Groups

1 Definition of a group

Definition 1.1. A *group* is a binary structure $(X, *)$ such that $*$ is associative, there exists an identity element for $*$, and every $x \in X$ has an inverse for $*$. Note that the identity e and the inverse x' of an element x are unique.

Example 1.2. (1) Groups where the operation is denoted $+$: $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, as well as vector space and matrix examples such as $(\mathbb{R}^n, +)$ or $(\mathbb{M}_{n,m}(\mathbb{R}), +)$.

(2) Groups where the operation is denoted $\cdot$: $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$ as well as $(U(1), \cdot)$ and $(\mu_n, \cdot)$.

(3) Groups of matrices under matrix multiplication: $(GL_n(\mathbb{R}), \cdot)$, $(SL_n(\mathbb{R}), \cdot)$, $(O_n, \cdot)$, $(SO_n, \cdot)$.

(4) $(S_X, \circ)$.

(5) Equivalence classes: $(\mathbb{Z}/n\mathbb{Z}, +)$ and $(\mathbb{R}/2\pi\mathbb{Z}, +)$.

Note that the groups $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$, as well as $(GL_n(\mathbb{R}), \cdot)$ and $(S_X, \circ)$, are all constructed following a similar principle: start with a binary structure $(X, *)$ which is associative and for which an identity exists. Then define $X' \subseteq X$ to be the subset of invertible elements. By (ii) of Proposition 3.3 of the notes on binary operations, X' is closed under $*$, i.e. for all $x, y \in X'$, $x * y \in X'$. It is then easy to see that $(X', *)$ is a group: associativity is inhrited from associativity in the larger set X, e is invertible since $e' = e$, and by definition every element of X' has an inverse, which is also in X'. Here $(\mathbb{Q}^*, \cdot)$ arises in this way from $(\mathbb{Q}, \cdot)$ (the only element without a multiplicative inverse is 0), and similarly for $(\mathbb{R}^*, \cdot)$ and $(\mathbb{C}^*, \cdot)$. By definition, $GL_n(\mathbb{R})$ is the subset if invertible elements in $M_n(\mathbb{R})$, and S_X is the set of functions with inverses in X^X.

From now on we will usually denote a group by $(G, *)$. In fact, the use of the letter G is so ingrained that mathematicians will usually automatically assume that the symbol G denotes a group.

Definition 1.3. Let $(G, *)$ be a group. Then G is *abelian* if $*$ is commutative.

The examples of the matrix groups and $(S_n, \circ)$, $n \geq 3$, show that there are a lot of interesting groups which are not abelian.

Groups occur naturally in mathematics in various ways:

1. Groups of numbers: $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ and $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$. These groups are the most familiar, but will also be the least interesting to us.

2. The groups $(\mathbb{Z}, +)$ and $(\mathbb{Z}/n\mathbb{Z}, +)$: these groups are connected with elementary number theory (in ways which we shall describe) as well as with periodic or repeating phenomena in the case of $(\mathbb{Z}/n\mathbb{Z}, +)$ (seven days in a week, 12 months in a year, ...)

3. Matrix groups: $(GL_n(\mathbb{R}), \cdot)$, $(SL_n(\mathbb{R}), \cdot)$, $(O_n, \cdot)$, $(SO_n, \cdot)$. These are naturally connected with linear algebra, but also (because SO_n is the rigid motions of $\mathbb{R}^n$ fixing 0) with physics and chemistry. For example, the laws of physics should be "invariant" under SO_3, thought of as changing rectangular coordinates in $\mathbb{R}^3$. Modern particle physics is based on this idea but for much more exotic symmetry groups. Also, these groups and their analogues have become very important in number theory, for example in the mathematics used to prove Fermat's last theorem.

4. The group S_n of permutations of the set $\{1, \ldots, n\}$ records the ways to shuffle a deck of n cards and is important in combinatorics and probability.

