

§24 Generators and Commutators

We introduce an important subgroup which distinguishes abelian factor groups from nonabelian ones. It is generated by the set of commutators. First we define 'generation'.

24.1 Definition: Let G be a group and let $X \subseteq G$. The intersection of all subgroups of G which contain X is called the *subgroup of G generated by X* and is denoted by $\langle X \rangle$.

Hence $\langle X \rangle = \bigcap_{X \subseteq H \leq G} H$. Here H runs through a nonempty set, since at least G is a subgroup of G that contains X . Note that $\langle \emptyset \rangle = 1$. When X is a finite set, for instance $X = \{x_1, x_2, \dots, x_n\}$, we write $\langle x_1, x_2, \dots, x_n \rangle$ rather than $\langle \{x_1, x_2, \dots, x_n\} \rangle$. In particular, if $X = \{x\}$ consists of a single element, then $\langle x \rangle = \langle \{x\} \rangle$ is the cyclic group generated by x , as we introduced in Definition 11.1. Definitions 11.1 and 24.1 are consistent, as will be proved in Lemma 24.2, below. Our notation $\langle \rho, \sigma \rangle$ for dihedral groups is also consistent with Definition 24.1.

When $K \leq G$ and $X \subseteq K$, then $\langle X \rangle \subseteq K$ by definition. So $\langle X \rangle$ is the smallest subgroup of G containing X . In particular, if $H \leq G$, then $\langle H \rangle = H$.

The elements of $\langle X \rangle$ are described in the next lemma. See also Ex. 1 at the end of this paragraph.

24.2 Lemma: *Let X be a nonempty subset of a group G . Then*

$$\langle X \rangle = \{x_1^{m_1} x_2^{m_2} \dots x_k^{m_k} \in G : k \in \mathbb{N}, x_i \in X \text{ and } m_i \in \mathbb{Z} \text{ for each } i = 1, 2, \dots, k\}.$$

Proof: Let Y be the set on the right hand side. We must show $Y \subseteq \langle X \rangle$ and $\langle X \rangle \subseteq Y$.

In order to prove $Y \subseteq \langle X \rangle$, we show that $Y \subseteq H$ for every $H \leq G$ such that $X \subseteq H$. This follows from the closure properties of subgroups. If $X \subseteq H$ and $H \leq G$, then, for any $x \in X$, there holds $x^n \in H$ for any $n \in \mathbb{N}$ since H is closed under multiplication, and also $x^n \in H$ for any $n \in \mathbb{Z}$ since H is closed under taking inverses and $x^0 = 1 \in H$. Hence, for any $k \in \mathbb{N}$, any $x_1, x_2, \dots, x_k \in X$, any $m_1, m_2, \dots, m_k \in \mathbb{Z}$, we have $x_1^{m_1}, x_2^{m_2}, \dots, x_k^{m_k} \in H$ and, from the closure of H under multiplication, we get $x_1^{m_1} x_2^{m_2} \dots x_k^{m_k} \in H$. Thus $Y \subseteq H$ whenever $X \subseteq H \leq G$. This proves $Y \subseteq \langle X \rangle$.

Now we show $\langle X \rangle \subseteq Y$. By definition of Y , we have $X \subseteq Y$ (take $k = 1$ and $m_1 = 1$). So $\langle X \rangle \subseteq Y$ will be proved if we show that Y is a subgroup of G . But Y is closed under multiplication (because k runs through \mathbb{N}) and under the forming of inverses (because $-m_i \in \mathbb{Z}$ when $m_i \in \mathbb{Z}$). So $X \subseteq Y \leq G$ and consequently $\langle X \rangle \subseteq Y$. \square

24.3 Remark: $\langle X \rangle$ consists of all finite products of elements in X and the inverses of the elements in X . Notice that the set Y of Lemma 24.2 does not change if the elements of X are replaced by their inverses. Thus $\langle X \rangle = \langle Z \rangle$, where $Z = \{x^{-1} \in G : x \in X\}$.

24.4 Definition: Let G be a group. If $X \subseteq G$ and $\langle X \rangle = G$, then X is called a *set of generators of G* , and G is said to be *generated by X* . If G has a finite set of generators, G is said to be a *finitely generated group*.

24.5 Examples: (a) If $x \in G$, then $\langle x \rangle = \{x^n : n \in \mathbb{Z}\}$ by Lemma 24.2. So $\langle x \rangle$ is the cyclic group generated by x as in Definition 11.1.

(b) Any element of the dihedral group D_{2n} can be written in the form $\rho^m \sigma^j$, where $m, j \in \mathbb{Z}$. Hence $D_{2n} = \langle \rho, \sigma \rangle$. So the notation of §14 is consistent with Definition 24.1.

