

§8

Conventions and Some Computational Lemmas

In our study of groups, we are interested in how $a \circ b$ depends on a and b , not in the name or sign of the operation. For this reason, we suppress the operation sign altogether and use juxtaposition. Henceforward, we will write ab (and also occasionally $a \cdot b$) for $a \circ b$. We will refer to the operation as *multiplication*. Thus "multiplication" will be used in a broad sense. It can mean the usual multiplication of numbers, but also the composition of mappings, the taking of symmetric differences of two sets, or some rather artificial operation like those in Example 7.4. With this convention, there is no need to refer to the operation all the time when we discuss groups. So we call the *set* G a group, instead of the ordered pair (G, \circ) (we keep in mind of course that there can be many groups on the same set). We say then that the group is written *multiplicatively* or that G is a *multiplicative* group. Conforming to this, we call ab the *product of a and b* . Also, we write 1 for the identity element of the group. Thus 1 is not necessarily the number one. It is perhaps the identity mapping, perhaps the empty set, perhaps some other object. What it is depends on the group we are investigating. But a warning: we will *not* write $\frac{1}{a}$ for the inverse a^{-1} of an element a in a group.

This is the multiplicative notation for groups. Sometimes, we shall use the *additive* notation, too, especially when the group is commutative. Then the operation is denoted by "+" and is called *addition*. Like "multiplication", "addition" is used in a general sense. We call $a + b$ the *sum of a and b* . When we have an *additive* group, the identity element of the group will be written as 0 . So 0 is not necessarily the number zero. Also, we write $-a$ for the inverse of an element a in an additively written group. We call $-a$ the *opposite of a* .

8.1 Lemma: *Let G be a group and let $a, b, c \in G$.*

- (1) *If $ab = ac$, then $b = c$ (left cancellation).*
- (2) *If $ba = ca$, then $b = c$ (right cancellation).*

Proof: (1) If $ab = ac$, we multiply by a^{-1} on the left and get $a^{-1}(ab) = a^{-1}(ac)$. Using associativity, we obtain $(a^{-1}a)b = (a^{-1}a)c$. So $1b = 1c$. Since 1 is the identity element of G , we finally get $b = c$.

(2) The proof of (2) is similar and is left to the reader. □

We must be careful when we want to use Lemma 8.1 to make cancellation. If the group is not commutative, left multiplication by an element and right multiplication by the same element give in general different results. In the proof of Lemma 8.1, we multiplied by a^{-1} on the same side. We cannot conclude $b = c$ from $ab = ca$, for instance. Indeed, we have

$$ab = ca \implies a^{-1}(ab) = a^{-1}(ca) \implies (a^{-1}a)b = (a^{-1}c)a \implies b = a^{-1}ca$$

and this is all we can say. In general, $a^{-1}ca \neq c$, so $b \neq c$. You must always make sure that you cancel on the same side.

Cancellations are multiplications by inverse elements. We now evaluate the inverse of an inverse, and the inverse of a product.

8.2 Lemma: *Let G be a group and let $a, b \in G$. Then*

- (1) $(a^{-1})^{-1} = a$,
- (2) $(ab)^{-1} = b^{-1}a^{-1}$.

Proof: (1) $aa^{-1} = 1$ by the definition of a^{-1} . So a is a left inverse of a^{-1} . So a is the inverse of a^{-1} (Lemma 7.3).

(2) $(ab)(b^{-1}a^{-1}) = a(b(b^{-1}a^{-1})) = a((bb^{-1})a^{-1}) = a(1a^{-1}) = aa^{-1} = 1$, and so $b^{-1}a^{-1}$ is the inverse of ab . □

Therefore, the inverse of the inverse of an element is the element itself. Also, the inverse of a product is the product of the inverses, but in the *reverse* order. Do *not* write $(ab)^{-1} = a^{-1}b^{-1}$. This is wrong unless $a^{-1}b^{-1} = b^{-1}a^{-1}$, which is equivalent to $ab = ba$ (why?) and which is not true in general.

*
* *

We defined the product of *two* elements. The product of a and b is ab . We now want to define the product of n elements and prove that the usual exponentiation rules are valid. The rest of this paragraph is extremely dull. The reader may just glance at the assertions and skip the proofs if she (or he) wishes.

