

Group Theory

Sophie Huczynska

October 2, 2003

Chapter 1.

Definitions and examples

1. Definitions, basic properties and isomorphisms

Algebra is a part of mathematics which studies abstract sets with certain operations defined on them. Group theory is one of the key subjects in algebra.

Definition 1.1. A *group* is a set G , together with a binary operation $*$, such that the following axioms hold:

Closure: G is closed under the operation $*$: $x, y \in G \implies x * y \in G$;

Associativity: $(x * y) * z = x * (y * z)$ for all $x, y, z \in G$;

Identity: there exists an element $e \in G$ (called the identity of G) such that $x * e = e * x = x$ for all $x \in G$;

Inverses: for every element $x \in G$ there exists an element $x^{-1} \in G$ (called the inverse of x) such that $x * x^{-1} = x^{-1} * x = e$.

Remark 1.2. *It is usual, when working with groups, to replace $*$ by \cdot , or even omit the dot altogether and simply juxtapose the elements being combined, i.e. $x * y$ is written $x \cdot y$ or simply xy . We call this method of combination “multiplication”, and $x * y$ (or xy) the “product” of x and y . The identity element e may also be written as 1_G or just 1 .*

Associativity allows us to write abc for either of $(ab)c$ or $a(bc)$. More generally, if x_1, \dots, x_n are group elements then $x_1x_2\dots x_n$ is unambiguous (the same however we bracket it). This in turn enables one to use the power notation:

$$a^n = \begin{cases} \underbrace{aa \dots a}_{n} & \text{if } n > 0 \\ \underbrace{a^{-1}a^{-1} \dots a^{-1}}_{-n} & \text{if } n < 0 \\ e & \text{if } n = 0. \end{cases}$$

Theorem 1.3. *The following statements are true for any group G .*

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

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

(iii) *The identity element e is unique.*

(iv) *The inverse of any element is unique.*

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

(vi) $(ab)^{-1} = b^{-1}a^{-1}$ for all $a, b \in G$. ■

Definition 1.4. The *order* of a group G (denoted by $|G|$) is the number of elements of G .

Definition 1.5. A group G is said to be *abelian* if the binary operation $*$ is commutative, i.e. if $x * y = y * x$ for all $x, y \in G$.

Remark 1.6. *By convention, the operation $*$ is often replaced by $+$ for abelian groups, i.e. $x * y$ is written $x + y$ (and the commutative law is written in the form $x + y = y + x$ for all $x, y \in G$).*

The basic, general (and impossible) task of group theory is to classify all groups. The first trivial but important step is to realize that not all the groups that seem to be different are in fact different. For example consider the multiplicative group $\{1, -1\}$ and the group $\{0, 1\}$ under addition modulo 2. The multiplication tables for these two groups are

$$\begin{array}{c|cc} & 1 & -1 \\ \hline 1 & 1 & -1 \\ -1 & -1 & 1 \end{array} \quad \begin{array}{c|cc} & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array}$$

(where the product xy lies at the intersection of the *row* x and *column* y).

We see that these two tables differ only by the names of the elements.

Let us make this more formal.

Definition 1.7. Two groups $(G, *)$ and (H, \circ) are said to be *isomorphic* ($G \cong H$) if there is a bijection $f : G \rightarrow H$, which agrees with their structures, in the sense that

$$(x * y)f = (xf) \circ (yf),$$

for all $x, y \in G$. Any such mapping is called an *isomorphism*.

Where no confusion is likely to arise, we generally use the more compact notation

$$(xy)f = (xf)(yf).$$

This definition means that isomorphic groups ‘look the same’: one can be obtained from the other by simply renaming the elements. It is clear that \cong is an equivalence relation, in the sense that for any groups G, H, K we have: $G \cong G$; $G \cong H \Rightarrow H \cong G$; $G \cong H \wedge H \cong K \Rightarrow G \cong K$. Thus the class of all groups is split into *isomorphism classes*. From the point of view of group theory, groups belonging to the same class are considered to be identical. The general task of group theory can now be rephrased as describing all the groups up to isomorphism.

2. Examples of groups

In this section we give some examples of groups; further examples will be given in the following sections.

Groups of numbers

The sets \mathbb{Z} of integers, \mathbb{Q} of rationals, \mathbb{R} of reals, and \mathbb{C} of complex numbers all form abelian groups under addition. Also the set $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ under addition modulo n forms a group. \mathbb{N} does *not* form a group under addition (no identity 0 and no inverses).

None of the above sets is a group with respect to multiplication. However, if 0 is removed from the sets $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, multiplicative groups are obtained. $\mathbb{Z} \setminus \{0\}$ is not a group under multiplication, as no element apart from 1 and -1 has an inverse. The set $\mathbb{Z}_n \setminus \{0\}$ is a group under the multiplication if and only if n is a prime.