(c) Any permutation in S_n ($n \geq 2$) can be written as a product of transpositions (Theorem 16.2). Let T be the set of all transpositions in S_n . Then $S_n = \langle T \rangle$ by Lemma 24.2.

(d) $SL(2, \mathbb{Z})$ is generated by $\left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\}$. A proof of this is outlined in Ex. 9.

24.6 Lemma: Let G be a group and let X be a nonempty subset of G . Suppose $x\sigma \in X$ for all $x \in X$ and for all $\sigma \in \text{Aut}(G)$ [respectively for all $\sigma \in \text{Inn}(G)$]. Then $\langle X \rangle$ is a characteristic [respectively normal] subgroup of G .

Proof: Let $y \in \langle X \rangle$. Then $y = x_1^{m_1} x_2^{m_2} \dots x_k^{m_k}$ for some suitable $k \in \mathbb{N}$, $x_1, x_2, \dots, x_k \in X$, and $m_1, m_2, \dots, m_k \in \mathbb{Z}$ (Lemma 24.2). Then, for any σ in $\text{Aut}(G)$ [respectively for any σ in $\text{Inn}(G)$],

$$y\sigma = (x_1^{m_1} x_2^{m_2} \dots x_k^{m_k})\sigma = (x_1\sigma)^{m_1} (x_2\sigma)^{m_2} \dots (x_k\sigma)^{m_k} \in X$$

by Lemma 24.2, for $x_1\sigma, x_2\sigma, \dots, x_k\sigma \in X$ by hypothesis. Thus $\langle X \rangle\sigma \subseteq \langle X \rangle$ for any $\sigma \in \text{Aut}(G)$ [respectively for any $\sigma \in \text{Inn}(G)$]. But then we have $\langle X \rangle\sigma^{-1} \subseteq \langle X \rangle$ for any $\sigma \in \text{Aut}(G)$ [respectively for any $\sigma \in \text{Inn}(G)$], too. Then $\langle X \rangle = \langle X \rangle\sigma^{-1}\sigma \subseteq \langle X \rangle\sigma \subseteq \langle X \rangle$. Hence $\langle X \rangle\sigma = \langle X \rangle$ for all $\sigma \in \text{Aut}(G)$ [respectively for all $\sigma \in \text{Inn}(G)$] and $\langle X \rangle$ is a characteristic [respectively normal] subgroup of G . \square

We are now in a position to introduce commutator subgroups.

24.7 Definition: Let G be a group and $x, y \in G$. Then

$$x^{-1}y^{-1}xy \in G$$

is called the *commutator of x and y* (in this order) and is denoted by $[x, y]$.

Some authors define $[x, y]$ to be $xyx^{-1}y^{-1}$. In this book, $[x, y]$ will always stand for $x^{-1}y^{-1}xy$. Clearly, $xy = yx[x, y]$ for any $x, y \in G$. In general, $xy \neq yx$, and $[x, y]$ is that element z in G for which $xy = yx.z$, whence the name commutator.

24.8 Lemma: Let G be a group and $x, y \in G$.

(1) $[x, y]^{-1} = [y, x]$.

(2) $[x, y] = 1$ if and only if x and y commute: $xy = yx$.

Proof: (1) $[x, y]^{-1} = (x^{-1}y^{-1}xy)^{-1} = y^{-1}x^{-1}(y^{-1})^{-1}(x^{-1})^{-1} = y^{-1}x^{-1}yx = [y, x]$.

(2) $[x, y] = 1$ means $x^{-1}y^{-1}xy = 1$, and this means $xy = yx$. □

From Lemma 24.8(2), we understand that commutators measure, so to speak, how nonabelian a group is. When the set of commutators consists of 1 only, then the group is abelian. Rather sloppily, the more nonidentity commutators a group has, the more elements of G fail to commute with other elements of G , and the more nonabelian G is. This vague statement will acquire a precise meaning below (Lemma 24.12 and Theorem 24.14).

24.9 Definition: Let $H, K \leq G$. We define the *commutator subgroup* corresponding to H and K as

$$[H, K] = \langle [h, k] \in G : h \in H, k \in K \rangle.$$

We saw in Lemma 24.8(1) that the inverse of a commutator is a commutator. However, when H and K are subgroups of G , the inverse of a commutator of the form $[h, k]$, where $h \in H, k \in K$, need *not* be a commutator of the form $[h', k']$, with $h' \in H, k' \in K$. Also, the product of two commutators is not a commutator in general. The commutator subgroups are defined to be the subgroups *generated* by the set of appropriate commutators, *not* as the *set* of commutators.