By the product of three elements a, b, c in a group G , we understand an element abc of G . Let us recall we agreed to denote by abc the element $(ab)c = a(bc)$. So the product of a, b, c in this order is evaluated by two successive multiplications. Either we evaluate ab first, then multiply it by c , or we evaluate bc first, then multiply a by it. In either way, we get the same result by associativity and this result is denoted by abc , without parentheses.

Now let us consider the product of four elements a, b, c, d . Their product in this order will be defined by three successive multiplications of two elements. This can be done in five distinct ways:

$$a(b(cd)), a((bc)d), (ab)(cd), ((ab)c)d, (a(bc))d,$$

but these five products are all equal by associativity. The first two products are equal since $b(cd) = (bc)d$. The last two products are equal since $(ab)c = a(bc)$. Further, we have $a(b(cd)) = (ab)(cd)$ [put $cd = e$, then $a(be) = (ab)e$] and $(ab)(cd) = ((ab)c)d$ [put $ab = f$, then $f(cd) = (fc)d$]. So the five products are equal. This renders it possible to drop the parentheses and write simply $abcd$. This is the product of a, b, c, d in the given order.

More generally, we want to define the product of n elements a_1, a_2, \dots, a_n in a group G ($n > 2$). The product of a_1, a_2, \dots, a_n will be defined by $n - 1$ successive multiplications of two elements. By inserting parentheses in all possible ways, we obtain many products (their exact number is $2 \cdot 4 \cdot \dots \cdot (4n - 6)/n!$), but associativity assures that these products are equal. Now we prove this. In view of some later applications, the following lemma is stated more generally than for groups.

8.3 Lemma: Let G be a nonempty set and let there be defined an associative binary operation on G , denoted by juxtaposition. Let $a_1, a_2, \dots, a_n \in G$. Then the products of a_1, a_2, \dots, a_n are independent of the mode of putting parentheses. This means the following. We define

$$P_1(a_1) = \{a_1\}$$

$$P_2(a_1, a_2) = \{a_1 a_2\}$$

$$P_3(a_1, a_2, a_3) = \{(a_1 a_2) a_3, a_1 (a_2 a_3)\}$$

$$= \{xy: x \in P_1(a_1), y \in P_2(a_2, a_3) \text{ or } x \in P_2(a_1, a_2), y \in P_1(a_3)\}$$

$$P_4(a_1, a_2, a_3, a_4) = \{a_1(a_2(a_3 a_4)), a_1((a_2 a_3) a_4), (a_1 a_2)(a_3 a_4), ((a_1 a_2) a_3) a_4, (a_1(a_2 a_3)) a_4\}$$

$$= \{xy: x \in P_1(a_1), y \in P_3(a_2, a_3, a_4) \text{ or } x \in P_2(a_1, a_2), y \in P_2(a_3, a_4) \text{ or}$$

$$x \in P_3(a_1, a_2, a_3), y \in P_1(a_4)\}$$

.....

$$P_k(a_1, a_2, \dots, a_k) = \{xy: x \in P_i(a_1, a_2, \dots, a_i), y \in P_{k-i}(a_{i+1}, \dots, a_k) \text{ for some}$$

$$i = 1, 2, \dots, k\}$$

for $k = 1, 2, \dots, n$. Thus P_k are subsets of G whose elements are the products of a_1, a_2, \dots, a_k , reduced to $k - 1$ successive multiplications of two elements in G .

Claim: For all $n \in \mathbb{N}$ and for all $a_1, a_2, \dots, a_n \in G$, the set $P_n(a_1, a_2, \dots, a_n)$ contains one and only one element.

Proof: The proof will be by induction on n (in the form 4.5). For $n = 1, 2$, it is evident that $P_1(a_1), P_2(a_1, a_2)$ each have exactly one element. For $n = 3$, the claim is just the associativity of multiplication. For $n = 4$, the argument preceding the lemma proves the claim. Notice that we used only the associativity of multiplication there.

