(i) $(a \star b) \star c = a \star (b \star c)$, for all $a, b, c \in G$, i.e., $\star$ is *associative*,

(ii) there exists an element e in G, called an *identity* of G, such that for all $a \in G$ we have $a \star e = e \star a = a$,

(iii) for each $a \in G$ there is an element a^{-1} of G, called an *inverse* of a, such that $a \star a^{-1} = a^{-1} \star a = e$.

(2) The group $(G, \star)$ is called *abelian* (or *commutative*) if $a \star b = b \star a$ for all $a, b \in G$.

We shall immediately become less formal and say G is a group under $\star$ if $(G, \star)$ is a group (or just G is a group when the operation $\star$ is clear from the context). Also, we say G is a *finite group* if in addition G is a finite set. Note that axiom (ii) ensures that a group is always nonempty.

Examples

(1) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are groups under $+$ with $e = 0$ and $a^{-1} = -a$, for all a.

(2) $\mathbb{Q} - \{0\}$, $\mathbb{R} - \{0\}$, $\mathbb{C} - \{0\}$, $\mathbb{Q}^+$, $\mathbb{R}^+$ are groups under $\times$ with $e = 1$ and $a^{-1} = \dfrac{1}{a}$, for all a. Note however that $\mathbb{Z} - \{0\}$ is *not* a group under $\times$ because although $\times$ is an associative binary operation on $\mathbb{Z} - \{0\}$, the element 2 (for instance) does not have an inverse in $\mathbb{Z} - \{0\}$.

We have glossed over the fact that the associative law holds in these familiar examples. For $\mathbb{Z}$ under $+$ this is a consequence of the axiom of associativity for addition of natural numbers. The associative law for $\mathbb{Q}$ under $+$ follows from the associative law for $\mathbb{Z}$ — a proof of this will be outlined later when we rigorously construct $\mathbb{Q}$ from $\mathbb{Z}$ (cf. Section 7.5). The associative laws for $\mathbb{R}$ and, in turn, $\mathbb{C}$ under $+$ are proved in elementary analysis courses when $\mathbb{R}$ is constructed by completing $\mathbb{Q}$ — ultimately, associativity is again a consequence of associativity for $\mathbb{Z}$. The associative axiom for multiplication may be established via a similar development, starting first with $\mathbb{Z}$. Since $\mathbb{R}$ and $\mathbb{C}$ will be used largely for illustrative purposes and we shall not construct $\mathbb{R}$ from $\mathbb{Q}$ (although we shall construct $\mathbb{C}$ from $\mathbb{R}$) we shall take the associative laws (under $+$ and $\times$) for $\mathbb{R}$ and $\mathbb{C}$ as given.

Examples (continued)

(3) The axioms for a vector space V include those axioms which specify that $(V, +)$ is an abelian group (the operation $+$ is called vector addition). Thus any vector space such as $\mathbb{R}^n$ is, in particular, an additive group.

(4) For $n \in \mathbb{Z}^+$, $\mathbb{Z}/n\mathbb{Z}$ is an abelian group under the operation $+$ of addition of residue classes as described in Chapter 0. We shall prove in Chapter 3 (in a more general context) that this binary operation $+$ is well defined and associative; for now we take this for granted. The identity in this group is the element $\bar{0}$ and for each $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$, the inverse of $\bar{a}$ is $\overline{-a}$. Henceforth, when we talk about the group $\mathbb{Z}/n\mathbb{Z}$ it will be understood that the group operation is addition of classes mod n.

(5) For $n \in \mathbb{Z}^+$, the set $(\mathbb{Z}/n\mathbb{Z})^\times$ of equivalence classes $\bar{a}$ which have multiplicative inverses mod n is an abelian group under *multiplication* of residue classes as described in Chapter 0. Again, we shall take for granted (for the moment) that this operation is well defined and associative. The identity of this group is the element $\bar{1}$ and, by

definition of $(\mathbb{Z}/n\mathbb{Z})^\times$, each element has a multiplicative inverse. Henceforth, when we talk about the group $(\mathbb{Z}/n\mathbb{Z})^\times$ it will be understood that the group operation is multiplication of classes mod n.