24.10 Lemma: Let $H, K \leq G$. Then $[H, K] = [K, H]$.

Proof: We have $[H, K] = \langle [h, k] \in G : h \in H, k \in K \rangle$
 $= \langle [h, k]^{-1} \in G : h \in H, k \in K \rangle$ (by Remark 24.3)

$$\begin{aligned}
&= \langle [k,h] \in G: k \in K, h \in H \rangle \\
&= [K,H].
\end{aligned}$$

□

24.11 Lemma: *Let $H, K \leq G$. If H and K are characteristic [respectively normal] subgroups of G , then $[H,K]$ is characteristic [respectively normal] in G .*

Proof: We use Lemma 24.6, with $X = \{[h,k] : h \in H, k \in K\}$. It suffices to show that $x\sigma \in X$ for all $x \in X$ and for all $\sigma \in \text{Aut}(G)$ [respectively for all $\sigma \in \text{Inn}(G)$]. This follows from

$$\begin{aligned}
x &= [h,k] \text{ for some } h \in H, k \in K, \\
x\sigma &= [h,k]\sigma = (h^{-1}k^{-1}hk)\sigma = (h\sigma)^{-1}(k\sigma)^{-1}(h\sigma)(k\sigma) = [h\sigma, k\sigma] \in X
\end{aligned}$$

as $h\sigma \in H, k\sigma \in K$ for any $\sigma \in \text{Aut}(G)$ [respectively for any $\sigma \in \text{Inn}(G)$] when H and K are characteristic [respectively normal] subgroups of G . □

24.12 Lemma: *Let $H \trianglelefteq G, K \trianglelefteq G$. Then $[H,K] \leq H \cap K$. In particular, if $H \cap K = 1$, then every element of H commutes with every element of K .*

Proof: It suffices to show that $[h,k] \in H \cap K$ for all $h \in H, k \in K$. For any $h \in H, k \in K$, we have indeed

$$\begin{aligned}
[h,k] &= h^{-1}.k^{-1}hk \in H \text{ since } H \trianglelefteq G \\
[h,k] &= h^{-1}k^{-1}h.k \in K \text{ since } K \trianglelefteq G,
\end{aligned}$$

yielding $[h,k] \in H \cap K$.

If $H \cap K = 1$, then $[h,k] \in H \cap K = 1$ and $[h,k] = 1$, so $hk = kh$ for all $h \in H$, and $k \in K$. □

The preceding lemma supports our vague remark that commutators measure how nonabelian a group is. Suppose we treat, somehow, commutators like the identity. Then the group will be like an abelian group. The formal way of treating commutators like 1 is to define an equivalence relation on the group in such a way that all commutators will be equivalent to 1. The most natural equivalence relation of this type is right congruence modulo the subgroup generated by all commutators

(Definition 10.4). The equivalence classes are the right cosets of this subgroup, which is normal, form a factor group. We expect this factor group to be abelian. First we give a name to the subgroup.

24.13 Definition: Let G be a group. Then the subgroup

$$[G,G] = \langle [g,g'] : g,g' \in G \rangle$$

generated by all commutators in G is called the *derived subgroup* of G , denoted by G' .

G is abelian if and only if $G' = 1$. Now G' is a characteristic subgroup of G (Lemma 24.11), hence we can build the factor group G/G' . We expect G/G' is abelian. In fact, much more is true.

24.14 Theorem: Let $K \trianglelefteq G$. Then G/K is abelian if and only if $G' \leq K$.

Proof: G/K is abelian $\Leftrightarrow (xK)(yK) = (yK)(xK)$ for all $x,y \in G$
 $\Leftrightarrow xyK = yxK$ for all $x,y \in G$
 $\Leftrightarrow x^{-1}y^{-1}xyK = K$ for all $x,y \in G$
 $\Leftrightarrow x^{-1}y^{-1}xy \in K$ for all $x,y \in G$
 $\Leftrightarrow [x,y] \in K$ for all $x,y \in G$
 $\Leftrightarrow \langle [x,y] : x,y \in G \rangle \leq K$
 $\Leftrightarrow G' \leq K. \quad \square$

Exercises

1. Let G be a group and X a nonempty subset of G . Prove that $\langle X \rangle = \{x_1^{\mathbb{E}_1} x_2^{\mathbb{E}_2} \dots x_k^{\mathbb{E}_k} \in G : k \in \mathbb{N}, x_i \in X \text{ and } \mathbb{E}_i = \mp 1 \text{ for all } i = 1, 2, \dots, k\}$.
2. Show that $S_n = \langle (12), (123 \dots n-1, n) \rangle$ when $n \geq 3$.
3. If $H \leq G$, $|G:H|$ is finite and G is finitely generated, show that H is also finitely generated.

