

§19 Product Sets in Groups

In the preceding paragraph, we introduced a multiplication on the set of right cosets of a subgroup H of a given group G . This involved selecting elements from the cosets to be multiplied. Selecting elements from the cosets is an artificial step in this coset multiplication. We showed in Theorem 18.4 that the resulting coset is independent of the elements chosen when (and only when) H is a normal subgroup of G . However, this does not get rid of the inherent artificiality of the coset multiplication we studied in §18. A more natural multiplication would treat the elements of cosets on equal standing, rather than distinguishing (selecting) one of them (as in Suggestion 18.1) and then showing (as in Theorem 18.4) that no injustice to the remaining elements has been committed. We introduce in this paragraph a natural multiplication of cosets, and in fact more generally of arbitrary nonempty subsets in a group. The new multiplication will coincide with the one of Suggestion 18.1.

19.1 Definition: Let G be a group. For any nonempty subsets X, Y of G , the *product set* XY is defined to be

$$XY = \{xy \in G : x \in X, y \in Y\}.$$

When X has only one element, say when $X = \{x\}$, we write xY instead of $\{x\}Y$. Likewise, we write Xy instead of $X\{y\}$. This is consistent with the definition of cosets (Definition 10.1).

This multiplication is associative.

19.2 Lemma: *Let G be a group. For any nonempty subsets X, Y, Z of G , there holds $(XY)Z = X(YZ)$.*

Proof: This follows from the associativity of multiplication in G :

$$\begin{aligned}
(XY)Z &= \{uz \in G: u \in XY, z \in Z\} \\
&= \{(xy)z \in G: x \in X, y \in Y, z \in Z\} \\
&= \{x(yz) \in G: x \in X, y \in Y, z \in Z\} \\
&= \{xv \in G: x \in X, v \in YZ\} \\
&= X(YZ). \quad \square
\end{aligned}$$

Using Lemma 8.3, we may and do drop the parentheses in any product set involving more than two subsets. For example, we write $XYZUV$ for $(XY)(Z(UV))$.

19.3 Examples: (a) Let $H \leq G$. As we have remarked earlier, $H\{x\} = Hx = \{hx: h \in H\}$ is the right coset of H in G containing $x \in G$. Analogously, $\{x\}H = xH$ is the left coset of H that contains x .

(b) Let G be a group, $H \leq G$ and $x \in G$. Then $x^{-1}Hx = \{x^{-1}hx: h \in H\}$ (see Lemma 18.2) is the product of the sets $\{x^{-1}\}, H, \{x\}$.

(c) Let G be a group and let X be a nonempty subset of G . Then XX consists of all products x_1x_2 , where x_1 and x_2 run through X independently. Notice that $XX \neq \{x^2 \in G: x \in X\}$ in general. X is a multiplicatively closed subset of G if and only if $XX \subseteq X$. In particular, $HH \subseteq H$ for any subgroup H of G .

(d) Let G be a group and let X, Y be nonempty subsets of G . It follows from Definition 19.1 that

$$XY = \bigcup_{y \in Y} Xy = \bigcup_{x \in X} xY.$$

(e) Let $X = \{i, (12)\}$, $Y = \{i, (13)\}$. Now X and Y are subgroups of S_3 . Then $XY = \{i, \tau(13), (12)\tau(12)(13)\} = \{i, (13), (12), (123)\}$. Notice that X, Y are subgroups of S_3 , but XY is not. So the product of two subgroups is not necessarily a subgroup.

(f) Let $X = \{i, (13)\}$ and $V_4 = \{i, (12)(34), (13)(24), (14)(23)\}$. Then $X \leq S_4$ and $V_4 \trianglelefteq S_4$ (Example 18.10(d)). Here XV_4

$$\begin{aligned}
&= \\
&\{i, \tau(12)(34), \tau(13)(24), \tau(14)(23), (13)\tau(13)(12)(34), (13)(13)(24), (13)(14)(23)\}.
\end{aligned}$$

$= \{1, (12)(34), (13)(24), (14)(23), (13), (1432), (24), (1234)\}$

is easily seen to be closed under multiplication, hence XV_4 is a subgroup of S_4 (Lemma 9.3(2)), but not a normal subgroup of S_4 , for $(13) \in XV_4$ but $(12)^{-1}(13)(12) = (23) \notin XV_4$ (Lemma 18.2(1)). We see that the product of two subgroups is not necessarily a normal subgroup even if one of the factors is a normal subgroup.

