21-237: Math Studies Algebra I September 2, 2022

Lecture 3 : Least subgroups and cyclic groups

Lecturer: James Cummings

Scribe: Rajeev Godse

1 Subgroups

Recall: Let G be a group. A subgroup H is a subset of G that contains 1 and is closed under group operation and inverse. We can say that $H \leq G$.

$\leq$ is sensible notation: the subgroup relation is reflexive, anti-symmetric, and transitive.

Fact: Let G be a group. Let $\mathfrak{F}$ be a set of subgroups of S. Then, $\bigcap \mathfrak{F} = \{g \in G : \forall H \in \mathfrak{F}. g \in H\}$ is a subgroup of G.

2 Least subgroup

Given subset X of group G, let $\langle X \rangle = \bigcap \{H \subseteq G : H \leq G, X \subseteq H\}$. We call $\langle X \rangle$ the subgroup of G generated by X.

- $\langle X \rangle \leq G$
- $X \subseteq \langle X \rangle$
- For any $H \subseteq G$, $X \subseteq H \implies \langle X \rangle \leq H$

This top-down definition is nice, but we'd prefer a bottom-up one.

3 Exponentiation

Let G be a group, $g \in G, n > 0$. We define g^n as the product of n copies of g. We define g^{-1} to be the inverse of g, and for $n > 0$, g^{-n} to be $(g^{-1})^n$.

Easy fact: For all $m, n \in \mathbb{Z}$, $g^m g^n = g^{m+n}$.

Another one: For all $a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.

Keep going: For all $m, n \in \mathbb{Z}$, $(g^m)^n = g^{mn}$.

4 Bottom-up

Theorem: Let G be a group and $X \subseteq S$. Then, $\langle X \rangle = 1$ if $X = \emptyset$, where $1 = \{1_G\} \leq G$. Otherwise, $\langle X \rangle = \{x_1^{m_1} \dots x_t^{n_t}. t > 0, x_j \in X, n_j \in \mathbb{Z} \text{ for } 1 \leq j \leq t\}$.

Proof: Suppose $X = \emptyset$, then $X \subseteq 1$ and 1 is the least subgroup of G, so we are done.

Suppose $X \neq \emptyset$. Let $H = \{x_1^{n_1} \dots x_t^{n_t}. t > 0, x_j \in X, n_j \in \mathbb{Z} \text{ for } 1 \leq j \leq t\}$.

(1) $1_G \in H$, via $x \in X$ for which $x^0 = 1 \in H$.

(2) H is closed under multiplication by extreme easiness.

(3) H is closed under inverse: $(x_1^{n_1} \dots x_t^{n_t})^{-1} = x_t^{-n_t} \dots x_1^{-n_1} \in H$.

(4) $X \subseteq H$: Let $x \in X$. $x = x^1 \in H$.

(5) For all K such that $X \subseteq K$, $K \leq G$, $H \leq K$: $X \subseteq K$, K closed under products and inverses, done.

To be a bit more formal, we could show that $x^n \in K$ for all $x \in X$, $n \in \mathbb{Z}$.

By (1), (2), (3), H is a subgroup of G.

With (4), we have that H is a subgroup of X.

With (5), we have that H is the least subgroup generated by X.

Notation: if $G = \langle X \rangle$, we say X generates G or X is a set of generators for G.

5 Cyclic groups

If $g \in G$, we will write $\langle g \rangle$ for $\langle \{g\} \rangle$. Similarly $\langle g_1, g_2 \rangle$ for $\langle \{g_1, g_2\} \rangle$ and so on.

We say a group G is **abelian** if $ab = ba$ for all $a, b \in S$.

We say a group G is **cyclic** if there is $g \in G$, $G = \langle g \rangle$.

Note: If $G = \langle g \rangle$, then $G = \{g^n : n \in \mathbb{Z}\}$. This follows from both definitions.

Let G be a group, $g \in G$. Then the **order** of g, denoted $|g|$, is the least $n > 0$ such that $g^n = 1$ or ∞ if no such n exists.

1. If $|g| = \infty$, then the integer powers g^n of g are all distinct, because if we had $m, n \in \mathbb{Z}$ with $m < n$ and $g^{n-m} = g^n(g^m)^{-1} = 1$.

   In this case, every element of $\langle g \rangle$ is g^n for unique $n \in \mathbb{Z}$. And $g^{n_1} g^{n_2} = g^{n_1 + n_2}$.

   Accordingly, $\langle g \rangle \simeq (\mathbb{Z}, +)$ via bijection $g^n \leftrightarrow n$ for $n \in \mathbb{Z}$.

2. (not in lecture) If $|g| = m$, then $\langle g \rangle \simeq (\mathbb{Z}_m, +)$.