Week 4

4.1 Cyclic subgroups (cont'd)

Proposition 4.1.1. *Every subgroup of a cyclic group is cyclic.*

Proof. Let $G = \langle g \rangle$ be a cyclic group, and $H < G$ a subgroup. If H is trivial, then it is cyclic (generated by the identity e). If H is nontrivial, then there exists $k \in \mathbb{Z}_{>0}$ such that $g^k \in H$. We set

$$m := \min\{k \in \mathbb{Z}_{>0} : g^k \in H\}.$$

We claim that H is generated by g^m. First of all, we obviously have $\langle g^m \rangle \subset H$. Conversely, let g^n be an arbitrary element in H. By the Division Theorem, there exist (uniquely) integers q and $0 \leq r \leq m-1$ such that $n = mq + r$. So $g^n = (g^m)^q \cdot g^r$ which implies that $g^r = (g^m)^{-q} \cdot g^n \in H$. This forces $r = 0$. Thus $g^n \in \langle g^m \rangle$, and we have shown that $H \subset \langle g^m \rangle$. This completes the proof. $\square$

Corollary 4.1.2. *Any subgroup of* $(\mathbb{Z}, +)$ *is of the form* $n\mathbb{Z}$ *for some* $n \in \mathbb{Z}$.

Because of this corollary, we can define the gcd of two integers as follows. For any $a, b \in \mathbb{Z}$, the subset

$$\langle a, b \rangle := \{ma + nb : m, n \in \mathbb{Z}\}$$

is a subgroup of $\mathbb{Z}$ using Proposition 3.2.5 (check this!). Corollary 4.1.2 implies that $\langle a, b \rangle$ is of the form $d\mathbb{Z}$ for some positive integer d. We then define the **greatest common divisor (gcd)**, denoted as $\gcd(a, b)$, to be this positive integer d. One can check that this gcd satisfies the following properties (as expected):

- $d \mid a$ and $d \mid b$,
- $d = ka + lb$ for some $k, l \in \mathbb{Z}$, and
- if $k \mid a$ and $k \mid b$, then $k \mid d$.

Proposition 4.1.3. *Let G be a cyclic group of order n and $g \in G$ be a generator of G, i.e. $G = \langle g \rangle$. Let $g^s \in G$ be an element in G. Then*

$$|g^s| = n/d,$$

where $d = gcd(s, n)$. Moreover, $\langle g^s \rangle = \langle g^t \rangle$ if and only if $gcd(s, n) = gcd(t, n)$.

Proof. Let us write $a = g^s$ and let $m := |a|$. First of all, we have $a^{n/d} = (g^s)^{n/d} = (g^n)^{s/d} = e$ since $|G| = n$. Proposition 2.1.1 implies that $m \mid (n/d)$. On the other hand, we have $e = a^m = g^{sm}$ which implies, again by Proposition 2.1.1, that $n \mid sm$. Dividing both sides by d gives $(n/d) \mid (s/d)m$. But n/d and s/d are relatively prime, so we must have $(n/d) \mid m$. This proves that $|g^s| = m = n/d$ where $d = \gcd(s, n)$.

To prove the second assertion, we first show that there is an equality of subgroups $\langle g^s \rangle = \langle g^d \rangle$ where $d = \gcd(s, n)$. One inclusion is clear: as $d \mid s$, we have $g^s \in \langle g^d \rangle$ which implies $\langle g^s \rangle \subset \langle g^d \rangle$. Conversely, note that there exist $k, l \in \mathbb{Z}$ such that $d = ks + ln$. So we have $g^d = (g^s)^k \cdot (g^n)^l = (g^s)^k \in \langle g^s \rangle$ and hence $\langle g^d \rangle \subset \langle g^s \rangle$. This proves the equality we claimed.

Now, $\langle g^s \rangle = \langle g^t \rangle$ implies that $|g^s| = |g^t|$ which in turn gives $\gcd(s, n) = \gcd(t, n)$. Conversely, if we have $\gcd(s, n) = \gcd(t, n) =: d$, then $\langle g^s \rangle = \langle g^d \rangle = \langle g^t \rangle$. □

Corollary 4.1.4. *All generators of a cyclic group $G = \langle g \rangle$ of order n are of the form g^r where r is relatively prime to n.*

4.2 Generating sets

Let G be a group, S a nonempty subset of G. Then similar to the case of a cyclic subgroup, it can be proved using Proposition 3.2.5 that the subset:

$$\langle S \rangle := \{a_1^{m_1} a_2^{m_2} \cdots a_n^{m_n} : n \in \mathbb{N}, a_i \in S, m_i \in \mathbb{Z}\}$$

is the smallest subgroup of G containing S. We call $\langle S \rangle$ the subgroup of G **generated** by S. If $G = \langle S \rangle$, then we say S is a **generating set** for G.

