand, since $SL_n(\mathbb{F}) \subseteq GL_n(\mathbb{F})$, it follows that $SL_n(\mathbb{F})' \subseteq GL_n(\mathbb{F})'$. So, we have $SL_n(\mathbb{F})' \subseteq GL_n(\mathbb{F})' \subseteq SL_n(\mathbb{F})$. Consequently, it is enough to show that $SL_n(\mathbb{F})' = SL_n(\mathbb{F})$. To establish this equality, by Theorem 7.41, it is enough to show that each matrix of the form $E_{ij}(\lambda)$ with $i \neq j$ and $\lambda \in \mathbb{F}^*$, is a product of commutators. It is easy to check that for any distinct indices i, j, k,

$$[E_{ik}(\lambda), E_{kj}(1)] = E_{ik}(-\lambda)E_{kj}(-1)B_{ik}(\lambda)E_{kj}(1) = E_{ij}(\lambda).$$

his expresses each $E_{ij}(\lambda)$ as a commutator when $n \geq 3$. For $n = 2$, we have

$$\begin{aligned}\left[\begin{bmatrix} a^{-1} & 0 \\ 0 & a \end{bmatrix}, \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}\right] &= \begin{bmatrix} a^{-1} & 0 \\ 0 & a \end{bmatrix}^{-1} \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}^{-1} \begin{bmatrix} a^{-1} & 0 \\ 0 & a \end{bmatrix} \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix}^{-1} \begin{bmatrix} 1 & -b \\ 0 & 1 \end{bmatrix}^{-1} \begin{bmatrix} a^{-1} & 0 \\ 0 & a \end{bmatrix} \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & b(1-a^2) \\ 0 & 1 \end{bmatrix}.\end{aligned}$$

So, if $\mathbb{F}$ contains an element a such that $a \neq 0$ and $a^2 \neq 1$, then we can express any matrix $E_{12}(\lambda)$ as a commutator by taking $b = (1 - a^2)^{-1}\lambda$, and similarly for $E_{21}(\lambda)$.

This yields that $SL_n(\mathbb{F})' = SL_n(\mathbb{F})$ except when $n = 2$ and $a^3 = a$, for all $a \in \mathbb{F}$, and this happens only when $|\mathbb{F}| = 2$ or 3. ■

Theorem 10.16 *If D_n is the dihedral group of order $2n$, then by Corollary 7.74, we have $D_n = \langle R, S\rangle$, where S is a reflection and R is a rotation. Then, $D'_{2n} = \langle R^2\rangle$.*

Proof Since $[S, R]$ is $S^{-1}R^{-1}SR = SSRR = R^2$, it follows that R^2 is a commutator. Moreover, since $[S, R^i] = S^{-1}R^{-i}SR^i = SSR^iR^i = R^{2i}$, it follows that every element of $\langle R^2\rangle$ is a commutator. Now, we prove that every commutator belong to $\langle R^2\rangle$. Suppose that A and B are two arbitrary elements of D_{2n}. We consider the following cases:

Case 1: Both A and B are rotations. In this case, we can write $A = R^i$ and $B = R^j$, for some integers i and j. Since R^i and R^j commute, it follows that $[A, B] = I_n$.

Case 2: A is a rotation and B is a reflection. Then, we have $A = R^i$ and $B = R^jS$, for some integers i and j. Since $B = B^{-1}$, it follows that

$$[A, B] = A^{-1}B^{-1}AB = A^{-1}BAB = R^{-i}R^jSR^iR^jS = R^{j-i}SR^{i+j}S.$$

By Theorem 7.75, since $RS = SR^{-1}$, it follows that $[A, B] = R^{-2i} \in \langle R^2\rangle$.

Case 3: A is a reflection and B is a rotation. In this case, we have $[A, B]^{-1} = B^{-1}A^{-1}BA$. By the case (2), $[A, B]^{-1} \in \langle R^2\rangle$, and this implies that $[A, B] \in \langle R^2\rangle$.

Case 4: Both A and B are reflections. Then, we have $A = R^iS$ and $B = R^jS$. Hence, we obtain $A = A^{-1}$ and $B = B^{-1}$. So, we conclude that

$$\begin{aligned}[A, B] &= A^{-1}B^{-1}AB = ABAB = (AB)^2 = (R^iSR^jS)^2\\ &= (R^iR^{-j}SS)^2 = R^{2(i-j)} \in \langle R^2\rangle.\end{aligned}$$

This completes the proof. ■

Exercises

1. Compute $[GL_n(\mathbb{F}) : SL_n(\mathbb{F})]$, where $\mathbb{F}$ is finite.
2. Suppose that $O_n(\mathbb{F}) = \{A \in GL_n(\mathbb{F}) \mid A^tA = I_n\}$ and $SO_n(\mathbb{F}) = \{A \in O_n(\mathbb{F}) \mid \det(A) = 1\}$. Prove that $SO_n(\mathbb{F}) \trianglelefteq O_n(\mathbb{F})$ and compute $[O_n(\mathbb{F}) : SO_n(\mathbb{F})]$.
3. Determine the derived subgroup of $SO_n(\mathbb{F})$.