Suppose $n \geq 5$ and the lemma is proved for $1, 2, \dots, n - 1$. Let $u, v \in P_n(a_1, a_2, \dots, a_n)$. We are to prove $u = v$. By the definition of $P_n(a_1, a_2, \dots, a_n)$, we have $u = xy, v = st$, where

$$x \in P_i(a_1, a_2, \dots, a_i), y \in P_{n-i}(a_{i+1}, \dots, a_n), \quad i \in \mathbb{N}, \quad 1 \leq i \leq n - 1,$$

$$s \in P_j(a_1, a_2, \dots, a_j), t \in P_{n-j}(a_{j+1}, \dots, a_n), \quad j \in \mathbb{N}, \quad 1 \leq j \leq n - 1.$$

We prove $u = v$ first under the assumption $i = j$. By induction, the set $P_i(a_1, a_2, \dots, a_i)$ contains one and only one element. Hence $x = s$. Also, applying the induction hypothesis to $n - i$, with the elements a_{i+1}, \dots, a_n , we conclude that $P_{n-i}(a_{i+1}, \dots, a_n)$ has one and only one element. This gives $y = t$. Then we get $u = xy = sy = st = v$. So the claim is proved in case $i = j$.

Now suppose $i \neq j$. Without losing generality, we assume $i < j$. We put $j = i + h$, with $h \in \mathbb{N}$. Now apply the induction hypothesis to j , with the elements a_1, \dots, a_j . There is a unique element in $P_j(a_1, \dots, a_j)$, which we called s . Also by induction, applied to i with the elements a_1, \dots, a_i , there is a unique element in $P_i(a_1, a_2, \dots, a_i)$, namely x . Again by induction, applied to h with the elements a_{i+1}, \dots, a_j there is a unique element in $P_h(a_{i+1}, \dots, a_j)$, say b . By the definition of $P_j(a_1, \dots, a_j)$, we have $xb \in P_j(a_1, \dots, a_j)$, so $xb = s$.

We have $n - i = h + (n - j)$. By induction, applied to $n - i$ with the elements a_{i+1}, \dots, a_n , the set $P_{n-i}(a_{i+1}, \dots, a_n)$ has one and only one element, which we called y . Also by induction, applied to h with the elements a_{i+1}, \dots, a_j , there is a unique element in $P_h(a_{i+1}, \dots, a_j)$, namely b . Again by induction, applied to $n - j$ with the elements a_{j+1}, \dots, a_n , the set $P_{n-j}(a_{j+1}, \dots, a_n)$ has a unique element, namely t . By the definition of $P_{n-i}(a_{i+1}, \dots, a_{i+h}, a_{j+1}, \dots, a_n)$, we have $bt \in P_{n-i}(a_{i+1}, \dots, a_n)$, so $bt = y$.

Thus $xb = s$ and $bt = y$. This gives $u = xy = x(bt) = (xb)t = st = v$. This completes the proof. \square

8.4 Definition: The unique element in $P_n(a_1, a_2, \dots, a_n)$ of Lemma 8.3 is called the *product of a_1, a_2, \dots, a_n* (in this order) and is denoted by $a_1 a_2 \cdot a_n$

or by $\prod_{i=1}^n a_i$.

So the product of n elements in a given order can be written without parentheses. This simplifies the notation enormously.

Using the notation of Definition 8.4, we can reformulate Lemma 8.3 as follows. If G is a nonempty set with an associative multiplication on it, and if $a_1, a_2, \dots, a_n \in G$, then

$$a_1(a_2 \dots a_n) = (a_1 a_2)(a_3 \dots a_n) = (a_1 a_2 a_3)(a_4 \dots a_n) = \dots = (a_1 a_2 \dots a_{n-1})a_n = a_1 a_2 \dots a_n.$$

We write a^n for $a_1 a_2 \dots a_n$ in case a_1, a_2, \dots, a_n are all equal to $a \in G, n \in \mathbb{N}$. In particular, $a^1 = a$. We have $a^n = a^{n-1}a = aa^{n-1}$. More generally, the above reformulation of Lemma 8.3 gives

$$a^m a^n = a^{m+n}, \text{ for all } a \in G \text{ and } m, n \in \mathbb{N}. \quad (*)$$