Remark. Similar to the cyclic subgroup generated by a single element, we have

$$\langle S \rangle = \bigcap_{\{H: S \subset H < G\}} H.$$

If $S = \{a_1, a_2, \ldots, a_l\}$ is a finite set, we often write

$$\langle a_1, a_2, \ldots, a_l \rangle$$

to denote the subgroup generated by S.

Example 4.2.1. • The set of cycles and the set of transpositions are two examples of generating sets for S_n.

- We also have $S_n = \langle (12), (12\cdots n)\rangle$.
- We have $D_n = \langle r, s\rangle$ where r is the rotation by the angle $2\pi/n$ in the anticlockwise direction and s is any reflection.

If there exists a finite number of elements $a_1, a_2, \ldots, a_l \in G$ such that

$$G = \langle a_1, a_2, \ldots, a_l\rangle,$$

then we say that G is **finitely generated**.

For example, every cyclic group is finitely generated, for it is generated by one element. Every finite group is also finitely generated, since we may take the finite generating set S to be G itself. Finitely generated groups are much easier to understand. For instance, there is a simple classification for finitely generated abelian groups but not for those which are not finitely generated.

Exercise: The group $(\mathbb{Q}, +)$ is not finitely generated.

4.3 Equivalence relations and partitions

Let S be a set.

A **partition** P of S is a collection of subsets $\{S_i : i \in I\}$ of S (here I is some index set) such that

- $S_i \neq \emptyset$ for each $i \in I$,
- $S_i \cap S_j = \emptyset$ if $i \neq j$, and
- $\bigcup_{i\in I} S_i = S$.

We may also say that P is a subdivision of S into a disjoint union of nonempty subsets, written as

$$S = \bigsqcup_{i\in I} S_i.$$

An **equivalence relation** on S is a relation $\sim$ (i.e. a subset of $S \times S$) which is

- (Reflexive:) $a \sim a$ for any $a \in S$,
- (Symmetric:) if $a \sim b$, then $b \sim a$, and
- (Transitive:) if $a \sim b$ and $b \sim c$, then $a \sim c$.

In fact, partition and equivalence relation are two equivalent concepts.

First of all, given a partition $\{S_i : i \in I\}$ of S, we can define a relation on S by the rule $a \sim b$ if $a, b \in S_i$ for some $i \in I$. Then it is easy to check that $\sim$ is an equivalence relation on S.

Conversely, suppose we are given an equivalence relation $\sim$ on S. For any $a \in S$, the set

$$C_a = \{b \in S : a \sim b\}$$

is called the **equivalence class** of a. The reflexive axiom implies that $a \in C_a$; in particular, $C_a \neq \emptyset$ for all $a \in S$. Also, S is the union of all the equivalence classes C_a. Finally, we claim that if $C_a \cap C_b \neq \emptyset$, then $C_a = C_b$.

Proof of claim. Suppose there exists $c \in C_a \cap C_b$. So we have $a \sim c$ and $b \sim c$. The symmetric and transitive axioms then imply that $a \sim b$ (and $b \sim a$). Now for any $d \in C_a$, we have $d \sim a$, so $d \sim b$ by $a \sim b$ and the transitive axiom. Thus $d \in C_b$ and this shows that $C_a \subset C_b$. Reversing the roles of a and b in the same argument shows that $C_b = C_a$. Therefore $C_a = C_b$. □

We conclude that the collection of equivalence classes C_a, $a \in S$ gives a partition of S.

As an application, we give a proof of the fact that any permutation $\sigma \in S_n$ is a product of disjoint cycles:

Proof of Proposition 2.2.3. Let $\sigma \in S_n$ be a permutation on the set $I_n = \{1, 2, \ldots, n\}$. For $a, b \in I_n$, we say $a \sim b$ if and only if $b = \sigma^k(a)$ for some $k \in \mathbb{Z}$. **Exercise:** This defines an equivalence relation on I_n. So it produces a partition of I_n into a disjoint union of equivalence classes:

$$I_n = O_1 \sqcup O_2 \sqcup \cdots \sqcup O_m.$$

(The equivalence classes $O_1, O_2, \ldots, O_m \subset I_n$ are called **orbits** of σ.) Then, for $j = 1, 2, \ldots, m$, we define a permutation $\mu_j \in S_n$ by

$$\mu_j(a) = \begin{cases} \sigma(a) & \text{if } a \in O_j, \\ a & \text{if } a \notin O_j. \end{cases}$$

Each μ_j is a cycle (of length $|O_j|$). They are disjoint since the O_j's form a partition. Also we have

$$\sigma = \mu_1 \mu_2 \cdots \mu_m.$$

□