Math 332, Thursday, Feb. 19

☆ Announce talk

Quiz

(1) In two sentences or less, explain why every group is a subgroup of a permutation group (Cayley's theorem).

(2) Let H be a subgroup of a group G. What is a left coset of H?

(3) State Lagrange's thm. for a subgroup H of a finite group G.

Def. If $H < G$ and $a \in G$, then

$aH = \{ah : h \in H\}$ is called a left coset of H.

$Ha = \{ha : h \in H\}$ is a right coset.

Examples / Remarks

* If G is abelian, left cosets and right cosets are the same.
* The cosets of $\langle 3 \rangle < \mathbb{Z}$ are $0 + \langle 3 \rangle$, $1 + \langle 3 \rangle$, $2 + \langle 3 \rangle$.

  Note: $3 + \langle 3 \rangle = 0 + \langle 3 \rangle$, $-5 + \langle 3 \rangle = 1 + \langle 3 \rangle$, etc.
* The left cosets of $\langle (12) \rangle < S_3 = \{(), (12), (13), (23), (123), (132)\}$

① $() \cdot \{(), (12)\} = (1,2) \cdot \{(), (12)\} = \{(), (12)\}$

② $(13) \cdot \{(), (12)\} = \{(13), (123)\} = (123) \cdot \{(), (12)\}$

③ $(23) = \{(), (12)\} = \{(23), (132)\} = (132)\{(), (12)\}$

There are 3 distinct, disjoint cosets.

* The left cosets of $\langle (123) \rangle < S_3$

① $() \cdot \{(), (123), (132)\} = (123) \cdot \{(), (123), (132)\} = (132) \cdot \{(), (123), (132)\}$

② $(12) \cdot \{(), (123), (132)\} = (13) \cdot \{(), (123), (132)\} = (23) \cdot \{(), (123), (132)\}$.

There are 2 distinct disjoint cosets.

Prop. (1) $H < G$. The left cosets of H are either disjoint or equal. (The same holds for right cosets.)

(2) Any coset of H has the same cardinality as H.

Pf/ (1). See the text.

(2) For each $a \in G$, the mapping $H \to aH$ is a
$h \longmapsto ah$

bijection (but probably not a homomorphism). □

Note: The previous theorem is essential. While sure you can prove it easily!

Def. If H is a subgroup of a finite group G

$[G:H]$ is the number of distinct left cosets.

Remark: This is the same as the number of distinct right cosets:

$aH \longleftrightarrow Ha$ and $aH = bH \Rightarrow Ha^{-1} = Hb^{-1}$

Cor. (Lagrange's theorem) If H is a subgroup of a finite group, then

$$|G| = |H|\,[G:H].$$

Pf/ Let $a_1H, \ldots, a_kH$ be the distinct left cosets of H. Then

(1) each element of G is in some coset

Pf/ If $b \in G$, then $b \in bH$ since $1 \in H$.

(1.5) Each element is in exactly one coset (by the Proposition).

(2) and each coset has the same number of elements (by the proposition). ← # elts. $= |H|$

So the left cosets of H partition G into equal-sized piles, each pile of size $|H|$. □

Cor. If $|G| = p$ for a prime p, then G has only two subgroups: $\{1\}$ and G.

Pf/ Let $H < G$. If $\exists\ a \in H$, $a \neq 1$, then $\langle a \rangle < H < G$. By Lagrange, $|\langle a \rangle|$ divides G evenly. Since $|G|$ is prime, we have $\langle a \rangle = G$. Hence, $H = G$. $\square$

Prop. Let G be a finite group, and let $a \in G$. Then

(1) $|a|$ divides $|G|$.

(2) $a^{|G|} = 1$. $\boxtimes$

Cor. (Euler's thm.) Let n be a positive integer and let a be an integer relatively prime to n. Let $\phi(n)$ be the number of elements in $\{k \in \mathbb{Z} : 1 \leq k < n,\ \gcd(k,n) = 1\}$. Then

$$a^{\phi(n)} = 1 \mod n$$

Pf/ Apply the preceding Proposition to U_n. $\square$

Cor. (Fermat's little theorem) If p is prime an $a \in \mathbb{Z}$ is not divisible by p, then

$$a^{p-1} \equiv 1 \bmod p.$$

Pf/ Apply the previous theorem with $n = p$. Then $\phi(p) = p-1$ and a is relatively prime to p. $\square$

Variation p prime, $a \in \mathbb{Z}$. Then

$$a^p = a \bmod p$$

Pf/ If a is relatively prime to p, then $a^{p-1} = 1 \bmod p \Rightarrow$ $a^p \equiv a \bmod p$. Otherwise, $a = 0 \bmod p$ and again $a^p \equiv a \bmod p$. $\square$