Coset properties

Lemma. Let $H \leq G$ be a subgroup of a group G, and fix $g_1, g_2 \in G$. Then TFAE:

(1) $g_1 H = g_2 H$; ← g_1 & g_2 represent the same left coset

(2) $H g_1^{-1} = H g_2^{-1}$;

(3) $g_1 H \subseteq g_2 H$;

(4) $g_2 \in g_1 H$;

(5) $g_1^{-1} g_2 \in H$. ← "the difference in g_1 & g_2 is an element of H"

Thm. Let $H \leq G$ be a subgroup of a group G. Then the left (or right) cosets of H partition G.

(Proof) NTS: $\forall\ g_1, g_2 \in G$, $g_1 H$ & $g_2 H$ are either disjoint or equal as sets.

$\S$ $g_1 H \cap g_2 H \neq \emptyset$. Pick $a \in g_1 H \cap g_2 H$.

Then $a = g_1 h_1$ and $a = g_2 h_2$, for some $h_1, h_2 \in H$.

So $g_1 h_1 = g_2 h_2$. Then $g_1 = g_2(h_2 h_1^{-1}) \in g_2 H$.

By the lemma, $g_1 H = g_2 H$.

Same argument works for right cosets. $\blacksquare$

Cor. We can define an equivalence relation on G by

$$g_1 \sim g_2 \iff g_1 H = g_2 H.$$

Def The **index** of a subgroup $H \leq G$ is the number of left cosets of H in G, denoted $[G:H]$.

Ex. (1) $[\mathbb{Z}:3\mathbb{Z}]=3$ and $[\mathbb{Z}:n\mathbb{Z}]=n$

(2) $[S_3:H]=3$, where $H=\{(1),(12)\}$.

Thm. Let H be a subgroup of G, $\mathcal{L}_H$ the collection of left cosets of H, $\mathcal{R}_H$ the right cosets. Then $\mathcal{L}_H$ and $\mathcal{R}_H$ have the same cardinality.

(Proof.) We need a bijection $\phi: \mathcal{L}_H \to \mathcal{R}_H$. Define ϕ by $\phi(gH) := Hg^{-1}$. Apply the lemma above to show that ϕ is well-defined & injective. B/c $\phi(g^{-1}H) = Hg$, ϕ is surjective. ∎

Lagrange's Theorem

Prop. Let $H \leq G$ be a subgroup of G. Then every left (respectively, right) coset of H in G has cardinality equal to that of H.

(Proof.) For any $g \in G$, we'll construct a bijection

$$\phi_g : H \longrightarrow gH.$$

Namely, $\phi_g(h) := gh \in gH$.

Injectivity: $\phi_g(h_1) = \phi_g(h_2) \Rightarrow gh_1 = gh_2$

$\Rightarrow h_1 = h_2$ (left cancellation)

Surjectivity: By def'n, $gH = \{gh \mid h \in H\}$

$= \{\phi_g(h) \mid h \in H\}$.

So every element in gH has the form $\phi_g(h)$.

Analogous proof works for right cosets. $\blacksquare$

<u>Thm</u> (Lagrange) Let $H \leq G$ be a subgroup of a finite group G. Then the index $[G:H]$ is given by

$$[G:H] = \frac{|G|}{|H|}.$$

(Proof.) The left cosets of H in G partition G. There are $[G:H]$ of them. Each left coset has cardinality $|H|$, so $|G| = |H| \cdot [G:H]$. So $[G:H] = |G|/|H|$. $\blacksquare$

<u>Cor</u>. Let G be a finite group. Then all subgroups and elements of G have order dividing $|G|$.

<u>Cor</u> Any group of prime order is cyclic, and is generated by each of its non-identity elements.

(Proof.) Say $|G| = p$ is prime. Then every element has order 1 or p. Thus non-identity elements have order $p = |G|$. ∎

<u>Cor</u> Let $K \subseteq H \subseteq G$ be subgroups of a finite group G. Then $[G:K] = [G:H] \cdot [H:K]$.

<u>Rmk</u>. We are not assured a subgroup or element of order equal to every factor of $|G|$.
e.g., $|A_4| = 12$, but A_4 has no subgroup of order 6.
(Proof using cosets in book.)

<u>Number-theoretic corollaries</u>

<u>Recall</u>: • The generators of $(\mathbb{Z}_n, +)$ are those integers $1 \leq k < n$ s.t. $\gcd(n,k) = 1$.

• The group of multiplicative units $U(n) \subset \mathbb{Z}_n$ consists of these same integers.

<u>Def</u>. The Euler-ϕ function $\phi : \mathbb{N} \to \mathbb{N}$ is defined by $\phi(1) := 1$ and

$$\phi(n) := \left| \{ k \in \mathbb{N} \mid 1 \leq k < n \ ; \ \gcd(n,k) = 1 \} \right|,$$

for $n > 1$.

<u>Thm</u> (Euler) Let a & n be relatively prime integers, with $n>0$. Then $a^{\phi(n)} \equiv 1 \pmod{n}$.

(Proof.) Choose $0 \le r < n$ s.t. $a \equiv r \pmod{n}$, by the division algorithm. Since $\gcd(n,a)=1$, $\gcd(n,r)=1$.

So $r \in U(n)$. $|U(n)| = \phi(n)$.

So $r^{\phi(n)} = 1$ in $U(n)$. ☆

☆ Added after class: This is where we're using Lagrange's theorem: $|g| \mid |G|$ $\Rightarrow g^{|G|}=e$ in a finite group.

So $r^{\phi(n)} \equiv 1 \pmod{n}$.

$\therefore$ $a^{\phi(n)} \equiv r^{\phi(n)} \equiv 1 \pmod{n}$. ∎

Added later:

<u>Thm</u> (Fermat's Little Theorem)

Let p be any prime, a any integer. Then either $a \equiv 0 \mod p$ or $a^{p-1} \equiv 1 \mod p$. In either case $a^p \equiv a \mod p$.

(Proof.) p prime $\Rightarrow \gcd(p,a) = 1$ or p.

If $\gcd(p,a)=p$, then $a \equiv 0 \mod p$.

If $\gcd(p,a)=1$, then $a^{\phi(p)} \equiv 1 \mod p$, by Euler.

i.e., $a^{p-1} \equiv 1 \mod p$.

Multiplying either by a gives $a^p \equiv a \mod p$. ∎