10.3 Maximal Subgroups

A maximal subgroup of a given group G is a proper subgroup of G, that is, a subgroup which is neither the identity nor G itself, and in order to be maximal, it can not be contained in a larger proper subgroup of G. More precisely:

Definition 10.17 A subgroup M of a group G is called a *maximal subgroup* if $M \neq G$ and the only subgroups containing M are M and G.

Example 10.18 We know that the subgroups of $\mathbb{Z}$ are of the form $n\mathbb{Z}$. Note that $n\mathbb{Z} \subseteq m\mathbb{Z}$ if and only if $m|n$, and so the maximal subgroups of $\mathbb{Z}$ are precisely $p\mathbb{Z}$ for p prime.

Example 10.19 In each Hasse diagram, the lower subgroup is a maximal subgroup in the upper one.

Theorem 10.20 *If H is a proper subgroup of a finite group G, then there is a maximal subgroup of G containing H.*

Proof If H is a maximal subgroup of G, then we have nothing to do. If H is not a maximal subgroup, we pick a proper subgroup H_1 of G such that $H \subset H_1$. Again, if H_1 is maximal in G,then we are done; otherwise, we pick a proper subgroup H_2 of G such that $H \subset H_1 \subset H_2$. Continuing in this way, we construct a chain of proper subgroups of G:

$$H \subset H_1 \subset H_2 \subset \ldots,$$

and this gives a strictly increasing chain of integers

$$|H| < |H_1| < |H_2| < \ldots,$$

which is bounded above by $|G|$, and so must terminate. Consequently, we obtain a maximal subgroup containing H. ■

We conclude that in non-trivial finite groups, maximal subgroups will always exist. However, not all groups will have maximal subgroups.

Example 10.21 The rational numbers $\mathbb{Q}$ under addition have no maximal subgroups. To see the reason, suppose that M is a maximal subgroup of $\mathbb{Q}$. There exists a rational number r/s ($r, s \in \mathbb{Z}$ and $s \neq 0$) such that $r/s \notin M$. Since $\mathbb{Z}$ is a proper subgroup of $\mathbb{Q}$, it follows that $M \neq \{0\}$. Let $m/n \in M$ with $m, n \in \mathbb{Z}$ and $mn \neq 0$. Since $m/n \in M$, it follows that $nm/n \in M$, and so $m \in M$. Since M is a maximal subgroup, it follows that

$$M + \langle r/s \rangle = \mathbb{Q}. \tag{10.5}$$

Consider $r/sms \in \mathbb{Q}$. Then, by (10.5), there exist $h \in M$ and $t \in \mathbb{Z}$ such that $r/sms = h + tr/s$. Hence, we have $r/s = msh + tmr = m(sh + tr)$. Since $m \in M$, it follows that $r/s \in M$. This is a contradiction.

Theorem 10.22 *The center of a group G is properly contained in every maximal subgroup of G having a composite index.*

Proof Let M be a maximal subgroup of G with composite index. Suppose that $Z(G)$ is not contained in M. Then, there exists $a \in Z(G)$ such that $a \notin M$. We consider

$\langle M, a\rangle$, the subgroup generated by $M \cup \{a\}$. Since M is a maximal subgroup and $M \subset \langle M, a\rangle$, it follows that $\langle M, a\rangle = G$. Assume that $x \in G$ is an arbitrary element. Since $a \in Z(G)$, it follows that $x = a^k b$, for some $b \in M$ and $k \in \mathbb{Z}$. Now, for every $y \in M$, we have

$$xyx^{-1} = (a^k b)y(a^k b)^{-1} = a^k byb^{-1}a^{-k} = byb^{-1},$$

because $a \in Z(G)$. Since $b, y \in M$, it follows that $byb^{-1} \in M$. This means that $xyx^{-1} \in M$, and so M is a normal subgroup of G. Since G/M has composite order, we conclude that G/M has a non-trivial subgroup, say H/M. Hence, $\{M\} \subset H/M \subset G/M$. This yields that $M \subset H \subset G$, and this is a contradiction with the maximality of M.

