1.8 Order of a group

We now introduce the *order* of a group, which is a description of its size. Finite and infinite groups behave quite differently!

Definition 1.52. The **order** of a group G is the number of elements that the set G contains, and is denoted $|G|$.

- If $|G|$ is finite, then G is a *finite group*. In this case, we write $|G| = n$.
- If $|G|$ is infinite, we don't usually make any further distinctions about the cardinality of G. We just write $|G| = \infty$, and say that G is an infinite group.

Exercise 1.53. What is the order of C_n? D_n? $\mathbb{Z}$?

1.9 Order of an element

Given an element x in a group G, we can also define the *order of the element*, which is related to the notion of the order of a group.

Definition 1.54. Let $x \in G$. The **cyclic subgroup generated by** x is

$$\langle x \rangle := \{g \in G \mid g = x^k \text{ for some } k \in \mathbb{Z}\}.$$

Exercise 1.55. Prove that $\langle x \rangle$ really is a subgroup of G.

Notice that we use the notation $\langle \cdot \rangle$ to mean *generated by*. This is similar to the notation we use for generators and relations in a group presentation. We will continue to use this notation. For example, if we want to describe the subgroup generated by a subset $X \subset G$, we can write $\langle X \rangle$.

Definition 1.56. The **order** of an element $x \in G$, denoted $|x|$, is the order of the cyclic subgroup $\langle x \rangle$ generated by x.

If $|x| = n \in \mathbb{N}$, then we say x *has order* n or *is of order* n. If $|x| = \infty$, then x is an element of *infinite order.*

Example 1.57. The order of $1_G \in G$ (the element) is always 1 (the natural number).

Exercise 1.58. Convince yourself that if $x \in G$, then $|x| \leq |G|$. When would $|x| = |G|$?

Exercise 1.59. In $\mathbb{C}^\times = (\mathbb{C} - \{0\}, \cdot)$, what are the elements of finite order? What is the order of the element i?

Exercise 1.60. (The Klein four group ♫) Recall that $GL_2(\mathbb{R})$ is the group of invertible 2×2 matrices with real coefficients. Inside $GL_2(\mathbb{R})$, there is a subgroup called the **Klein four group** V:

$$V = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \right\}$$

Use the concept of *order of an element* to prove that V is *not* cyclic.
Solution: By inspection, every element has order either 1 or 2. If V were cyclic, then it would be generated by a single element g; since $\langle g \rangle = 4$, the order of g would be 4.

Exercise 1.61. Let $a, b \in G$. Prove that $|ab| = |ba|$. This is on HW02.

Exercise 1.62. Show by example that the product of elements of finite order in a group need not have finite order. What if the group is abelian? This is on HW02.

1.10 Subgroups of $\mathbb{Z}$

At this point you might already have some guesses for what the subgroups of $\mathbb{Z}$ are.

Theorem 1.63. Let S be a subgroup of $(\mathbb{Z}, +)$. Then S is either

- the trivial subgroup $\{0\}$ or
- of the form $n\mathbb{Z}$, where n is the smallest positive integer in the set S.

Proof.

- Since 0 is the additive identity, $0 \in S$. If $S \neq \{0\}$, then there exist integers $n, -n \neq 0$ in S. So S contains a positive integer.
- Let a be the smallest positive integer in S. We want to show that $a\mathbb{Z} = S$, so we need to show that $a\mathbb{Z} \leq S$ and $S \leq a\mathbb{Z}$.
- To check that $a\mathbb{Z} \leq S$, observe that (1) closure and induction imply $ka \in S$, (2) $0 = 0a \in S$, and (3) S contains inverses, so $-ka \in S$.
- To show $S \subseteq a\mathbb{Z}$, pick any $n \in S$. Use division with remainder to write $n = qa + r$, where $q, r \in \mathbb{Z}$ and $0 \leq r < a$.
  - Since S is a *subgroup*, $r = n - qa \in S$.
  - Since a is the smallest positive integer in S, r must $= 0$.
  - Therefore $n = qa \in a\mathbb{Z}$.

□

The argument in this proof is very useful, and we will see it again in this course.

Proposition 1.64. Let $x \in G$, and let S denote the *set* of integers k such that $x^k = 1$:

$$S = \{k \in \mathbb{Z} \mid x^k = 1\}.$$

(a) S is a subgroup of $\mathbb{Z}$

(b) If $x^r = x^s$ (say, $r \geq s$), then $x^{r-s} = 1$, i.e. $r - s \in S$.

(c) Suppose that S is not the trivial subgroup $\{0\} \leq \mathbb{Z}$. Then $S = n\mathbb{Z}$ for some positive integer n. The powers $\{1, x, x^2, \ldots, x^{n-1}\}$ are the distinct elements of the subgroup $\langle x \rangle$, and so the order of $\langle x \rangle$ is n.

Proof. (a) Let's use the subgroup criterion. Since $0 \in S$, $S \neq \emptyset$. If $k, \ell \in S$, then $x^{k-\ell} = x^k(x^\ell)^{-1} = 1 \cdot 1 = 1$. (You can also just check the three subgroup conditions.)

(b) This follows from the Cancellation Law (i.e. manipulating the algebraic equation).

(c) Suppose $S \neq \{0\}$. Then by Theorem 1.63, $S = n\mathbb{Z}$, where n is the smallest positive integer in S.

Now let x^k be an arbitrary power of x. We can write $k = qn + r$ with $0 \leq r < n$. Then $x^{qn} = 1^q = 1$, so $x^k = x^{qn}x^r = x^r$. Therefore every x^k is equal to one of the elements x^r where $0 \leq r < n$.

It remains to check that the powers $\{1, x, x^2, \ldots x^{n-1}\}$ are all distinct. If $x^p = x^q$ with $0 \leq p < q < n-1$, then by (b), $q - p$ is a positive multiple of n; this is impossible.

□

Part (c) therefore gives an equivalent definition of the order of an element in a group:

Corollary 1.65. If $|g| \neq \infty$, then $|g| = \min\{n \in \mathbb{N} \mid g^n = 1$.

Exercise 1.66. Prove that every subgroup of a cyclic group is cyclic. *Hint: Work with exponents and use the description of the subgroups of* $\mathbb{Z}^+$. This is on HW03.