5. Certain symmetries of geometric objects such as a regular n-gon, or one of the 5 Platonic solids (the tetrahedron, cube, octahedron, dodecahedron, or icosahedron), or Rubik's cube, are important to understanding various patterns. Examples: repeating wallpaper patterns, crystals.

6. Many interesting infinite groups arise in topology and geometry.

In this course, our main interest will be in understanding **finite groups**.

2 Product groups

One way to construct new groups from old is via *product groups*:

Definition 2.1. Let $(X_1, *_1)$ and $(X_2, *_2)$ be two binary structures. We define the *product binary structure* to be the set $X_1 \times X_2$, together with the binary operation $*$ defined by: for all $(x_1, x_2), (y_1, y_2) \in X_1 \times X_2$,

$$(x_1, x_2) * (y_1, y_2) = (x_1 *_1 y_1, x_2 *_2 y_2).$$

In other words, we combine the elements of the product by combining in each component. The product of n binary operations $(X_1, *_1), \ldots, (X_n, *_n)$ is defined in a similar way.

It is easy to see:

Lemma 2.2. *If $(G_1 *_1)$ and $(G_2, *_2)$ are groups, then $(G_1 \times G_2, *)$ is a group. More generally, we can define the Cartesian product $G_1 \times \cdots \times G_n$ of n groups and it is a group.*

Proof. A tedious but straightforward argument shows that, if $(X_1, *_1)$ and $(X_2, *_2)$ are two associative binary structures, then the product binary structure on $X_1 \times X_2$ is associative. Thus $(G_1 \times G_2, *)$ is associative. The element (e_1, e_2) is an identity for $G_1 \times G_2$, where e_1 is the identity for G_1 and e_2 is the identity for G_2. If $(g_1, g_2) \in G_1 \times G_2$, then (g_1', g_2') is an inverse for (g_1, g_2). □

For example, $\mathbb{R}^2$ and more generally $\mathbb{R}^n$ are examples of this construction. Here, since the group operation on $\mathbb{R}$ is $+$, the identity in $\mathbb{R}^n$ is the zero vector $(0, \ldots, 0)$ and the inverse of $(v_1, \ldots, v_n)$ is $-(v_1, \ldots, v_n) = (-v_1, \ldots, -v_n)$.

If If $(G_1 *_1)$ and $(G_2, *_2)$ are finite groups, then $(G_1 \times G_2, *)$ is also a finite group, and $\#(G_1 \times G_2) = \#(G_1)\#(G_2)$. For example, $((\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}), +)$ is a group with 4 elements:

$$(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) = \{([0], [0]), ([1], [0]), ([0], [1]), ([1], [1])\}.$$

3 First properties of groups

Here are two easy but fundamental results about groups:

Proposition 3.1 (Cancellation law)**.** *Let $(G, *)$ be a group. Then for all $a, b, c \in G$, if $a * b = a * c$, then $b = c$. Likewise, if $b * a = c * a$, then $b = c$.*

Proof. Suppose for example that $a * b = a * c$. Multiplying both sides on the left by a', the inverse of a, we see that

$$a' * (a * b) = a' * (a * c).$$

But $a' * (a * b) = (a' * a) * b = e * b = b$, and similarly $a' * (a * c) = (a' * a) * c = e * c = c$. Hence $b = c$. The case where $b * a = c * a$ is similar. □

Remark 3.2. If $(G, *)$ is not abelian, there is no "mixed" cancellation law. In other words, if $a * b = c * a$, we can't in general conclude that $b = c$.