In particular, $(a^m)^2 = a^m a^m = a^{m+m} = a^{2m} = a^{m2}$. We prove more generally $(a^m)^n = a^{mn}$ by induction on n . The case $n = 1$ is trivial and the case $n = 2$ has just been shown. Assume now $n \geq 3$ and $(a^m)^{n-1} = a^{m(n-1)}$ for all $a \in G$. We want to show $(a^m)^n = a^{mn}$ for all $a \in G$. We have $(a^m)^n = (a^m)^{1+(n-1)} = (a^m)^1 (a^m)^{n-1} = a^m (a^m)^{n-1}$ by $(*)$, with $a^m, 1, n-1$ in place of a, m, n , respectively. Then we get $(a^m)^n = a^m a^{m(n-1)} = a^m a^{mn-m} = a^{m+(mn-m)}$ by $(*)$, with $a, m, mn-m$ in place of a, m, n , respectively. This gives $(a^m)^n = a^{mn}$. Thus we proved the

8.5 Lemma: *If there is an associative multiplication on a nonempty set G , denoted by juxtaposition, then*

$$a^m a^n = a^{m+n} \text{ and } (a^m)^n = a^{mn} \text{ for all } a \in G \text{ and } m, n \in \mathbb{N}. \quad \square$$

Lemma 8.5 can be extended to arbitrary integral powers in the case of groups. We give the relevant definitions.

8.6 Definition: Let G be a group, $a \in G, m \in \mathbb{N}$. We put

$$a^0 = 1 = \text{identity of } G, \text{ and } a^{-m} = (a^m)^{-1} = \text{inverse of } a^m.$$

8.7 Lemma: *Let G be a group. Then*

- (1) $a^m a^n = a^{m+n}$,
- (2) $(a^{-1})^m = a^{-m}$,
- (3) $(a^m)^n = a^{mn}$,

for all $a \in G$ and $m, n \in \mathbb{Z}$.

Proof: (1) We prove $a^m a^n = a^{m+n}$. If $m \geq 1, n \geq 1$, Lemma 8.5 yields the result. If $m = 0$, then $a^0 a^n = 1 a^n = a^n = a^{0+n}$ for all $n \in \mathbb{Z}$; and if $n = 0$, then $a^m a^0 = a^m 1 = a^m = a^{m+0}$ for all $m \in \mathbb{Z}$. So we have

$$a^m a^n = a^{m+n} \text{ whenever } m, n \geq 0. \quad (e)$$

We must prove this relation also when $m \geq 0, n \leq 0; m \leq 0, n \geq 0; m \leq 0, n \leq 0$. Changing our notation (replacing m, n by $|m|, |n|$) we must prove (i) $a^m a^{-n} = a^{m-n}$; (ii) $a^{-m} a^n = a^{-m+n}$; (iii) $a^{-m} a^{-n} = a^{-m+(-n)}$ for all $m, n \geq 0$.

(i) Let $m, n \geq 0$. If $m \geq n$, then $a^{m-n} a^n = a^m$ by (e). Multiplying by $(a^n)^{-1} = a^{-n}$ on the right, we get $a^{m-n} = a^m a^{-n}$ if $m \geq n$. Taking the inverses of both sides of this equation, we get, in case $m \geq n$, $a^n a^{-m} = [(a^n)^{-1}]^{-1} (a^m)^{-1} = [a^m (a^n)^{-1}]^{-1} = (a^m a^{-n})^{-1} = (a^{m-n})^{-1} = a^{-(m-n)} = a^{-m+n}$. Interchanging m and n , we get $a^m a^{-n} = a^{-n+m} = a^{m-n}$ in case $n \geq m$. So $a^m a^{-n} = a^{m-n}$, irrespective of whether $m \geq n$ or $n \geq m$.

(ii) Let $m, n \geq 0$. If $n \geq m$, then $a^m a^{-m+n} = a^n$ by (e). Multiplying by $(a^m)^{-1} = a^{-m}$ on the left, we get $a^{-m+n} = a^{-m} a^n$ if $n \geq m$. Taking the inverses of both sides of this equation, we get, in case $n \geq m$, $a^{-n} a^m = a^{-n} [(a^m)^{-1}]^{-1} = (a^n)^{-1} (a^{-m})^{-1} = (a^{-m} a^n)^{-1} = (a^{-m+n})^{-1} = (a^{n-m})^{-1} = a^{-(n-m)} = a^{-n+m}$. Interchanging n and m , we get $a^{-m} a^n = a^{-m+n}$ in case $m \geq n$. So $a^{-m} a^n = a^{-m+n}$, irrespective of whether $m \geq n$ or $n \geq m$.