In Example 19.3(f) above, it is easy to see $XV_4 = V_4X$. This is the basic reason why XV_4 turns out to be a subgroup of S_4 . The next lemma describes the situation.

19.4 Lemma: *Let $H \leq G$ and $K \leq G$.*

- (1) *$HK \leq G$ if and only if $HK = KH$.*
- (2) *If $H \trianglelefteq G$ or $K \trianglelefteq G$, then $HK \leq G$.*
- (3) *If $H \trianglelefteq G$ and $K \trianglelefteq G$, then $HK \trianglelefteq G$.*

Proof: Before we present the proof, it will be worthwhile to discuss the equation $HK = KH$. What does it mean? Well, HK and KH are subsets of G and equality of them is equivalent to the inclusions

$$HK \subseteq KH \text{ and } KH \subseteq HK.$$

The first inclusion means, for any $h \in H$ and $k \in K$, the element hk of G belongs to KH , so that there are $k_1 \in K$ and $h_1 \in H$ such that $hk = k_1h_1$. Similarly, the second inclusion means, for any $k \in K$ and $h \in H$, there are $h_2 \in H$ and $k_2 \in K$ such that $kh = h_2k_2$.

$HK = KH$ does *not* mean that $hk = kh$ for all $h \in H, k \in K$. Of course, if $hk = kh$ for all $h \in H, k \in K$, then trivially $HK = KH$. However, it does not follow from $HK = KH$ that $hk = kh$ for all $h \in H, k \in K$. From $HK = KH$, it follows only that, for any $h \in H, k \in K$, there are $k_1 \in K, h_1 \in H$ and $h_2 \in H, k_2 \in K$ such that $hk = k_1h_1$ and $kh = h_2k_2$.

Now the proof.

- (1) We are to show: (a) if $HK = KH$, then $HK \leq G$; and (b) if $HK \leq G$, then $HK = KH$.

(a) Suppose first $HK = KH$. We prove that HK is closed under multiplication and the forming of inverses (Lemma 9.2).

(i) If $HK = KH$, then $HK.HK = H.KH.K = H.HK.K = HH.KK \subseteq HK$ and so HK is closed under multiplication (see Example 19.3(c)). If you are not satisfied with this demonstration, here is another. Let $x, y \in HK$, say $x = hk$, $y = h_1k_1$ with $h, h_1 \in H$ and $k, k_1 \in K$. We wish to show $xy \in HK$. Now $xy = hk.h_1k_1 = h.kh_1.k_1$ and $kh_1 \in KH = HK$ by hypothesis, so $kh_1 = h_2k_2$ for some $h_2 \in H, k_2 \in K$. So $xy = h.kh_1.k_1 = h.h_2k_2.k_1 = hh_2.k_2k_1 \in HK$ since $hh_2 \in H$ and $k_2k_1 \in K$ as $H \leq G$ and $K \leq G$. Thus HK is closed under multiplication.

(ii) Let $x \in HK$, say $x = hk$ with $h \in H, k \in K$. We are to show that $x^{-1} \in HK$. We have $x^{-1} = (hk)^{-1} = k^{-1}h^{-1} \in KH = HK$, because $k^{-1} \in K$ and $h^{-1} \in H$ as K and H are subgroups of G . So HK is closed under the forming of inverses.

This proves that $HK \leq G$ whenever $H \leq G, K \leq G$ and $HK = KH$.