Proposition 3.3 (Unique solution of linear equations)**.** *Let $(G, *)$ be a group. Then for all $a, b \in G$, there exists a unique $x \in G$ such that $a * x = b$. In other words, given a, b, the "linear equation" $a * x = b$ has a unique solution $x \in G$. Likewise, for all $a, b \in G$, there exists a unique $y \in G$ such that $y * a = b$. In other words, given a, b, the "linear equation" $y * a = b$ has a unique solution $y \in G$.*

Proof. First we show uniqueness (although this fact is an immediate consequence of the cancellation law). If $a * x = b$, then, multiplying both sides on the left by a', we see that

$$a' * (a * x) = a' * b,$$

and hence, as $a' * (a * x) = (a' * a) * x = e * x = x$, that $x = a' * b$. This establishes uniqueness, but also existence, since if we let $x = a' * b$, then

$$a * x = a * (a' * b) = (a * a') * b = e * b = b.$$

The case of the equation $y * a = b$ is similar. □

Corollary 3.4. *Let $(G, *)$ be a group and let $a \in G$. Define functions $\ell_a \colon G \to G$ and $r_a \colon G \to G$ by the rules:*

$$\ell_a(x) = a * x;$$
$$r_a(x) = x * a.$$

Then, for all $a \in G$, ℓ_a and r_a are bijections from G to G, and hence $\ell_a, r_a \in S_G$.

Proof. The statement that, for all $b \in G$, there exists a unique $x \in G$ such that $a * x = \ell_a(x) = b$ says that ℓ_a is both surjective and injective, hence a bijection. (Alternatively, the function $\ell_{a'}$ is an inverse function, as one sees by checking that

$$\ell_{a'} \circ \ell_a(x) = \ell_a \circ \ell_{a'}(x) = x$$

for all $x \in G$.) The argument for r_a is similar. □

As a consequence, given a finite group $(G, *)$ described by a group table, every row of the table contains every element of G exactly once, and similarly every column of the table contains every element of G exactly once ("Sudoku property").

4 Notation and conventions; exponents

We have already seen that we will use the letter G when discussing groups. Also, we will usually speak of a "group G" instead of a "group $(G, *)$," since the binary operation will usually be clear from the context or will be the only possible obvious binary operation for which $(G, *)$ is a group. For example, if we say "the group $\mathbb{Z}$," we will understand that the operation is $+$, since $\mathbb{Z}$ is not a group under $\cdot$ and still less so under $-$. Likewise, the only natural operation on $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ which yield groups is $+$, and the only natural operation on $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$, $U(1)$, μ_n which yield groups is $\cdot$. For the matrix groups $GL_n(\mathbb{R})$, $SL_n(\mathbb{R})$, O_n, SO_n, the operation is always understood to be matrix multiplication, and for S_X or S_n it is function composition $\circ$ (which we will end up abbreviating by $\cdot$ in any case).

Next, we will drop the use of exotic symbols such as $*$ to denote the binary operation on a group. Typically, we will use $+$ or $\cdot$ to denote the operation, and for $\cdot$, we will usually just write ab instead of $a \cdot b$. Another convention is that $+$ is **always abelian**, whereas $\cdot$ might or might not be abelian. In case the operation is denoted $+$, we will denote the identity element by 0 (or occasionally $\mathbf{0}$ or O if we are discussing vectors or matrices) and the inverse of an element g by $-g$. In case the operation is $\cdot$, we will denote the identity by 1 (or occasionally I or Id or Id_X) and the inverse of an element g by g^{-1}. (For various reasons, we tend not to use $1/g$.)

If we are discussing results about a general group G, we will usually use $\cdot$ to denote the operation, leaving open the possibility that G is or is not abelian.

If G is finite, we call $\#(G)$, the number of elements of G, the *order* of G and say that G has *finite order*. (Some people write $|G|$ for $\#(G)$.) If G is infinite, we say that G has *infinite order*.

Next we turn to exponential notation. Given a group G, where the operation is $\cdot$, we abbreviate $g \cdot g$ by g^2 and, for $n \in \mathbb{N}$, we define g^n inductively by: $g^{n+1} = g \cdot g^n$. It is easy to see (and will follow from what we say below) that g^{n+1} is also equal to $g^n \cdot g$. As with the usual kinds of numbers, we define $g^0 = 1$ (here the 1 on the right denotes the identity in G), g^{-1} to be the inverse of g (so this is consistent with our convention above), and, for $n \in \mathbb{N}$, we define $g^{-n} = (g^{-1})^n$. Thus g^n is defined for all $n \in \mathbb{Z}$.

