Basic Axioms and definitions

We start with a set of definitions that will help us define the main object of interest this semester: a group.
A binary operation $*$ on a set G is a function of the form $* : G \times G \to G$. We write $a * b$ or ab for short (since groups will only have one binary operation associated with them).

Definition. A *group* is a pair $(G, *)$ where G is a set and $*$ is a binary operation on G if Def. 1.1 p.16

(0) G is closed under $*$. This is included in the definition of $*$ but it is often good to check explicitly.

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

(ii) G has an identity element: $\exists e \in G$ such that $a * e = e * a = a$ for all $a \in G$. (e is often written as 1 even when elements of G are not real numbers, since we tend to call $*$ multiplication.)

(iii) G has inverses: for every $a \in G$ there is an element $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$. (Again, the notation a^{-1} suggests that $*$ is multiplication but we use it for any binary group operation.)

The group G is said to be *abelian* or *commutative* if $*$ is commutative: $a * b = b * a$ for all $a, b \in G$.

Note that we usually write G to mean both the group and the set interchangeably. Technically the group is the pair $(G, *)$, but usually we assume that $*$ is understood or only needs to be mentioned once. For the following proposition, practice writing out the proofs yourself, either before reading the proofs in the book, or a few hours or days after reading them.

Proposition 1. If G is a group under the operation $*$, then p.18

(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) $(a * b)^{-1} = b^{-1} * a^{-1}$ for all $a, b \in G$

(5) for any $a_1, \ldots, a_n \in G$, the value of $a_1 * \cdots * a_n$ is idnependent of how the expression is bracketed: generalized associativity.

Definition. We have two definitions of order, one for a group itself and one for individual elements:

- The order $|G|$ of a group G is the number of elements. This notation is the usual notation for cardinality of a set.
- The order $|x|$ of an element x is the smallest $n \in \mathbb{N}$ such that $x^n = e$. Note that this could be infinite.

Exercise 1. For x an element of a group G, show that x and x^{-1} have the same order. 1.1.20

Exercise 2. If x is an element of finite order n in G, prove that the elements $1, x, x^2, \ldots, x^{n-1}$ are all distinct. We can deduce that $|x| \leq |G|$. 1.1.32

Cyclic Group

The cyclic group is in many ways the simplest group structure we have. We can think of it as the set of rotational symmetries of an n-gon.

Example. The cyclic group C_4 can be described as the symmetries of a Dutch windmill. We Let r denote a rotation of the square over 90° clockwise. Then the other rotations over 180° and 270° can be expressed as r^2 and r^3 respectively. Then $C_4 = \{1, r, r^2, r^3\}$.

The integers modulo n

Consider the integers $\mathbb{Z}$, and define an equivalence relation $a \sim b$ if $a = b + kn$, for $a, b, k \in \mathbb{Z}$. This generates a partition of the integers into residue classes modulo n. Denote the residue class of an integer a by $\overline{a}$. We can now do modular arithmetic as follows: Sec. 0.3 p.8

$$\overline{a} + \overline{b} = \overline{a + b} \text{ and } \overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

It is not immediately obvious that this is well-defined, but stated in the following Theorem (and proven in the book).

Theorem. *The operations of addition and multiplication on $\mathbb{Z}/n\mathbb{Z}$ defined above are both well-defined: they do not depend on the choice of representatives for the residue classes involved.* Thm. 3 p.9

Exercise 3. Show that $\mathbb{Z}/n\mathbb{Z}$ is a group under addition of residue classes. You may notice a similarity to the cyclic group described in the previous section. These groups are isomorphic, which is a concept that we'll define formally later on in Chapter 1.

Exercise 4. Show that multiplication of residue classes in $\mathbb{Z}/n\mathbb{Z}$ is associative. Then, show that, for $n > 1$, $\mathbb{Z}/n\mathbb{Z}$ is not a group under multiplication of residue classes. 1.1.4 1.1.5

Exercise 5. Find the orders of each element of the additive group $\mathbb{Z}/8\mathbb{Z}$. 1.1.11

Multiplication Tables, Generators and Cayley Diagrams

Given a group G, we need a way to define or present the group. Sometimes it is straighforward to define the binary operation. For example, if we have the group $\mathbb{Z}$ under addition. Other times, for small groups, we may write out a full *multiplication table*, which has rows and columns for each element of G, and shows the value of $g_i g_j$ in entry ij. Such a table may be helpful at times, but it is usually more cumbersome and less informative than other respresentations.

A set of *generators* of a group G is a set of elements of G such that every other element can be expressed in terms of the generators and their inverses. You can compare this (somewhat) to a basis of a vector space in linear algebra. This often makes it easier to understand the structure of the group. Note that groups may have many different possible sets of generators, and that minimal generator sets may have different cardinalities for the same group. We call an equation that is satisfied by the generators a *relation*. If we take a set of generators and a set of relations, such that any other relation in G can be deduced from them, we have a *presentation* of G (i.e. a way to define G). Again, note that presentations are not unique. p.26

One important note about presentations is that when we write $x^n = e$ as one of the relations, this means that $|x| = n$.

