Wed, Week 9

Cosets & Lagrange's Thm

Cosets: for a subgroup H, aH (left coset) $aH = \{ah \mid h \in H\}$

For $(\mathbb{Z}_{10}, +)$ we denote cosets w/ + : $a + H$.

Ex If $H = \{0, 5\}$, $H \leq \mathbb{Z}_{10}$. Say $a = 3$.

$$\left.\begin{aligned}
3 + H &= \{3, 8\} = 8 + H \\
4 + H &= \{4, 9\} = 9 + H \\
5 + H &= \{5, 0\} = H \\
6 + H &= \{6, 1\} = 1 + H \\
7 + H &= \{7, 2\} = 2 + H
\end{aligned}\right\}$$

$\mathbb{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

Notice:

- cosets partition group.
- cosets are pair-wise disjoint.
- # of elements in each coset is same

Lagrange's Theorem: (1770's)

Symmetric Polynomials: $x+y+z$, $3x+3y+3z$

- invariant if you permute variables
  - swap $x \leftrightarrow y$, i.e., (xy) leaves the polys the same

Non-symm. Polys: $x+y-z$

(xy) does nothing, but (xz) produces a new poly.

cycle notation
- swap x, y

3 variables, so $3!$ total permutations, some give new polys
$= 6$ - some don't.

All Polys obtained from $x+y-z$ by permuting x, y, z.

1	$x+y-z$	(xy) -12	(1)
2	$z+y-x$	(xz) -13	(xzy)
3	$x+z-y$	(yz) -23	(xyz)

$\Big\} 3$

Lagrange noticed: Total # of permutations of n variables $= n!$

Total # of different polys obtained by all these permutations divides $n!$

Modern Idea: # of distinct polys = # of left cosets of H in S_3 where H = subgp of S_3 that leaves the given poly invariant

2 ells in

1810 - Gauss (proved this fact for cyclic groups of prime order

1844 - Cauchy (S_n)

1860 - Jordan (all groups)

Lagrange's Thm:

For a finite group G, & any subgroup $H \leq G$,

1. $|H|$ divides $|G|$

2. The index of H in G, $|G:H| = \frac{|G|}{|H|}$

proof: All left cosets of H:

$a_1H, a_2H, a_3H, \ldots, a_kH$.

Every $a \in G$ lives in exactly one of these

the order of each a_iH is $|H|$.

So $G = a_1H \cup a_2H \cup \ldots \cup a_kH$

$$|G| = |a_1H| + |a_2H| + \ldots + |a_kH|$$
$$= |H| + |H| + \ldots + |H| = k \cdot |H|$$

$$|G| = k \cdot |H|$$

$8 = 4 \cdot 2$

$|H|$ divides $|G|$.

---

if P then Q,

converse: if Q then P

CONVERSE OF Langrange's Thm IS NOT TRUE (Friday)

Cor 1: If $a \in G$, $|a| \mid |G|$.

proof: $|a| = |\langle a \rangle|$, since $\langle a \rangle \leq G$, Lagrange $\Rightarrow$ $|\langle a \rangle| \mid |G|$ ■

Fact from cyclic groups.

Cor 2: If $a \in G$, $a^{|G|} = e$.

proof: By Cor 1, $|G| = |a| \cdot k$

so $a^{|G|} = a^{|a| \cdot k} = \left(a^{|a|}\right)^k = e^k = e$

Ex. $\mathbb{Z}_{84} = \{0, 1, 2, \ldots, 83\}$

$2^3 = 2 + 2 + 2 = 3 \cdot 2$

$2^{84} = \text{identity} = 0$

$2^{84} \bmod 84 = 0$

$7^{84} \bmod 84 = 0$

$79^{84} \bmod 84 = 0$

Cor 3: Any group of prime order is cyclic.

proof if $a \in G$, where $|G| = \text{prime}$.
non-identity

By Cor 1 $|a| \mid |G|$ so $|a| = |G|$, $G = \langle a \rangle$.

Fermat's Little Theorem: $a^p \bmod p = a \bmod p$.

Ex. $a = 5$, $p = 3$, $5^3 \bmod 3 = 125 \bmod 3 = 2$

$5 \bmod 3 = 2$