21-237: Math Studies Algebra I September 7, 2022

Lecture 4 : Cosets

Lecturer: James Cummings

Scribe: Rajeev Godse

1 Meditations on cyclic groups

Recall: for group G and $g \in G$, $\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$. The **order** of g, denoted $|g|$ is the least $j > 0$ with $g^j = 1$, or ∞ if no such j exists.

If $|g| = \infty$, then all powers g^n for $n \in \mathbb{Z}$ are distinct (easy proof), so $\langle g \rangle \simeq (\mathbb{Z}, +)$ via isomorphism $g^n \leftrightarrow n$ ($g^n g^m = g^{n+m}$).

If $|g| = n$, it is similarly easy to see the following:

1. All powers g^i for $0 \leq i < n$ are distinct.
2. Any power of g is equal to g^i for some $0 \leq i < n$ due to the remainder theorem.
3. For $0 \leq i_1, i_2 < n$, $g^{i_1} g^{i_2} = g^{i_3}$ where $i_3 \equiv i_1 + i_2 \bmod n$.

We use $(\mathbb{Z}/n\mathbb{Z}, +)$ to refer to the group formed by $\{i : 0 \leq i < n\}$ with addition modulo n. From our deductions above, $\langle g \rangle \simeq \mathbb{Z}/n\mathbb{Z}$ via isomorphism $g^i \leftrightarrow i$.

The **order of a group** G is given by $|G|$, and denoted $|G|$.

Then, stretching our understanding of infinity, we can observe that $|\langle g \rangle| = |g|$.

2 Cosets of a subgroup

Let G be a group, let $H \leq G$.

Define a binary relation $\sim$ on G where $a \sim b \iff \exists h \in H.\, ha = b$.

We show $\sim$ is an equivalence relation (ER).

- $a = 1a$, so $\sim$ is reflexive
- $a = hb \implies b = h^{-1}a$, so $\sim$ is symmetric
- $a = h_1 b, b = h_2 c \implies (h_1 h_2)c = h_1(h_2 c) = h_1 b = a$, so $\sim$ is transitive.

If $a \in G$, the equivalence class of a is $\{ha : h \in H\} = Ha$ (the **right coset** of a for H).

Key fact: There is a bijection between H and Ha given by $h \mapsto ha$ (the obvious two-sided inverse is $g \mapsto ga^{-1}$). This bijection gives us that any two right cosets have the same size, which is a very nice property for equivalence classes to have.

This yields **Lagrange's theorem**: if G is finite and $H \leq G$, then $|H| \mid |G|$.

Similarly, if you define $a \sim b \iff \exists h \in H.\, ah = b$, we get an ER whose classes are left cosets aH, all again in bijection with the subgroup H.

Example: For $G = \mathbb{Z}, +$, $H = 3\mathbb{Z}$, there are three cosets: the congruence classes $[0]_\equiv, [1]_\equiv, [2]_\equiv$.

The **index** of H in G, denoted $[G : H]$ is the number of cosets of $H \in G$.

If $|G|$ is finite, $[G : H] = \frac{|G|}{|H|}$ from above.

But wait! What if the number of left cosets is different from the number of right cosets? It won't be.

Proof: $H^{-1} = \{h^{-1} : h \in H\} = H$ via closure under inverse. Then, $(Ha)^{-1} = \{b^{-1} : b \in Ha\} = a^{-1}H^{-1} = a^{-1}H$. Thus, $Ha \leftrightarrow a^{-1}H$ is a bijection, i.e. the number of left and right cosets is always the same.

$S_3 = \{\sigma : [3] \to [3] \mid \sigma \text{ is a permutation}\}$ The elements are 1, the identity; (12), (13), (23), the two-cycles; and (123), (132), the three-cycles.

Note: If $H \leq G$, $|H| = p$, a prime and $h \in H$, $h \neq 1$, $\langle h \rangle \leq H$, then $|\langle h \rangle| \mid |H| = p$, and $|h| \neq 1$ since $h \neq 1$, so $p = |h|$ and $H = \langle h \rangle$.

$H = \{1, (12)\}$ is a subgroup of order 2. There are three left cosets below.

$1H = \{1, (12)\}$

$(13)H = \{(13), (13)(12)\} = \{(13), (123)\}$

$(23)H = \{(23), (23)(12)\} = \{(23), (132)\}$