Cayley diagrams give us a nice way to visually represent a group. We draw the group elements as points, and then draw an arrow $a \to b$ of label (or color) c if $ac = b$ (or if $ca = b$ depending on which direction we "read" the binary operation). It makes sense to only draw arrows for a set of generators of the group.

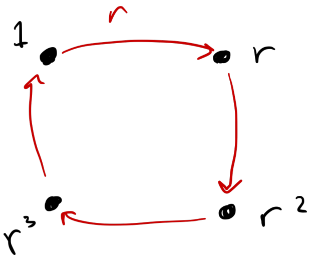
Example. Consider the cyclic group $C_4 = \{1, r, r^2, r^3\}$. Clearly, this group can be generated by r, and the only relation we need to know is that $r^4 = e$. Everything else can be deduced from this. Therefore, we write

$$C_4 = \langle r \mid r^4 = 1 \rangle.$$

We can also write out the full multiplication table:

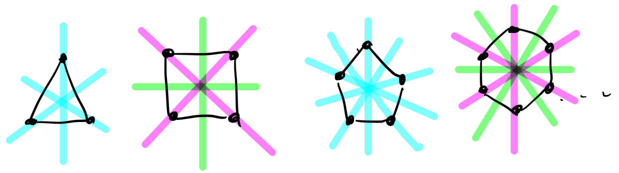
	1	r	r^2	r^3
1	1	r	r^2	r^3
r	r	r^2	r^3	1
r^2	r^2	r^3	1	r
r^3	r^3	1	r	r^2

Or the Cayley Diagram:



Dihedral Group

The dihedral group D_{2n} can be thought of as the set of symmetries of the n-gon, which has both rotational and reflectional symmetry. Note that many other authors use the notation D_n for this group, so be careful. The n-gon has n rotations, over $\frac{360°}{k}$, for $0 \leq k \leq n-1$, denoted by $1, r, \ldots, r^{n-1}$, respectively. And n reflections. We will call one of them s, usually. These reflections look slightly different for odd versus even n-gons. Even n-gons have two types of symmetry axes, while odd n-gons have only one type: p.23



This group is not abelian, and is generated by

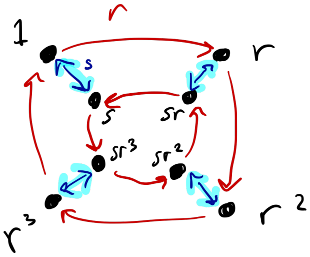
$$D_{2n} = \langle r, s \mid r^n = s^2 = 1,\ rs = sr^{-1} \rangle.$$

For reasons that will become clear later, we read the order of operations from right to left. So, rs means that we reflect first, and then rotate.

Example. The dihedral group D_8 can be described as the symmetries of a square. We Let r denote a rotation of the square over 90° clockwise. Then the other rotations over 180° and 270° can be expressed as r^2 and r^3 respectively. It is generated by

$$D_8 = \langle r, s \mid r^4 = s^2 = 1,\ rs = sr^{-1} \rangle.$$

It has Cayley diagram:



Exercise 6. Use generators and relations to show that if x is any element of D_{2n}, which is not a power of r, then $rx = xr^{-1}$. 1.2.2

The symmetric group

The symmetric groups are some of the most useful and versatile groups. In some sense, which we will see later, every group can be thought of as a subgroup of a symmetric group. So the symmetric groups contain a lot of interesting structure.

Definition. The *symmetric group of degree n*, denoted S_n, is the group whose elements are the permutations on the set $\{1, \ldots, n\}$, and the binary operation is function composition $\circ$. Note that $|S_n| = n!$. p.29

There are different conventions for writing down permutations. We will use the *cycle decomposition* notation most of the time. First, notice that permutations consist of disjoint cycles of the form $a_1 \mapsto a_2, a_2 \mapsto a_3, \ldots, a_k \mapsto a_1$. We write these cycles, starting at their minimum element first. Then we order the cycles by their first element. Finally, we don't write down cycles of length 1 (fixed points), for simplicity of notation. You can find an explicit algorithm and examples on pages 30-31 of D&F.

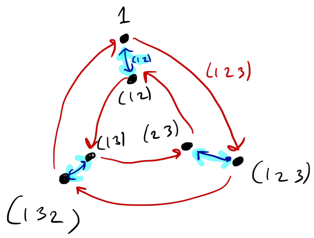
Example. The group S_3 has 3! elements:

$$\begin{aligned} &1 \\ &(1\ 2) \\ &(1\ 3) \\ &(2\ 3) \\ &(1\ 2\ 3) \\ &(1\ 3\ 2). \end{aligned}$$

We see that we can generate this group using elements (1 2) and (1 2 3), such that

$$\begin{array}{l}1\\(1\ 2)\\(1\ 3)=(1\ 2)(1\ 2\ 3)^2\\(2\ 3)=(1\ 2)(1\ 2\ 3)\\(1\ 2\ 3)\\(1\ 3\ 2)=(1\ 2\ 3)^2.\end{array}$$

So, we can draw Cayley diagram:



Compare this to D_6!