(iii) Let $m, n \geq 0$. We have $a^m a^n = a^{m+n}$ by (e). Taking the inverses of both sides of this equation, we get $a^{-m} a^{-n} = (a^m)^{-1} (a^n)^{-1} = (a^n a^m)^{-1} = (a^{m+n})^{-1} = a^{-(m+n)} = a^{-m+(-n)}$ for all $m, n \geq 0$.

Thus $a^m a^n = a^{m+n}$ for all $a \in G$ and $m, n \in \mathbb{Z}$.

(2) We prove $(a^{-1})^m = a^{-m}$. This is true if $m = 1$, since $(a^{-1})^1 = a^{-1} = (a^1)^{-1}$. Suppose now $m \in \mathbb{N}, m \geq 2$ and $(a^{-1})^{m-1} = a^{-(m-1)}$. Then $(a^{-1})^m = (a^{-1})^{m-1} (a^{-1}) = a^{-(m-1)} a^{-1} = a^{-m+1} a^{-1} = a^{-m+1-1} = a^{-m}$. So $(a^{-1})^m = a^{-m}$ for all $m \in \mathbb{N}$ by induction. It is also true when $m = 0$, as $(a^{-1})^0 = 1 = a^0 = a^{-0}$. Now we must prove it for $m < 0$. With a slight change in notation, we are prove $(a^{-1})^{-m} = a^m$ for all $m \in \mathbb{N}$. We have indeed $(a^{-1})^{-m} = [(a^{-1})^m]^{-1} = (a^{-m})^{-1} = [(a^m)^{-1}]^{-1} = a^m$. The first equality in this chain follows from Definition 8.6, with a^{-1} in place of a , the second from the fact that $(a^{-1})^m = a^{-m}$ for all $m \in \mathbb{N}$, which we just proved and the third from Definition 8.6.

So $(a^{-1})^m = a^{-m}$ for all $m \in \mathbb{Z}$.

(3) We prove $(a^m)^n = a^{mn}$. If $m \geq 1, n \geq 1$, Lemma 8.5 yields the result. If $m = 0$, then $(a^0)^n = 1^n = 1 = a^0 = a^{0n}$ for all $n \in \mathbb{Z}$; and if $n = 0$, then $(a^m)^0 = 1 = a^0 = a^{m0}$ for all $m \in \mathbb{Z}$. So we have

$$(a^m)^n = a^{mn} \text{ whenever } m, n \geq 0. \quad (e')$$

We must prove this relation also when $m \geq 0, n \leq 0$; $m \leq 0, n \geq 0$; $m \leq 0, n \leq 0$. Replacing m, n by $|m|, |n|$ we must prove (i) $(a^m)^{-n} = a^{m(-n)}$; (ii) $(a^{-m})^n = a^{(-m)n}$; (iii) $(a^{-m})^{-n} = a^{(-m)(-n)}$ for all $m, n \geq 0$.

Writing (e') with a^{-1} in place of a and using (2), we get $(a^m)^{-n} = [(a^m)^{-1}]^n = (a^{-m})^n = [(a^{-1})^m]^n = (a^{-1})^{mn} = a^{-(mn)} = a^{m(-n)}$. This proves (i). We also get $(a^{-m})^n = a^{-(mn)} = a^{(-m)n}$. This proves (ii). Finally, we have $(a^{-m})^{-n} = [(a^m)^{-1}]^{-n} = ([(a^m)^{-1}]^{-1})^n = (a^m)^n = a^{mn} = a^{(-m)(-n)}$. This proves (iii).

Thus $(a^m)^n = a^{mn}$ for all $m, n \in \mathbb{Z}$.

The proof is complete. \square

8.8 Lemma: *Let G be a group and $a_1, a_2, \dots, a_n \in G$. Then*

$$(a_1 a_2 \dots a_n)^{-1} = a_n^{-1} \dots a_2^{-1} a_1^{-1}.$$

Proof: By induction on n . If $n = 2$, the assertion is true by Lemma 8.2(2). Suppose now $n \in \mathbb{N}, n \geq 3$ and $(a_1 a_2 \dots a_{n-1})^{-1} = a_{n-1}^{-1} \dots a_2^{-1} a_1^{-1}$. Then

$$\begin{aligned} (a_1 a_2 \dots a_{n-1} a_n)^{-1} &= ((a_1 a_2 \dots a_{n-1}) a_n)^{-1} \\ &= a_n^{-1} (a_1 a_2 \dots a_{n-1})^{-1} \\ &= a_n^{-1} (a_{n-1}^{-1} \dots a_2^{-1} a_1^{-1}) \\ &= a_n^{-1} a_{n-1}^{-1} \dots a_2^{-1} a_1^{-1}, \end{aligned}$$

as was to be proved. \square

Lemma 8.8 gives an alternative proof of $(a^{-1})^m = (a^m)^{-1}$. When our group is commutative, we have additional results, for example $a^m b^n = b^n a^m$.

