Group Theory
Week 3, Lecture #9

Recall Lagrange's Theorem: If $H \leq G$ is a subgroup of a finite group G, then

$$\boxed{|H| \mid |G|}$$

As a corollary, the order of any element of G divides the order of G:

$$\boxed{o(a) \mid |G| \quad , \forall a \in G}$$

Corollary (Euler's Theorem) If $\gcd(a,n)=1$, then

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Proof Recall $\varphi(n) = |\mathbb{Z}_n^\times| = \#\{k \in \{1,\dots,n-1\} \mid \gcd(k,n)=1\}$

Thus:

$$[a^{\varphi(n)}]_n = \boxed{\left([a]_n\right)^{\varphi(n)} = 1 \quad \text{in } \mathbb{Z}_n^\times}$$

this is an element in $\mathbb{Z}_n^\times$, since $(a,n)=1$ by assumption

Therefore $a^{\varphi(n)} \equiv 1 \pmod{n}$ ∎

Cor (Fermat) p prime $\Longrightarrow a^p \equiv a \pmod{p}$ $\forall a \in \mathbb{Z}$

(eg: $2^5 \equiv 2 \pmod{5}$ check $2^5 = 32 = 6 \cdot 5 + 2$ ✓)

$15^{101} \equiv 15 \pmod{101}$

Proof
- If $p \mid a$, then $a \equiv 0 \pmod{p}$, and so $a^p \equiv a \equiv 0$
- If $p \nmid a$, then $\gcd(p,a)=1 \underset{\text{(Euler)}}{\Longrightarrow} a^{\varphi(p)} \equiv 1 \pmod{p}$

But $\varphi(p) = p-1$. Hence $a^{p-1} \equiv 1 \pmod{p} \Rightarrow a^p \equiv a \pmod{p}$ ∎

Corollary (to Lagrange's Theorem) Every group of prime order is cyclic.

Proof Let G be a group with $|G| = p$, a prime. Let $a \in G$, $a \neq e$. Then $o(a) \mid p$. (by cor. to Lagrange)

$\Updownarrow$

$o(a) \neq 1$

Hence, $o(a) = p$

$\therefore \; G = \langle a \rangle = \{e, a, a^2, \dots, a^{p-1}\}$ $\square$

To recap some of the discussion regarding the orders of the elements of a finite group G:

$$\boxed{t_n(G) := \#\{a \in G : o(a) = n\}}$$

Then:
(1) $0 \le t_n(G) \le |G|$
(2) $t_n(G) \neq 0 \implies n \mid |G|$ (by Cor. to Lagrange)
(3) $t_1(G) = 1$
(4) $t_{|G|}(G) \neq 0 \implies G$ cyclic (this happens if $|G| = p$)

eg: $G = \mathbb{Z}_4$

n	0	1	2	3	4
$t_n(G)$	0	1	1	0	2

or, shorter:

n	1	2	4
t_n	1	1	2

$G = \mathbb{Z}_2 \times \mathbb{Z}_2$

n	0	1	2	3	4
t_n	0	1	3	0	0

or shorter

n	1	2	4
t_n	1	3	0

We will use this numerical function $n \mapsto t_n(G)$ to distinguish isomorphism classes of finite groups (a partial test for isomorphism)

The above computation will show that

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \not\cong \mathbb{Z}_4$$

Group homomorphisms and isomorphisms

Definition Let $(G, *, e)$ and $(G', *', e')$ be two groups. A homomorphism between these two groups is a function $\varphi : G \to G'$ such that

$$(*) \quad \boxed{\varphi(a * b) = \varphi(a) *' \varphi(b), \quad \forall a, b \in G}$$

Lemma If $\varphi : G \to G'$ is a homomorphism, then:

(i) $\varphi(e) = e'$

(ii) $\varphi(a^{-1}) = \varphi(a)^{-1}$

Proof (i) $\varphi(e) \underset{\substack{\uparrow \\ e \text{ identity of } G}}{=} \varphi(e * e) \underset{\substack{\uparrow \\ \varphi \text{ hom.}}}{=} \varphi(e) *' \varphi(e) \underset{\substack{\text{cancellation} \\ \text{law in } G'}}{\Longrightarrow} e' = \varphi(e)$

