9.10.2025: Math 122 Lecture 3 Notes

Vasily Krylov

1 Last Time

We defined the group of permutations S_T (the T-set). We found that the structure of S_n is a symmetric group and established cycle notation and how to multiply permutations. Finally, we defined generators and relations, looking at the presentation of S_3. One such presentation is as follows:

$$S_3 = \langle x, y \mid x^3 = y^2 = 1, yx = x^2y \rangle,$$

where $x = (123)$ and $y = (12)$.

Another presentation uses $s_1 = (12)$ and $s_2 = (23)$.

Exercise: Show

$$S_3 = \langle s_1, s_2 \mid s_1^2 = s_2^2 = 1, s_1s_2s_1 = s_2s_1s_2.$$

Solution: We have that

$$(12)(23)(12) = (12)(132) = (13) = (23)(231) = (23)(12)(23).$$

We can generalize this to get the following theorem:
Theorem:

$$S_n = \langle s_1, \ldots, s_{n-1} \mid s_i^2 = 1, s_is_j = s_js_i, |i-j| > 1, s_is_{i+1}s_i = s_{i+1}s_is_{i+1} \rangle,$$

where $s_i = (i\ i+1)$. Try to check these relations!

2 More examples of generators/relations in presentations

$\mathbb{Z} = \langle x \rangle$, $x = 1$: note that there are no relations. Now, we take $\mathbb{Z}/n\mathbb{Z}$: it is generated by 1, so again $x = 1$. Since

$$\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}} = 0,$$

we have the relation $x^n = 1$.

Exercise: Prove $\mathbb{Z}/n\mathbb{Z} = \langle x \mid x^n = 1 \rangle$.

3 Why are symmetric groups important?

Symmetric groups are important because other groups are contained in them as subgroups.

Definition: a subset $H \subset S$ of a group S is a *subgroup* if it has the following properties:

- Closure: $\forall\, a, b \in H \Rightarrow ab \in H$.
- Identity: $e \in H$.
- Inverses: $\forall\, a \in H \Rightarrow a^{-1} \in H$.

Claim: if $H \subset S$ (here meaning H is a subgroup) then the product on S defines the group structure on H.

Proof: we take the subgroup axioms and use them to verify satisfaction of the group axioms in H. The identity and inverse axioms are satisfied. Associativity holds for H as it holds for S.

Proposition: Let G be a group. Then G is a subgroup of the group of permutations S_G.

Proof: We construct an embedding $G \overset{\varphi}{\hookrightarrow} S_G$ such that

$$g \mapsto (h \mapsto gh).$$

We denote the left multiplication $h \mapsto gh$ as λ_g.

1. λ_g is bijective because it has an *inverse* given by $\lambda_{g^{-1}}$.
2. φ is *injective*: to prove this, we check that if $\lambda_g = \lambda_{g'}$, $g = g'$. Note that
$$g = \lambda_g(1) = \lambda_{g'}(1) = g',$$
so this holds.
3. φ identifies multiplication in G with multiplication in S_G. In other words, we need to check that
$$\varphi(g \cdot_G h) = \varphi(g) \cdot_{S_G} \varphi(h),$$
where the left side multiplication is in G and the right side multiplication is in S_G. Indeed, we find that
$$e \overset{\varphi(gh)}{\longmapsto} (gh)e$$
and
$$e \mapsto he \overset{\varphi(g)\cdot\varphi(h)}{\longmapsto} g(he),$$
which are equal by the associative law.

4 Examples of subgroups

These are chains of subgroups: $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ and $\mathbb{Z}^\times \subset \mathbb{Q}^\times \subset \mathbb{R}^\times \subset \mathbb{C}^\times$.

Another interesting example is $S \subset \mathbb{C}^\times$, where $S := \{a + bi \in \mathbb{C}^\times \mid a^2 + b^2 = 1\}$.

Exercise: Prove that S forms a subgroup of $(\mathbb{C}^\times, \cdot)$.

5 Cyclic subgroups

We take the group S with element $x \in S$. The cyclic subgroup of S generated by x is

$$\langle x \rangle : \{\dots, x^{-2}, x^{-1}, 1, x, x^2, \dots\}.$$

Examples:

- $S = \mathbb{Z}$ and $x = n$; then $\langle n \rangle = n\mathbb{Z}$, which is infinite.
- $S = (\mathbb{R}^\times, \cdot)$; then for $x = -1$, $\langle -1 \rangle = \{\pm 1\}$, so the cyclic subgroup consists of two elements.

Our goal is to understand what $\langle x \rangle$ can look like. First, let's describe *all* subgroups in $(\mathbb{Z}, +)$.

Theorem: Let S be a subgroup of $\mathbb{Z}$. Either S is the trivial subgroup $\{0\}$, or else it has the form $\mathbb{Z}a$, where a is the smallest positive integer in S.

Proof:

- By the definition of a subgroup, $0 \in S$; if $S = \{0\}$ then part of our theorem follows.
- If $\exists\, n \in S$, $n \neq 0 \Rightarrow n, -n \in S$. So S contains some positive integer. Let a be the *smallest* positive integer in S.

Our goal is now to show that $S = \mathbb{Z}a$.

1. $\mathbb{Z}a \subset S$. In particular, if $a \in S$, then $a + a = 2a \in S$, and so on until we have

   $$ka \in S \;\forall\, k \in \mathbb{Z} > 0.$$

   Now, if $ka \in S$, $-ka \in S$. So we conclude that

   $$\mathbb{Z}a \subset S.$$

2. $S \subset \mathbb{Z}a$. Pick $n \in S$ and divide with the remainder:

   $$n = qa + r,$$

   where $q \in \mathbb{Z}$ and $r \in \{0, 1, \dots, a-1\}$. Per item 1, $qa \in S$, so $-qa \in S$, and therefore $\underbrace{n - qa}_{r} \in S$.

   Note now that since a is the *smallest* positive integer in S and $r < a$, we must have that $r = 0$. So we conclude that $n = qa \in \mathbb{Z}a$, and therefore that $S \subset \mathbb{Z}a$.

Combining items 1 and 2 gives $S = \mathbb{Z}a$, as desired.