Section 1.3 Subgroups and Generating Sets

Definition

Let G be a group and let H be a subset of G. Then H is called a *subgroup* of G if H is itself a group under the operation of G.

Not every group has proper subgroups. For example, consider the group of fifth roots of unity in $\mathbb{C}$.

Examples of subgroups of $\mathbb{C}^\times$:

1. The set $\mathbb{R}^\times$ of non-zero real numbers.
2. The set $S = \{a + bi \in \mathbb{C} : a^2 + b^2 = 1\}$; S is the set of complex numbers of modulus 1, geometrically it is the unit circle in the complex plane. Why is this set closed under multiplication and taking inverses?
3. Is the set of *pure imaginary* numbers a subgroup of $\mathbb{C}^\times$?

Cyclic subgroups of a group

Let G be a group (with operation $\star$), and let $a \in G$.
We use the shorthand a^2 for $a \star a$, a^3 for $a \star a \star a$, etc.
We think of these elements as "positive integer powers" of a.
We also adopt the convention that a^0 means the identity element.
We already have a^{-1} representing the inverse of a, we define negative integer powers of a by defining a^{-k} to mean $(a^{-1})^k$.

Notation: We denote by $\langle a \rangle$ the set of *all* integer powers of the element a (which may or may not be distinct elements of G).

Lemma

For each $a \in G$, $\langle a \rangle$ is a subgroup of G.

It is called the cyclic subgroup of G generated by a.
In general a subgroup of a group G is said to be cyclic if it is equal to $\langle a \rangle$ for *some* element a of G.

Cyclic groups

Definition: A group G is cyclic if $G = \langle a \rangle$ for some element a of G. In this case a is said to be a *generator* of G.

Examples

1. $(\mathbb{Z}, +)$ is an infinite cyclic group, with 1 as a generator.
   Question: There is one other generator. What is it?
2. For a natural number n, the group of nth roots of unity in $\mathbb{C}^\times$ is a cyclic group of order n, with (for example) $e^{\frac{2\pi i}{n}}$ as a generator.
   Question to think about: What other elements generate this group?
3. For $n \geq 3$, the group of rotational symmetries of a regular n-gon is a cyclic group of order n, generated (for example) by the rotation through $\frac{2\pi}{n}$ in a counterclockwise direction.

Generators of cyclic groups

We often denote a cyclic group of order n by C_n, and an infinite cyclic group by C_∞.

Question: If C_n is generated by x, what other elements (i.e. which powers of x) also generate the group?

- If $C_4 = \langle x \rangle$, then x and x^3 are generators.
- If $C_5 = \langle x \rangle$, then x, x^2, x^3, x^4 all generate C_5.
- If $C_6 = \langle x \rangle$, then only x and x^5 generate C_6.

Theorem 1.3.7 Suppose that x is a generator of C_n. Then the elements of C_n that generate it as a cyclic group are those elements of the form x^i where $\gcd(i, n) = 1$. The number of generators is $\phi(n)$.