Note that if $Z(G) = M$, then M is a normal subgroup of G and by the same arguments, we obtain a contradiction. ■

Lemma 10.23 *If an element of a group is not contained in any maximal subgroup, then the group is cyclic.*

Proof Suppose that G is a group and $x \in G$ with x is not in any maximal subgroup of G. Since x is not in any maximal subgroup, it follows that $\langle x\rangle$ is not maximal. Moreover, since x is not in any maximal subgroup, it follows that $\langle x\rangle$ is not a subset of any maximal subgroup. This yields that $\langle x\rangle = G$. ■

Theorem 10.24 *Let G be a finite group. If G has exactly one maximal subgroup, then the order of G is a power of a prime.*

Proof First, we show that G is cyclic. Assume that M is the unique maximal subgroup of G. Let $x \in G - M$. Then, the subgroup generated by x is contained in no maximal subgroup and hence is equal to G. Consequently, G is a cyclic group.

Clearly, we have $|G| > 1$. Assume that $|G|$ has more than one prime factor. Then, it may be written $|G| = p^k m$, where p is prime, k, m are positive integers and $(p, m) = 1$. Since G is cyclic, if k is a divisor of $|G|$, then G has a subgroup of order k. In particular, let $m = qr$ with q prime. So, G has a subgroup of order $p^k r$ and $p^{k-1}m$. Since $(p^k r, p^{k-1}m) = 1$, neither of these is a subgroup of the other. Since the order of each of these is less than that of order G, it follows that each of them is a proper subgroup of G. Since there are no proper divisors of $|G|$ greater than the order of either of these, no proper subgroup contains either of them. Therefore, we conclude that both of these are maximal subgroups. Since G is defined to have exactly one maximal subgroup, the assumption that $|G|$ has more than one prime factor must be invalid. ■

Theorem 10.25 *If a finite group has exactly two maximal subgroups, then it is a cyclic group.*

Proof Suppose that G is a finite group. Let M_1 and M_2 be the only distinct maximal subgroups of G. By Lagrange's Theorem, if a group is finite, the order of any of its

proper subgroups can be no greater than half the order of the group. So, we have $|M_1| \leq |G|/2$ and $M_2| \leq |G|/2$. Therefore, we can write

$$|M_1 \cup M_2| \leq |M_1| + |M_2| - 1 \leq |G|/2 + |G|/2 - 1 = |G| - 1 < |G|.$$

Consequently, there exists $x \in G$ such that $x \notin M_1 \cup M_2$. Hence, by Lemma 10.23, we conclude that G is cyclic. ■

If M is a maximal subgroup of a group G, then also every conjugate aMa^{-1} of M is maximal in G. Indeed, $aMa^{-1} \subset H < G$ implies that $M < a^{-1}Ha < G$. For this reason the maximal subgroups are studied up to conjugation.

Exercises

1. Let M be a maximal subgroup of a group G. Prove that if $M \trianglelefteq G$, then $[G : M]$ is finite and equal to a prime number.
2. Let G be the additive group consisting of all rational numbers. Prove that G contains no maximal subgroup.
3. Let G be a group in which each proper subgroup is contained in maximal subgroup of finite index in G. If every two maximal subgroups on G are conjugate in G, prove that G is a cyclic group.
4. If G is a perfect group and M is a maximal subgroup of G, prove that

   (1) M contains the center of G;
   (2) $M/Z(G)$ is maximal in $G/Z(G)$.

10.4 Worked-Out Problems

Problem 10.26 If $n \geq 5$, prove that A_n is the unique proper non-trivial normal subgroup of the symmetric group S_n.

Solution Suppose that N is a proper non-trivial normal subgroup of S_n and let σ be a non-identity permutation in N. Then, there exists i such that $i\sigma \neq i$. We choose $j \neq i,\ i\sigma$. Now, if $\tau = (i\ j)$, then $\alpha = \sigma\tau\sigma^{-1}\tau^{-1}$ is non-identity and lies in N. Moreover, α is a product of the transpositions $\sigma\tau\sigma^{-1}$ and τ. Consequently, it is either a cycle of length 3 or a permutation of the form $(a\ b)(c\ d)$. Since N is normal, it contains either all cycles of length 3 or all permutations of type $(a\ b)(c\ d)$. Therefore, by Theorem 5.43, we deduce that $N = A_n$. ■

Problem 10.27 The fact that the set of all commutators in a group need not be a subgroup is an old result; the following example is due to P.J. Cassidy (1979).

(a) Let $\mathbb{F}[x, y]$ denote the ring of all polynomials in two variables over a field $\mathbb{F}$, and let $\mathbb{F}[x]$ and $\mathbb{F}[y]$ denote the subrings of all polynomials in x and in y, respectively. Define G to be the set of all matrices of the form

$$A = \begin{bmatrix} 1 & f(x) & h(x,y) \\ 0 & 1 & g(y) \\ 0 & 0 & 1 \end{bmatrix},$$

where $f(x) \in \mathbb{F}[x]$ and $g(y) \in \mathbb{F}[y]$ and $h(x, y) \in \mathbb{F}[x, y]$. Prove that G is a multiplicative group and that G' consists of all those matrices for which $f(x) = 0 = g(y)$.