(b) Now suppose $H \leq G, K \leq G$ and $HK \leq G$. We want to show $HK = KH$, that is, $HK \subseteq KH$ and $KH \subseteq HK$. These inclusions follow from the fact that HK is closed under taking inverses. Indeed, if $x \in HK$, then $x^{-1} \in HK$, say $x^{-1} = hk$ with $h \in H, k \in K$. Then $x = (hk)^{-1} = k^{-1}h^{-1} \in KH$. So $HK \subseteq KH$. The other inclusion is proved in the same way.

This proves that $H \leq G, K \leq G$ and $HK \leq G$ implies $HK = KH$.

The proof of (1) is complete.

(2) We suppose $H \triangleleft G, K \leq G$ and prove that $HK \leq G$. According to part (1), it suffices to show $HK = KH$. First we prove $HK \subseteq KH$. Let $h \in H, k \in K$. Then $k^{-1}hk \in H$ since $H \triangleleft G$ (Lemma 18.2(1)) and $hk = k.k^{-1}hk \in KH$. This proves $HK \subseteq KH$. Now we prove $KH \subseteq HK$. For any $h \in H, k \in K$, we have $khk^{-1} \in H$ since $H \triangleleft G$ and thus $kh = khk^{-1}.k \in HK$ and $KH \subseteq HK$. Therefore $HK = KH$ and $HK \leq G$.

The proof of $HK \leq G$ under the hypotheses $H \leq G, K \triangleleft G$ follows similar lines and is left to the reader.

(3) We now assume $H \triangleleft G, K \triangleleft G$. From part (2), we get $HK \leq G$. We are to show $HK \triangleleft G$. To do that, we prove $g^{-1}xg \in HK$ for all $g \in G, x \in HK$ (Lemma 18.2(1)). For any $x \in HK$, there are $h \in H, k \in K$ with $x = hk$ and

$g^{-1}xg = g^{-1}hkg = g^{-1}hg.g^{-1}kg \in HK$ since $g^{-1}hg \in H$ and $g^{-1}kg \in K$ as $H \trianglelefteq G$ and $K \trianglelefteq G$. Hence $HK \trianglelefteq G$.

This completes the proof. □

In Lemma 19.4(3), it would not be enough to prove that $g^{-1}xg \in HK$ for all $g \in G, x \in HK$. It is necessary to show $HK \leq G$ also. Generally speaking, " $A \trianglelefteq B$ " summarizes two conditions on A and B : that A is a subgroup of B and that A is normal in B . We must check both of them whenever we want to show $A \trianglelefteq B$.

We turn our attention to the product of two right cosets. The product of two right cosets, as in Definition 19.1, is a subset of the group under discussion. When is it a right coset? The next lemma gives the answer.

19.5 Lemma: *Let $H \leq G$. The product of arbitrary right cosets of H in G , according to Definition 19.1, is always a right coset of H in G if and only if $H \trianglelefteq G$.*

Proof: The product of Ha and Hb (where $a, b \in G$) is

$$HaHb = \{hah_1b \in G: h, h_1 \in H\}$$

and $ab = 1a1b \in HaHb$. Thus $HaHb$ is a right coset of H in G if and only if it is the right coset of H in G to which ab belongs:

$$H \text{ is the right coset of } H \text{ in } G \iff HaHb = Hab.$$

We show that $HaHb = Hab$ for all $a, b \in G$ if and only if $H \trianglelefteq G$.

If $H \trianglelefteq G$, then $HaHb = Hab$ for all $a, b \in G$. Indeed, if $H \trianglelefteq G$, then $aH = Ha$ for all $a \in G$ (Lemma 18.2(4)), and, for any $a, b \in G$, we have

$$HaHb = H.aH.b = H.Ha.b = HH.ab = Hab.$$

Here we use $HH = H$, which follows from $HH \subseteq H$ (Example 19.3(c)) and $H = 1H \subseteq HH$.

