5. Basic Properties of Groups

Lemma 5.1. *Let G be a group.*

(1) G contains exactly one identity element.
(2) Every element of G contains exactly one inverse.
(3) Let a and b be any two elements of G. Then the equation

$$ax = b$$

has exactly one solution in G, namely $x = a^{-1}b$.
(4) Let a and b be any two elements of G. Then the equation

$$ya = b$$

has exactly one solution, namely $y = ba^{-1}$.
(5) For every $a \in G$,

$$(a^{-1})^{-1} = a.$$

In words the inverse of the inverse of a is a.
(6) For every a and b in G,

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

That is, the inverse of a product is the product of the inverses, in the opposite order.

Proof. We first prove (1).

By definition G has to contain at least one identity element. Suppose that both e and f are identity elements in G. We compute the product ef.

As e is an identity in G,

$$ef = f.$$

On the other hand as f is an identity in G,

$$ef = e.$$

Thus $e = ef = f$. Thus the identity is unique. Hence (1).

Now we prove (2). Suppose that g is an element of G. Then g has at least one inverse by definition. Suppose that there were two elements h and k that were both inverses of g. We compute hgk (by associativity we can drop the parentheses). On the one hand we get

$$\begin{aligned} hgk &= (hg)k && \text{by associativity} \\ &= ek && \text{property of inverse} \\ &= k && \text{property of identity.} \end{aligned}$$

On the other hand

$$\begin{aligned} hgk &= h(gk) \qquad \text{by associativity} \\ &= he \qquad \text{property of inverse} \\ &= h \qquad \text{property of identity.} \end{aligned}$$

Thus $h = hgk = k$. Thus g has only one inverse and (2) holds.

Suppose that $x \in G$ is a solution to the equation

$$ax = b.$$

Multiply both sides by a^{-1}. We get

$$a^{-1}(ax) = a^{-1}b.$$

By associativity the LHS is equal to

$$(a^{-1}a)x = ex = x.$$

Thus $x = a^{-1}b$. Now we check that this is indeed a solution of the equation,

$$a(a^{-1}b) = (aa^{-1})b = eb = b.$$

Thus $x = a^{-1}b$ is the unique solution to the equation

$$ax = b.$$

Hence (3). (4) is similar to (3) and is left as an exercise for the reader.

Now we prove (5). Let $b = a^{-1}$ and $c = b^{-1} = (a^{-1})^{-1}$. We want to prove that $c = a$. This follows from (2), if we can show that both a and c are the inverse of b. c is by definition an inverse of b.

We check that a is also an inverse of b. We have

$$ab = aa^{-1} = e \qquad \text{and} \qquad ba = a^{-1}a = e.$$

So a is an inverse of b. By uniqueness of the inverse $a = c$. Hence (5).

Finally we prove (6). Suppose $c = b^{-1}a^{-1}$. We have to check that

$$(ab)c = c(ab) = e.$$

But

$$\begin{aligned} (ab)c &= (ab)(b^{-1}a^{-1}) \qquad \text{substituting for } c \\ &= a(bb^{-1})a^{-1} \qquad \text{by associativity} \\ &= a(e)a^{-1} \qquad \text{property of inverses} \\ &= (ae)a^{-1} \qquad \text{by associativity} \\ &= aa^{-1} \qquad \text{property of identity} \\ &= e \qquad \text{property of inverses,} \end{aligned}$$

and

$$\begin{aligned} c(ab) &= (b^{-1}a^{-1})(ab) && \text{substituting for } c \\ &= b^{-1}(a^{-1}a)b && \text{by associativity} \\ &= b^{-1}(e)b && \text{property of inverses} \\ &= (a^{-1}e)a && \text{by associativity} \\ &= a^{-1}a && \text{property of identity} \\ &= e && \text{property of inverses.} \end{aligned}$$

Thus c is the inverse of ab. Hence (6). □

In some sense, results (3) and (4) of (5.1) are the reason for the axioms of a group. One wants a minimal set of axioms that allows one to mimic the standard methods of algebra in a much larger context than ordinary arithmetic of numbers.

Let us go back to the problem of classifying groups of small order. Suppose that we start with $\{e, a, b\}$ where e is the identity.

Using the property of the identity we get

$*$	e	a	b
e	e	a	b
a	a	?	
b	b		

The only question is how to fill in the four spaces. The point is to use rules (3) and (4) of (5.1). Translated to the context of multiplication tables, these rules state that every row contains a permutation of the set $\{e, a, b\}$ and so does every column. Now the row corresponding to a already contains the entry a. So in the middle we can either put e or b. Let us try to put e. Then we get

$*$	e	a	b
e	e	a	b
a	a	e	?
b	b		

But this forces the rest of the entries of the table and in fact we are stuck, since looking at the row that contains a we ought to put in the entry b. But looking at the column that contains b we must put in anything other than b.

So putting e as the first question mark was wrong. Instead lets try putting b.

$*$	e	a	b
e	e	a	b
a	a	b	
b	b		

But this forces the rest of the entries of the table,

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

With this choice of multiplication, there is an identity and every element has an inverse (a is the inverse of b and vice-versa). It remains to check associativity. Can we avoid this?

The answer is yes, because we know that there is at least one group of order 3, the group of rotations of a triangle. So this must be its group table.

It is curious to see what the group table looks like in terms of rotations.

$*$	I	R	R^2
I	I	R	R^2
R	R	R^2	R
R^2	R^2	I	$R.$

For example, we can think of a as corresponding to R and b as corresponding to R^2.