(6) If $(A, \star)$ and $(B, \diamond)$ are groups, we can form a new group $A \times B$, called their *direct product*, whose elements are those in the Cartesian product

$$A \times B = \{(a, b) \mid a \in A,\ b \in B\}$$

and whose operation is defined componentwise:

$$(a_1, b_1)(a_2, b_2) = (a_1 \star a_2, b_1 \diamond b_2).$$

For example, if we take $A = B = \mathbb{R}$ (both operations addition), $\mathbb{R} \times \mathbb{R}$ is the familiar Euclidean plane. The proof that the direct product of two groups is again a group is left as a straightforward exercise (later) — the proof that each group axiom holds in $A \times B$ is a consequence of that axiom holding in both A and B together with the fact that the operation in $A \times B$ is defined componentwise.

There should be no confusion between the groups $\mathbb{Z}/n\mathbb{Z}$ (under addition) and $(\mathbb{Z}/n\mathbb{Z})^\times$ (under multiplication), even though the latter is a subset of the former — the superscript $\times$ will always indicate that the operation is multiplication.

Before continuing with more elaborate examples we prove two basic results which in particular enable us to talk about *the* identity and *the* inverse of an element.

Proposition 1. If G is a group under the operation $\star$, then

(1) the identity of G is unique

(2) for each $a \in G$, a^{-1} is uniquely determined

(3) $(a^{-1})^{-1} = a$ for all $a \in G$

(4) $(a \star b)^{-1} = (b^{-1}) \star (a^{-1})$

(5) for any $a_1, a_2, \ldots, a_n \in G$ the value of $a_1 \star a_2 \star \cdots \star a_n$ is independent of how the expression is bracketed (this is called the *generalized associative law*).

Proof: (1) If f and g are both identities, then by axiom (ii) of the definition of a group $f \star g = f$ (take $a = f$ and $e = g$). By the same axiom $f \star g = g$ (take $a = g$ and $e = f$). Thus $f = g$, and the identity is unique.

(2) Assume b and c are both inverses of a and let e be the identity of G. By axiom (iii), $a \star b = e$ and $c \star a = e$. Thus

$$\begin{aligned} c &= c \star e && \text{(definition of } e \text{ - axiom (ii))} \\ &= c \star (a \star b) && \text{(since } e = a \star b \text{)} \\ &= (c \star a) \star b && \text{(associative law)} \\ &= e \star b && \text{(since } e = c \star a \text{)} \\ &= b && \text{(axiom (ii)).} \end{aligned}$$

(3) To show $(a^{-1})^{-1} = a$ is exactly the problem of showing a is the inverse of a^{-1} (since by part (2) a has a unique inverse). Reading the definition of a^{-1}, with the roles of a and a^{-1} mentally interchanged shows that a satisfies the defining property for the inverse of a^{-1}, hence a is the inverse of a^{-1}.

(4) Let $c = (a \star b)^{-1}$ so by definition of c, $(a \star b) \star c = e$. By the associative law

$$a \star (b \star c) = e.$$

Multiply both sides on the left by a^{-1} to get

$$a^{-1} \star (a \star (b \star c)) = a^{-1} \star e.$$

The associative law on the left hand side and the definition of e on the right give

$$(a^{-1} \star a) \star (b \star c) = a^{-1}$$

so

$$e \star (b \star c) = a^{-1}$$

hence

$$b \star c = a^{-1}.$$

Now multiply both sides on the left by b^{-1} and simplify similarly:

$$\begin{aligned} b^{-1} \star (b \star c) &= b^{-1} \star a^{-1} \\ (b^{-1} \star b) \star c &= b^{-1} \star a^{-1} \\ e \star c &= b^{-1} \star a^{-1} \\ c &= b^{-1} \star a^{-1}, \end{aligned}$$

as claimed.

(5) This is left as a good exercise using induction on n. First show the result is true for $n = 1, 2$, and 3. Next assume for any $k < n$ that any bracketing of a product of k elements, $b_1 \star b_2 \star \cdots \star b_k$ can be reduced (without altering the value of the product) to an expression of the form

$$b_1 \star (b_2 \star (b_3 \star (\cdots \star b_k)) \ldots).$$

Now argue that any bracketing of the product $a_1 \star a_2 \star \cdots \star a_n$ must break into 2 subproducts, say $(a_1 \star a_2 \star \cdots \star a_k) \star (a_{k+1} \star a_{k+2} \star \cdots \star a_n)$, where each sub-product is bracketed in some fashion. Apply the induction assumption to each of these two sub-products and finally reduce the result to the form $a_1 \star (a_2 \star (a_3 \star (\cdots \star a_n)) \ldots)$ to complete the induction.

