Cosets

Recall: If $H \leq G$, then the left (or right) of H partition G.

i.e., $g_1 \sim g_2$ defined by $g_1^{-1}g_2 \in H$ is an equivalence relation on G.

Ex. $G = D_3$, $H = \langle (12) \rangle$

H	$(13)H$	$(23)H$
(1)	(123)	(132)
(12)	(13)	(23)

Def. The index of a subgroup $H \leq G$ is the number of left cosets of H in G, denoted $[G:H]$. (Could be infinite.)

Ex ① $[D_3 : \langle (12) \rangle] = 3$

② $[\mathbb{Z} : n\mathbb{Z}] = n$

$$n\mathbb{Z} = \{\dots, -2n, -n, 0, n, 2n, \dots\}$$
$$1 + n\mathbb{Z} = \{\dots, -2n+1, -n+1, 1, n+1, 2n+1, \dots\}$$
$$\vdots$$
$$(n-1) + n\mathbb{Z} = \{\dots, -n-1, -1, n-1, 2n-1, 3n-1, \dots\}$$
$$n + n\mathbb{Z} = \{\dots, -n, 0, n, 2n, 3n, \dots\} = n\mathbb{Z} \leftarrow \text{repeat}$$

Thm. Let $H \leq G$ and let $\mathcal{L}_H, \mathcal{R}_H$ denote the collections of left and right cosets of H, respectively. Then $\mathcal{L}_H$ & $\mathcal{R}_H$ have the same cardinality.

(Proof idea) We can define a map $\phi : \mathcal{L}_H \to \mathcal{R}_H$ by

$$\phi(gH) := Hg^{-1}.$$

Certainly ϕ is surjective: given $Hg \in \mathcal{R}_H$,

$$\phi(g^{-1}H) = Hg.$$

Now use coset properties to show that ϕ is well-defined and injective.

Then ϕ is a bijection, so $|\mathcal{L}_H| = |\mathcal{R}_H|$. ▨

i.e., check that if $g_1H = g_2H$, then $\phi(g_1H) = \phi(g_2H)$.

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

(Proof.) For any $g \in G$, consider the map

$$\begin{aligned} \phi_g : H &\longrightarrow gH \\ h &\longmapsto gh. \end{aligned}$$

For any $h_1, h_2 \in H$, if $\phi_g(h_1) = \phi_g(h_2)$

then $gh_1 = gh_2$,

so $h_1 = h_2$ by cancellation.

So ϕ_g is injective.

OTOH, every element of gH has the form $gh = \phi_g(h)$, so ϕ_g is surjective. ▨

Thm [Lagrange's Theorem] Let H be a subgroup of a finite group G. Then the index $[G:H]$ is given by

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

(Proof.) Recall that the left cosets of H partition G into $[G:H]$ subsets. By our proposition, each of these subsets has cardinality $|H|$.

$$\therefore\ |G| = [G:H]\cdot|H| \Rightarrow [G:H] = \frac{|G|}{|H|}.$$ ∎

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

<u>Ex.</u> $|D_3| = 6$, so there is no subgroup of order 5.

<u>Cor.</u> Any group with prime order is cyclic and is generated by any non-identity element.

(Proof.) In a group of prime order p, prev. corollary says every element has order 1 or p. So every non-identity element has order p, and thus generates the entire group. ∎

<u>Cor.</u> Let $K \leq H \leq G$. Then $[G:K] = [G:H]\cdot[H:K]$.

<u>Number-theoretic corollaries</u>

The Euler ϕ-function $\phi: \mathbb{N} \to \mathbb{N}$ is defined by $\phi(1) := 1$ and

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

for $n > 1$.

Note: $\phi(n) = |U(n)|$.

<u>Thm</u> [Euler's Theorem]
Let a and n be relatively prime integers with $n>0$.
Then
$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

<u>Ex</u>. $a=-5$, $n=7$. $\phi(7)=6$. $7\cdot 17+6=125$

$$a^{\phi(7)} = (-5)^6 = (125)^2 \equiv 6^2 \pmod{7}$$
$$\equiv 36 \pmod{7}$$
$$\equiv 1 \pmod{7}.$$

(Proof.) Use the division algorithm to write
$$a = nq+r,$$
with $0 \le r < n$. Then $a \equiv r \pmod{n}$, so $\gcd(r,n)=1$. So $r \in U(n)$. Since $|U(n)| = \phi(n)$, the order of r in $U(n)$ divides $\phi(n)$.
In particular,
$$r^{\phi(n)} = 1 \text{ in } U(n)$$
i.e., $$r^{\phi(n)} \equiv 1 \pmod{n}.$$
But then
$$a^{\phi(n)} = (nq+r)^{\phi(n)} \equiv r^{\phi(n)} \pmod{n} \equiv 1 \pmod{n}. \quad \blacksquare$$

<u>Thm</u>. [Fermat's Little Theorem] Let p be any prime integer, a any integer. Then $a^p \equiv a \pmod{p}$.
(Proof.) Since p is prime, $\gcd(a,p)=1$ or p. If it's p, then $a \equiv 0 \pmod{p}$, so $a^p \equiv 0 \pmod{p} \equiv a \pmod{p}$.
Otherwise, Euler's gives $a^{\phi(p)} = a^{p-1} \equiv 1 \pmod{p}$. Mult. by a. $\blacksquare$