There is analogous notation for operations written $+$. We write $g + g = 2 \cdot g$ and define $n \cdot g$ by the inductive formula $(n+1) \cdot g = n \cdot g + g$. Then we let $0 \cdot g = 0$, where the 0 on the left is the integer 0 and the 0 on the right is the identity in G. Finally, set $(-1) \cdot g = -g$ and $(-n) \cdot g = -(n \cdot g)$.

Then $n \cdot g$ is defined for all $n \in G$, but it is not a product in any usual sense, especially since $\mathbb{Z}$ will not usually be a subset of G, but rather it is an additive version of an exponential. However, for $G = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, $n \cdot x$ is the same thing as the product nx, viewing $\mathbb{Z}$ as a subset of $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

The laws of exponents become: for all $g \in G$ and $n, m \in \mathbb{Z}$,

$$g^n \cdot g^m = g^{n+m};$$
$$(g^n)^m = g^{nm}.$$

Note that the first law implies that

$$g^n \cdot g^m = g^{n+m} = g^{m+n} = g^m \cdot g^n.$$

This says that, even if G is not abelian, every power of an element g commutes with every other power of the **same** element g. In case G is not abelian, however, we **do not** have the other usual law of exponents $(gh)^n = g^n h^n$. For example, $(gh)^2 = ghgh$, and it is easy to see that this is equal to $g^2h^2 \iff gh = hg$.

We won't write down a proof of these laws, but the proofs for a general group are the same as the proofs for rational numbers, say: they follow easily via induction, after breaking up into the various cases for n, m.

The additive version of these laws is as follows: if $(G, +)$ is a group (assumed abelian because of the choice of notation), then, for all $g \in G$ and $n, m \in \mathbb{Z}$,

$$(n \cdot g) + m \cdot g = (n + m) \cdot g;$$
$$m \cdot (n \cdot g) = (nm) \cdot g.$$

Because G is abelian, we also have the remaining law

$$n \cdot (g + h) = (n \cdot g) + (n \cdot h).$$

Lastly we define the *order* of an element.

Definition 4.1. Let G be a group and let $g \in G$. If there exists an $n \in \mathbb{N}$ such that $g^n = 1$, we say g has *finite order*. In this case, the smallest possible n (which exists because of the well-ordering principle) is called the *order* of g. If g does not have finite order, we say that the order of g is *infinite*.

Note that the identity of G is the unique element of order 1. If G is written additively, then $g \in G$ has finite order if exists an $n \in \mathbb{N}$ such that $n \cdot g = 0$, and the smallest such n is then the order of g.

Example 4.2. (1) In $\mathbb{Z}$, 0 has order 1, but every other element has infinite order, since, for $a \in \mathbb{Z}$, $a \neq 0$, and $n \in \mathbb{N}$, $n \cdot a = na$ is never 0. Similarly, every nonzero element of $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$ has infinite order.

(2) In $\mathbb{R}^*$, an element of finite order n is in particular an element $x \in \mathbb{R}$ such that $x^n = 1$, $n \geq 1$. Clearly 1 has order 1, and the only other element of finite order is -1, which has order 2.

(3) In $\mathbb{C}^*$, there are lots of elements of finite order. In fact, an element of finite order is the same thing as an n^{th} root of unity, so the set of all finite order elements of $\mathbb{C}^*$ is $\bigcup_{n=1}^{\infty} \mu_n$, the set of all n^{th} roots of unity.

(4) In $\mathbb{Z}/4\mathbb{Z}$, computation shows that the order of $[0]$ is 1, the order of $[1]$ is 4, the order of $[2]$ is 2, and the order of $[3]$ is 4. What are the possible orders of the elements of $\mathbb{Z}/4\mathbb{Z}$?

(5) In $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, every element has order 1 (if $([0],[0])$) or 2 (otherwise).