Conversely, assume $HaHb = Hab$ for all $a, b \in G$. Then

$$\begin{aligned} HaH &= (HaH)(bb^{-1}) = (HaHb)b^{-1} = (Hab)b^{-1} = (Ha)bb^{-1} = Ha \\ HaH &= Ha \end{aligned}$$

$$aH = 1aH \subseteq HaH = Ha$$

and so $aH \subseteq Ha$ for all $a \in G$. From Lemma 18.2(5), we obtain $H \trianglelefteq G$

□

The product of any two right cosets of $H \leq G$, as in Suggestion 18.1, is always a right coset of H , provided this multiplication is well defined, and it is well defined if and only if $H \trianglelefteq G$. On the other hand, the product of any two right cosets of $H \leq G$, as in Definition 19.1, is always a definite subset of G , but this subset is a right coset of H if and only if $H \trianglelefteq G$. The relation $HaHb = Hab$ in the proof of Lemma 19.5 shows that these two multiplications are identical when $H \trianglelefteq G$.

We know that HK is not necessarily a subgroup of G even if $H \leq G$, $K \leq G$. It is a subset of G . We now determine the number of elements in it.

19.6 Lemma: *Let $H, K \leq G$ and assume that H and K are finite. Then HK is a finite subset of G , whose cardinality is given by*

$$|HK| = \frac{|H| |K|}{|H \cap K|}.$$

Proof: We list all products hk , where h and k run through H and K , respectively. In this way, we get $|H| |K|$ elements of G . These are the elements of HK . Naïvely, we expect $|HK|$ to be equal to $|H| |K|$, but there may be repetitions in our list: the same element of HK may be written more than once. We have to keep account of repetitions. We show that each of the $|H| |K|$ products hk appears exactly n times in our list, where $n := |H \cap K|$. Thus there are $|H| |K|/n$ distinct elements in the list and $|HK| = |H| |K|/n$. In other words, the mapping

$$\begin{aligned} \varphi: H \times K &\rightarrow HK \\ (h, k) &\rightarrow hk \end{aligned}$$

is an n -to-one mapping. By this, we understand that exactly n elements in the domain $H \times K$ have the same image under φ .

To prove that φ is an n -to-one mapping, let us investigate when we have $(h_1, k_1)\varphi = (h_2, k_2)\varphi$. Well, $(h_1, k_1)\varphi = (h_2, k_2)\varphi$ if and only if $h_1 k_1 = h_2 k_2$ and

therefore if and only if $h_1^{-1}h_2 = k_1k_2^{-1} = s$ belongs to $H \cap K$. Thus (h_1, k_1) and (h_2, k_2) have the same image under φ if and only if $h_2 = h_1s$ and $k_2 = s^{-1}k_1$ for some $s \in H \cap K$. Denoting by $1 = s_1, s_2, \dots, s_n$ the $n = |H \cap K|$ elements of $H \cap K$, we conclude that the n ordered pairs

$$(h_1, k_1), (h_1s_2, s_2^{-1}k_1), (h_1s_3, s_3^{-1}k_1), \dots, (h_1s_n, s_n^{-1}k_1)$$

and only these ordered pairs have the image h_1k_1 under φ . This proves that φ is indeed n -to-one, and consequently

$$|HK| = \frac{|H| |K|}{|H \cap K|}.$$

Exercises

1. Let X, Y be arbitrary nonempty subsets of a group G and let g be an arbitrary element of G . Prove the following equivalences.

$$\begin{aligned} X \subseteq Y &\iff gX \subseteq gY &\iff g^{-1}Xg \subseteq g^{-1}Yg; \\ X = Y &\iff gX = gY &\iff Xg = Yg &\iff g^{-1}Xg = g^{-1}Yg; \\ X = gY &\iff g^{-1}X = Y. \end{aligned}$$

2. Let H, K be subgroups of a group G . Assume that G is finite, $|H| \geq \sqrt{|G|}$ and $|K| \geq \sqrt{|G|}$. Prove that $H \cap K \neq 1$.

3. Let A, B, C be subgroups of a group G , with $A \leq C$. Prove that

$$A(B \cap C) = AB \cap C.$$

4. Let H, K be subgroups of a group G and let $g \in G$. Prove that

$$|HgK| = \frac{|H| |K|}{|g^{-1}Hg \cap K|}.$$

(A subset of the form HgK is called a *double coset*.)