(b) If $(0, 0, h)$ is a commutator, show that there are polynomials $f(x), f'(x) \in \mathbb{F}[x]$ and $g(x), g'(x) \in \mathbb{F}[y]$ with $h(x, y) = f(x)g'(y) - f'(x)g(y)$.

(c) Show that $h(x, y) = x^2 + xy + y^2$ does not posses a decomposition as in part (b), and conclude that $(0, 0, h) \in G'$ is not a commutator.

solution (a) If A denoted by triple (f, g, h), then

$$(f, g, h)(f', g', h') = (f + f', g + g', h + h' + fg'). \tag{10.6}$$

Since G is a subset of a matrix group, we need only to check the subgroup axioms, i.e., it is not necessary to check the associativity. The operation in (10.6) shows that the multiplication of two elements of G is also in G. It is clear that $I_3 \in G$ with $f(x) = h(x, y) = g(y) = 0$. Moreover, if $f + f' = 0$, $g + g' = 0$ and $h + h' + fg' = 0$, then we get $f' = f$, $g' = -g$ and $h' = -h + fg$. This yields that the element $(-f, -g, -h + fg)$ is the inverse of (f, g, h). Hence, we conclude that G is a group.

If $h = h(x, y) = \sum a_{ij}x^i y^j$, then

$$(0, 0, h) = \prod_{i,j}[(a_{ij}x^i, 0, 0), (0, y^j, 0)].$$

This shows that G' consists of all those matrices for which $f(x) = 0 = g(y)$.

(b) Let $(0, 0, h)$ be a commutator. Then we can write

$$\begin{aligned}
&(0, 0, h) = (f, g, h_1)(f', g', h_2)(f, g, h_1)^{-1}(f', g', h_2)^{-1} \\
&= (f, g, h_1)(f', g', h_2)(-f, -g, -h_1 + fg)(-f', -g', -h_2 + f'g') \\
&= (f + f', g + g', h_1 + h_2 + fg')(-f - f', -g - g', -h_1 - h_2 + fg + f'g' + fg') \\
&= \big(0, 0, fg' + fg' + fg + f'g' + (f + f')(-g - g')\big) \\
&= (0, 0, fg' - f'g).
\end{aligned}$$

(c) If $f(x) = \sum b_i x^i$ and $f'(x) = \sum c_i x^i$, then there are equations

$$\begin{aligned}
&h(0, y) = f(0)g'(y) - f'(0)g(y), \\
&\frac{\partial}{\partial x}h(x, y)\Big|_{x=0} = \frac{\partial}{\partial x}f(x)\Big|_{x=0}g'(y) - g(y)\frac{\partial}{\partial x}f'(x)\Big|_{x=0}, \\
&\frac{\partial^2}{\partial x^2}h(x, y)\Big|_{x=0} = \frac{\partial^2}{\partial x^2}f(x)\Big|_{x=0}g'(y) - g(y)\frac{\partial^2}{\partial x^2}f'(x)\Big|_{x=0}.
\end{aligned}$$

Hence, we obtain the following three equations

$$\begin{aligned} b_0 g'(y) - c_0 g(y) &= y^2, \\ b_1 g'(y) - c_1 g(y) &= y, \\ b_2 g'(y) - c_2 g(y) &= 1. \end{aligned}$$

Considering $\mathbb{F}[x, y]$ as a vector space over $\mathbb{F}$, one obtains the contradiction that the independent set $\{1, y, y^2\}$ is in the subspace spanned by $\{g, g'\}$.

10.5 Supplementary Exercises

1. If N is a normal subgroup of the group G, prove that $(G/N)' = G'N/N$.
2. Let a and b be two elements of order m and n, respectively, in group G. Prove that if a and b both commute with $[a, b]$, and d is the greatest common divisor of m and n, then $[a, b]^d = e$.
3. Suppose that G is a group and $|G| = p^n$, where p is a prime number. If $[G : C_G(x)] \leq p$, for all $x \in G$, prove that
   (a) $C_G(x) \trianglelefteq G$, for all $x \in G$;
   (b) $G' \leq Z(G)$;
   (c) $|G'| \leq p$.
4. Let G be a subgroup of a group G. If $[H, G'] = e$, prove that $[H', G] = e$.
5. Let p be prime and let G be a non-abelian group of order p^3. Show that $Z(G) = [G, G]$ and this is a subgroup of order p.
6. Let $K \leq M < G$, with $K \trianglelefteq G$. Prove that M/K is a maximal subgroup of G/K if and only if M is a maximal subgroup of G.