Symmetric groups S_n

Let X be an arbitrary set. A *permutation* on X is a bijection from X onto X . The set of all permutations of X is denoted by S_X . Given two permutations $\sigma, \tau \in S_X$, their product is defined to be their composition as mappings. Since we write mappings on the right, this means that to calculate the product $\sigma\tau$, one first applies σ and then τ ; symbolically: $i(\sigma\tau) = (i\sigma)\tau$, where $i \in X$. It is well known that the composition of two bijections is again a bijection, that composition of mappings is associative, that the identity mapping (sending each i into itself) acts as an identity element, and that each bijection has an inverse which is also a bijection. Hence S_X is a group; it is usually called the

symmetric group on X . If X is finite with n -elements, then we can simply assume that $X = \{1, \dots, n\}$. In this case we write S_X as S_n ; this is a finite group of order $n!$.

One may write permutations as mappings, specifying images of all elements of X . Thus, for example

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} \text{ and } \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

are two permutations from S_4 . According to our definition, their product is

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}.$$

The inverse of a permutation is obtained by interchanging the top and bottom rows (and reordering). For example

$$\sigma^{-1} = \begin{pmatrix} 3 & 1 & 2 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}.$$

If we calculate

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$$

we see that S_4 is not abelian. One can construct similar examples to show that S_n is not abelian for $n \geq 3$. It is also easy to check that S_1 and S_2 are abelian.

Another way to denote permutations is as products of disjoint cycles. A *cycle* $(i_1 i_2 \dots i_r)$ is the permutation sending i_1 into i_2 , i_2 into i_3 , etc., sending i_{r-1} into i_r , sending i_r into i_1 , and leaving all the other elements fixed. The number r is referred to as the *length* of the cycle, and is at the same time its order. Two cycles are *disjoint* if no element is moved by both of them; disjoint cycles commute. It is well known that every permutation from S_n can be written as a product of disjoint cycles, and that this decomposition is unique up to the order of factors. For example, the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 6 & 5 & 2 & 7 & 4 & 1 & 8 \end{pmatrix}$$

can be written as

$$\sigma = (1\ 3\ 5\ 7)(2\ 6\ 4).$$

A cycle of length 2 is called a *transposition*. Note that every cycle can be written as a product of transpositions:

$$(i_1 i_2 \dots i_k) = (i_{k-1} i_k) \dots (i_2 i_3)(i_1 i_2).$$

Therefore every permutation can be written as a product of transpositions. However, this decomposition is not unique.

General linear groups

Let \mathbb{F} be a field (typically \mathbb{Q} or \mathbb{R} or \mathbb{C} or \mathbb{Z}_p , where p is a prime), let $n \geq 2$, and let us consider the set of all $n \times n$ matrices with entries from \mathbb{F} . It is well known that the multiplication of matrices is associative, and that the identity matrix I (with ones on the diagonal and zeros elsewhere) is the identity element for the multiplication. However, not every matrix has an inverse, and so the set of all matrices is not a group. However, if we restrict our attention to those matrices which do have inverses (which are exactly those which have non-zero determinants), we obtain a group. This group is called the *general linear group* (of dimension n over \mathbb{F}) and is denoted by $GL(n, \mathbb{F})$. It is known that the multiplication of matrices is non-commutative, so that we have further examples of non-abelian groups.

Quaternion group Q_8

This group consists of elements $1, -1, i, -i, j, -j, k, -k$. Here the first four of them are the usual complex numbers (i being the imaginary unit). j and k are two further imaginary units. They multiply according to the rules:

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j.$$

The full multiplication table is

	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

Klein four group K_4

It is given by the following multiplication table:

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Example 2.1. “Real life” examples of the Klein four group

(i) Let G consist of the following symmetries of the rectangle:

$$\begin{aligned}e &= \text{identity mapping from the plane to itself} \\a &= \text{reflection in } x\text{-axis} \\b &= \text{reflection in } y\text{-axis} \\c &= \text{half-turn (i.e. rotation through } 180^\circ\text{)}\end{aligned}$$

We may check that $a^2 = b^2 = c^2 = e$; $ab = ba = c$, $bc = cb = a$ and $ca = ac = b$, and so G is closed under multiplication. Other properties of isometries of the plane show that G is a group. Specifically, comparison with the multiplication table above shows that G is a Klein four group.

(ii) Let G consist of the following permutations of S_4 :

$$\begin{aligned}e &= \text{identity permutation of } \{1,2,3,4\} \\a &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = (1\ 4)(2\ 3) \\b &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (1\ 2)(3\ 4) \\c &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (1\ 3)(2\ 4)\end{aligned}$$

We may check that this is a Klein four group. Moreover, if we think of the numbers 1-4 as corresponding to the corners of the rectangle in part (i), we may easily see the correspondence between the two examples.