8.9 Lemma: *Let G be a group and $a, b \in G$. If $ab = ba$, then*

- (1) $ab^n = b^n a$;
- (2) $a^m b^n = b^n a^m$;

for all $m, n \in \mathbb{Z}$.

Proof: (1) We prove $ab^n = b^n a$. The case $n = 0$ is trivial. Also, $ab^1 = ab = ba = b^1 a$ by hypothesis and the claim is true for $n = 1$. Suppose now $n \in \mathbb{N}, n \geq 2$ and the claim is proved for $n - 1$, so that $ab^{n-1} = b^{n-1} a$.

Then $ab^n = a(b^{n-1}b) = (ab^{n-1})b = (b^{n-1}a)b = b^{n-1}(ab) = b^{n-1}(ba) = (b^{n-1}b)a = b^na$. By induction, $ab^n = b^na$ for all $n \in \mathbb{N}$.

We multiply this relation by b^{-n} on the left and on the right. This gives $b^na = ab^{-n}$ for $n \in \mathbb{N}$. So $ab^n = b^na$ is true also when $n \leq -1$. So $ab^n = b^na$ for all $n \in \mathbb{Z}$.

(2) We have $b^na = ab^n$ by (1). We use this as a hypothesis and apply (1) with a, b, n replaced by b^n, a, m , respectively. Then we obtain $a^mb^n = b^na^m$ for all $m, n \in \mathbb{Z}$. \square

If G is not a group but merely a nonempty set with an associative multiplication on it, the proof remains valid for the case $m, n \in \mathbb{N}$; and also for the case $m = 0$ or $n = 0$, provided there is a unique identity e in G and we agree to write $a^0 = e$ for all $a \in G$:

8.10 Lemma: *Let G be a nonempty set with an associative multiplication on it. Let $a, b \in G$.*

(1) *If $ab = ba$, then $a^mb^n = b^na^m$ for all $m, n \in \mathbb{N}$.*

(2) *If, in addition, there is a unique $e \in G$ such that $ce = ec$ for all $c \in G$, and if we put $c^0 = e$ for all $c \in G$, then $a^mb^n = b^na^m$ also when $m = 0$ or $n = 0$.* \square

8.11 Lemma: *Let G be a nonempty set with an associative multiplication on it. For any $m \in \mathbb{N}$ and for any $a_1, a_2, \dots, a_m, b \in G$ such that*

$$a_i b = b a_i \text{ for all } i = 1, 2, \dots, m$$

there holds $(a_1 a_2 \dots a_m) b = b (a_1 a_2 \dots a_m)$.

Proof: By induction on m . The case $m = 1$ is included in the hypothesis. Suppose now $m \geq 2$ and the claim is true for $m - 1$. Then

$$\begin{aligned} (a_1 a_2 \dots a_{m-1} a_m) b &= ((a_1 a_2 \dots a_{m-1}) a_m) b \\ &= (a_1 a_2 \dots a_{m-1}) (a_m b) \\ &= (a_1 a_2 \dots a_{m-1}) (b a_m) \\ &= ((a_1 a_2 \dots a_{m-1}) b) a_m \end{aligned}$$

$$\begin{aligned}
&= (b(a_1 a_2 \cdots a_{m-1})) a_m \\
&= b((a_1 a_2 \cdots a_{m-1}) a_m) \\
&= b(a_1 a_2 \cdots a_{m-1} a_m),
\end{aligned}$$

as was to be proved. □

Lemma 8.11 gives a new proof of Lemma 8.10 when we choose $a_1 = a_2 = \cdots = a_m = a$ and replace b by b^n .

We proved in Lemma 8.3 that the product of n elements in a group (or in a set with an associative multiplication on it) is independent of the mode of putting parentheses. When the elements commute, the product is also independent of the order of elements.