4. If $H \trianglelefteq G$ and G is finitely generated, show that G/H is also finitely generated.

5. Show that every finitely generated subgroup of \mathbb{Q} is cyclic.

6. Let $H_1 \leq H_2 \leq H_3 \leq \dots$ be subgroups of G . Prove that $H := \bigcup_{i=1}^{\infty} H_i$ is a subgroup of G . Prove further that, if each H_i is a proper subgroup of G , then H is also a proper subgroup of G .

7. Let $\alpha: \mathbb{R} \rightarrow \mathbb{R}$ and $\beta: \mathbb{R} \rightarrow \mathbb{R}$ and put $G = \langle \alpha, \beta \rangle \leq S_{\mathbb{R}}$. Let $\alpha_n = \beta^n \alpha \beta^{-n}$ for

$$u \rightarrow u+1 \quad u \rightarrow 2u$$

$n \in \mathbb{N}$. Show that $\alpha_{n+1}^2 = \alpha_n$ for all $n \in \mathbb{N}$. Show that

$$\langle \alpha_1 \rangle < \langle \alpha_2 \rangle < \langle \alpha_3 \rangle < \dots$$

Prove that $\langle \alpha_n \rangle$ is a proper subgroup of $A := \bigcup_{i=1}^{\infty} \langle \alpha_i \rangle$ for all $n \in \mathbb{N}$. Using Ex. 6, conclude that A is not finitely generated. Thus a subgroup of a finitely generated group need not be finitely generated.

8. Let $M = \mathbb{Q} \setminus \{0, 1\}$ and $\alpha: M \rightarrow M$ and $\beta: M \rightarrow M$. Prove that $\langle \alpha, \beta \rangle \leq S_M$

$$x \rightarrow 1/x \quad x \rightarrow 1/(1-x)$$

and that $\langle \alpha, \beta \rangle$ is isomorphic to S_3 .

9. Show that $SL(2, \mathbb{Z}) = \langle T, S \rangle$, where $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ by going through the following steps. Let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbb{Z})$. If $c = 0$, then M is a power of T . Make induction: suppose a matrix in $SL(2, \mathbb{Z})$ belongs to $\langle T, S \rangle$ whenever its lower-left entry is positive and $< c$. If $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is a matrix whose lower-left entry is c , divide d by c , so that $d = qc + r$. Then MT^qS is in $\langle T, S \rangle$, and so is M . Thus $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \langle T, S \rangle$ whenever $c > 0$. If c is negative, $MS^2 \in \langle T, S \rangle$, and so $M \in \langle T, S \rangle$.

10. Let $H \leq G$. Prove that $[H, G] = 1$ if and only if $H \leq Z(G)$ and also that $[H, G] \leq H$ if and only if $H \trianglelefteq G$.

11. Show that, if $G' \leq N \leq G$, then N is a normal subgroup of G .

12. Let $K \trianglelefteq G$. Prove that $[xK, yK] = [x, y]K \in G/K$ for any $x, y \in G$. Then prove that $[HK/K, JK/K] = [H, J]K/K$ for all $H, J \leq G$.

13. Let $H_1, H_2 \leq H$ and $K_1, K_2 \leq K$. Show that $[H_1 \times K_1, H_2 \times K_2] = [H_1, H_2] \times [K_1, K_2]$ as subgroups of $H \times K$.
14. Show that $[xy, z] = y^{-1}[x, z]y \cdot [y, z]$ and $[x, yz] = [x, z] \cdot z^{-1}[x, y]z$ for any elements x, y, z of a group G . Deduce that $[HJ, K] = [H, K][J, K]$ whenever H, J, K are normal subgroups of G .
15. For any elements x, y, z of a group G , show that
$$y^{-1}[[x, y^{-1}], z]y \cdot z^{-1}[[y, z^{-1}], x]z \cdot x^{-1}[[z, x^{-1}], y]x = 1.$$
16. Let H, K, L be subgroups of a group G and $N \triangleleft G$. If two of the subgroups $[[H, K], L]$, $[[K, L], H]$, $[[L, H], K]$ are contained in N , prove that the third is also contained in N .
17. Give an example of a group and three subgroups H, K, L of G such that $[[H, K], L] \neq [H, [K, L]]$.
18. Prove: if $K \triangleleft G$, then $K' \triangleleft G$.
19. Find the derived subgroups of S_3, S_4, A_4, D_8, Q_8 (see §17, Ex. 15), $SL(2, \mathbb{Z}_3)$, $GL(2, \mathbb{Z}_3)$, S_n, A_n (for $n > 2$).
20. Let G be a group such that $G' \leq Z(G)$ and let a be a fixed element of G . Prove that the mapping $\phi: G \rightarrow G$ is a homomorphism.
$$x \rightarrow [x, a]$$