Note that throughout the proof of Proposition 1 we were careful not to change the *order* of any products (unless permitted by axioms (ii) and (iii)) since G may be non-abelian.

Notation:

(1) For an abstract group G it is tiresome to keep writing the operation $\star$ throughout our calculations. Henceforth (except when necessary) our abstract groups G, H, *etc.* will always be written with the operation as $\cdot$ and $a \cdot b$ will always be written as ab. In view of the generalized associative law, products of three or more group elements will not be bracketed (although the operation is still a binary operation). Finally, for an abstract group G (operation $\cdot$) we denote the identity of G by 1.

(2) For any group G (operation $\cdot$ implied) and $x \in G$ and $n \in \mathbb{Z}^+$ since the product $xx \cdots x$ (n terms) does not depend on how it is bracketed, we shall denote it by x^n. Denote $x^{-1}x^{-1} \cdots x^{-1}$ (n terms) by x^{-n}. Let $x^0 = 1$, the identity of G.

This new notation is pleasantly concise. Of course, when we are dealing with specific groups, we shall use the natural (given) operation. For example, when the operation is $+$, the identity will be denoted by 0 and for any element a, the inverse a^{-1} will be written $-a$ and $a+a+\cdots+a$ ($n > 0$ terms) will be written na; $-a-a\cdots-a$ (n terms) will be written $-na$ and $0a = 0$.

Proposition 2. Let G be a group and let $a, b \in G$. The equations $ax = b$ and $ya = b$ have unique solutions for $x, y \in G$. In particular, the left and right cancellation laws hold in G, i.e.,

(1) if $au = av$, then $u = v$, and

(2) if $ub = vb$, then $u = v$.

Proof: We can solve $ax = b$ by multiplying both sides on the left by a^{-1} and simplifying to get $x = a^{-1}b$. The uniqueness of x follows because a^{-1} is unique. Similarly, if $ya = b$, $y = ba^{-1}$. If $au = av$, multiply both sides on the left by a^{-1} and simplify to get $u = v$. Similarly, the right cancellation law holds.

One consequence of Proposition 2 is that if a is any element of G and for some $b \in G$, $ab = e$ or $ba = e$, then $b = a^{-1}$, i.e., we do not have to show both equations hold. Also, if for some $b \in G$, $ab = a$ (or $ba = a$), then b must be the identity of G, i.e., we do not have to check $bx = xb = x$ for all $x \in G$.

Definition. For G a group and $x \in G$ define the *order* of x to be the smallest positive integer n such that $x^n = 1$, and denote this integer by $|x|$. In this case x is said to be of order n. If no positive power of x is the identity, the order of x is defined to be infinity and x is said to be of infinite order.

The symbol for the order of x should not be confused with the absolute value symbol (when $G \subseteq \mathbb{R}$ we shall be careful to distinguish the two). It may seem injudicious to choose the same symbol for order of an element as the one used to denote the cardinality (or order) of a set, however, we shall see that the order of an element in a group is the same as the cardinality of the set of all its (distinct) powers so the two uses of the word "order" are naturally related.

Examples

(1) An element of a group has order 1 if and only if it is the identity.

(2) In the additive groups $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$ every nonzero (i.e., nonidentity) element has infinite order.

(3) In the multiplicative groups $\mathbb{R} - \{0\}$ or $\mathbb{Q} - \{0\}$ the element -1 has order 2 and all other nonidentity elements have infinite order.

(4) In the additive group $\mathbb{Z}/9\mathbb{Z}$ the element $\bar{6}$ has order 3, since $\bar{6} \neq \bar{0}$, $\bar{6}+\bar{6} = \overline{12} = \bar{3} \neq \bar{0}$, but $\bar{6}+\bar{6}+\bar{6} = \overline{18} = \bar{0}$, the identity in this group. Recall that in an *additive* group the powers of an element are the integer multiples of the element. Similarly, the order of the element $\bar{5}$ is 9, since 45 is the smallest positive multiple of 5 that is divisible by 9.