8.12 Lemma: *Let G be a nonempty set with an associative multiplication on it. For all $n \in \mathbb{N}$, for all $a_1, a_2, \dots, a_n \in G$ such that*

$$a_i a_j = a_j a_i \text{ whenever } i, j = 1, 2, \dots, n,$$

there holds

$$a_{k_1} a_{k_2} \cdots a_{k_n} = a_1 a_2 \cdots a_n$$

for each arrangement k_1, k_2, \dots, k_n of $1, 2, \dots, n$ (i.e., for each k_1, k_2, \dots, k_n such that $\{k_1, k_2, \dots, k_n\} = \{1, 2, \dots, n\}$).

Proof: By induction on n . The case $n = 1$ is trivial. Now assume $n \geq 2$ and the claim is proved for $n - 1$, for all pairwise commuting elements b_1, b_2, \dots, b_{n-1} of G , for all arrangements of $1, 2, \dots, n - 1$. Let a_1, a_2, \dots, a_n be n arbitrary pairwise commuting elements of G and let k_1, k_2, \dots, k_n be an arbitrary arrangement of $1, 2, \dots, n$. Then $n = k_j$ for some $j \in \{1, 2, \dots, n\}$. We have

$$\begin{aligned}
a_{k_1} a_{k_2} \cdots a_{k_n} &= (a_{k_1} \cdots a_{k_{j-1}}) a_{k_j} (a_{k_{j+1}} \cdots a_{k_n}) \\
&= (a_{k_1} \cdots a_{k_{j-1}}) (a_{k_j} (a_{k_{j+1}} \cdots a_{k_n})) \\
&= (a_{k_1} \cdots a_{k_{j-1}}) (a_{k_{j+1}} \cdots a_{k_n}) a_{k_j} \\
&= ((a_{k_1} \cdots a_{k_{j-1}}) (a_{k_{j+1}} \cdots a_{k_n})) a_{k_j} \\
&= (a_{k_1} \cdots a_{k_{j-1}} a_{k_{j+1}} \cdots a_{k_n}) a_{k_j}
\end{aligned}$$

and here $k_1, \dots, k_{j-1}, k_{j+1}, \dots, k_n$ are simply the numbers $1, 2, \dots, n - 1$ in some order. By the inductive hypothesis, applied to the elements a_1, a_2, \dots

., a_{n-1} and the arrangement $k_1, \dots, k_{j-1}, k_{j+1}, \dots, k_n$ of the numbers $1, 2, \dots, n - 1$, we have $a_{k_1} \dots a_{k_{j-1}} a_{k_{j+1}} \dots a_{k_n} = a_1 a_2 \dots a_{n-1}$; therefore

$$\begin{aligned} a_{k_1} a_{k_2} \dots a_{k_n} &= (a_{k_1} \dots a_{k_{j-1}} a_{k_{j+1}} \dots a_{k_n}) a_n \\ &= (a_1 a_2 \dots a_{n-1}) a_n \\ &= a_1 a_2 \dots a_{n-1} a_n \end{aligned}$$

and the induction argument goes through. In the chain of equations above, the term $(a_{k_1} \dots a_{k_{j-1}})$ is absent if $j = 1$ and the term $(a_{k_{j+1}} \dots a_{k_n})$ is absent if $j = n$. The argument remains valid in these cases. \square

8.13 Lemma: *Let G be a commutative group and let a_1, a_2, \dots, a_n be arbitrary elements of G . Then*

$$a_{k_1} a_{k_2} \dots a_{k_n} = a_1 a_2 \dots a_n$$

for all arrangements k_1, k_2, \dots, k_n of the indices $1, 2, \dots, n$.

Proof: This follows immediately from Lemma 8.12. \square

8.14 Lemma: *Let G be a nonempty set with an associative multiplication on it and let $a, b \in G$.*

- (1) *If $ab = ba$, then $(ab)^n = a^n b^n$ for all $n \in \mathbb{N}$.*
- (2) *If, in addition, there is a unique $e \in G$ such that $ce = ec$ for all $c \in G$, and if we put $c^0 = e$ for all $c \in G$, then $(ab)^0 = a^0 b^0$.*
- (3) *If, in addition, G is a group, then $(ab)^n = a^n b^n$ for all $n \in \mathbb{Z}$.*

Proof: (1) The claim is trivially true when $n = 1$. Suppose now $n \geq 2$ and assume $(ab)^{n-1} = a^{n-1} b^{n-1}$. Then

$$\begin{aligned} (ab)^n &= (ab)^{n-1}(ab) = (a^{n-1} b^{n-1})(ab) \\ &= a^{n-1}(b^{n-1} a) b \\ &= a^{n-1}(ab^{n-1}) b \quad (\text{by Lemma 8.10}) \\ &= (a^{n-1} a)(b^{n-1} b) \\ &= a^n b^n \end{aligned}$$

and the claim is true for n . So $(ab)^n = a^n b^n$ for all $n \in \mathbb{N}$.

(2) Writing e for c , we get $ee = e$. Thus $(ab)^0 = e = ee = a^0 e = a^0 b^0$.

(3) That $(ab)^n = a^n b^n$ is proved for $n \geq 0$. We are to prove it also when $n \leq -1$. Replacing n by $-n$, we are to prove that $(ab)^{-n} = a^{-n} b^{-n}$ for $n \in \mathbb{N}$.

We note that $ab = ba$ implies $b^{-1}a^{-1} = (ab)^{-1} = (ba)^{-1} = a^{-1}b^{-1}$, so the hypothesis of (1) is satisfied when we replace a by a^{-1} and b by b^{-1} . Using (1) with a^{-1}, b^{-1} in place of a, b , respectively, we obtain

$$(ab)^n = [(ab)^{-1}]^n = [(ba)^{-1}]^n = (a^{-1}b^{-1})^n = (a^{-1})^n(b^{-1})^n = a^{-n}b^{-n}$$

for $n \in \mathbb{N}$. Thus $(ab)^n = a^n b^n$ is valid also when $n \leq -1$. So $(ab)^n = a^n b^n$ for all $n \in \mathbb{Z}$.

□

8.15 Lemma: *Let G be a commutative group. Then $(ab)^n = a^n b^n$ for all $a, b \in G$ and for all $n \in \mathbb{Z}$.*

Proof: This follows immediately from Lemma 8.14. □

So far, we dealt with multiplicative groups. For additive groups, there are some modifications. In the case of an additive group, the unique element in $P_n(a_1, a_2, \dots, a_n)$ of Lemma 8.3 is called the *sum of a_1, a_2, \dots, a_n*

and is denoted by $a_1 + a_2 + \dots + a_n$ or by $\sum_{i=1}^n a_i$. We write na for $a_1 + a_2 + \dots$

$+ a_n$ in case $n \in \mathbb{N}$ and a_1, a_2, \dots, a_n are all equal to $a \in G$. Also, we define $0a = 0$ (the first 0 is the integer 0, the second 0 is the identity element of G) and $(-m)a = -(ma)$ for $m \in \mathbb{N}$. Thus we defined na for all $n \in \mathbb{Z}$, $a \in G$.

8.16 Lemma: *Let G be an additively written commutative group. Then*

(1) $ma + na = (m + n)a$;

(2) $(-m)a = m(-a)$;

(3) $n(ma) = (nm)a$;

(4) $n(a + b) = na + nb$

for all $m, n \in \mathbb{Z}$, $a, b \in G$.

Proof: (1),(2),(3) follow from Lemma 8.7 and (4) from Lemma 8.15. Notice that commutativity is essential for (4). □

Exercises

1. Let G be a group such that $a^2 = 1$ for all $a \in G$. Prove that G is commutative.

2. Justify each step in the proof of Lemma 8.11.

3. Let G be a group and $a, b, c \in G$. Suppose $ab = ba$. Prove that $(a^m b^n c^r)^{-1} = c^{-r} a^{-m} b^{-n}$ for all $m, n, r \in \mathbb{Z}$, justifying each detail.

(4) Let G be a nonempty set with an associative multiplication on it and let a_1, a_2, \dots, a_n be pairwise commuting elements of G . Show that

$$(a_1 a_2 \dots a_n)^m = a_1^m a_2^m \dots a_n^m$$

for all $m \in \mathbb{N}$.

(5) Show that, if G is an additive commutative group, then

$$-(a_1 + a_2 + \dots + a_n) = (-a_1) + (-a_2) + \dots + (-a_n)$$

for all a_1, a_2, \dots, a_n in G .