(ii) $\varphi(a) *' \varphi(a^{-1}) \underset{\substack{\uparrow \\ \varphi \text{ hom}}}{=} \varphi(a * a^{-1}) \underset{\substack{\uparrow \\ a^{-1} \text{ is inverse} \\ \text{of } a \text{ in } G}}{=} \varphi(e) = e'$ $\boxtimes$

Notation: • when both groups have $* = \cdot$, we write $(*)$ $\boxed{\varphi(ab) = \varphi(a)\varphi(b)}$

" " " " $* = +$, " $\boxed{\varphi(a+b) = \varphi(a) + \varphi(b)}$

Examples

(1) $\varphi = \mathrm{id}_G : G \to G$, $\varphi(a) = a$ is a hom.

(2) $\varphi : G \to G'$, $\varphi(a) = e'$ is a hom. (the trivial hom)

(3) $\varphi_n : \mathbb{Z} \to \mathbb{Z}$, $\varphi_n(k) = nk$ is a hom.

[Check: $\varphi_n(k+\ell) = n(k+\ell)$, $\varphi_n(k) + \varphi_n(\ell) = nk + n\ell$ $\Rightarrow$ by distributivity of $\cdot$ wrt $+$]

(4) $\exp : (\mathbb{R}, +, 0) \longrightarrow (\mathbb{R}^{>0}, \cdot, 1)$ $x \mapsto e^x$ is a hom

[Check: $\exp(x+y) = e^{x+y} \Longrightarrow$ $\exp(0) = 1$ ✓

$$\exp(x)\cdot\exp(y) = e^x \cdot e^y = e^{x+y}$$

(5) $\overline{} : \mathbb{C} \longrightarrow \mathbb{C}$, $\underset{x+iy}{\overset{\shortparallel}{z}} \mapsto \underset{x-iy}{\overset{\shortparallel}{\bar{z}}}$ is also a hom, since $\overline{z+w} = \bar{z}+\bar{w}$

(6) $|\ | : \mathbb{C}^\times \longrightarrow \mathbb{R}^\times$, $\underset{x+iy}{\overset{\shortparallel}{z}} \mapsto \underset{\sqrt{x^2+y^2}}{\overset{\shortparallel}{|z|}}$ is also a hom, since $|zw| = |z||w|$

(7) $|\ | : (\mathbb{C},+) \longrightarrow (\mathbb{R},+)$, $z \mapsto |z|$ is not a hom, since, for instance

$|0| = 0$
$|-z| = |z|$

take $z=1$, $w=i$; then: $|z+w| = |1+i| = \sqrt{2}$ $\times$
$|z|+|w| = |1|+|i| = 1+1 = 2$

(8) $\varphi: \mathbb{Z}_6 \longrightarrow \mathbb{Z}_2$ $[a]_6 \longrightarrow [1]_2$ is not a hom, since
$$\varphi([0]_6) = [1]_2 \neq [0]_2$$

(9) $\varphi: GL_n(\mathbb{R}) \longrightarrow \mathbb{R}^\times$, $\varphi(a) = \det(A)$ is a hom:
$$\det(A\cdot B) = (\det A)\cdot(\det B) \quad \checkmark$$
$$\left(\Rightarrow \det(I_n) = 1 \qquad \det(A^{-1}) = \frac{1}{\det(A)}\right)$$

Proposition The image of a homomorphism is a subgroup, i.e.,

$$\boxed{\text{If } \varphi: G \longrightarrow G' \text{ hom, then } \varphi(G) \leq G'}$$

(here: $\operatorname{im}(\varphi) = \varphi(G) = \{y \in G' : \exists x \in G \text{ s.t. } \varphi(x) = y\}$)

Proof Recall: $\left(H \leq G \text{ is a subgroup of } G\right) \Longleftrightarrow \left(ab^{-1} \in H,\ \forall a,b \in H\right)$

So let $a, b \in \varphi(G)$. Write $a = \varphi(x)$, $b = \varphi(y)$, $x,y \in G$. Then
$$ab^{-1} = \varphi(x)\cdot(\varphi(y))^{-1} \underset{\text{Lemma (ii)}}{=} \varphi(x)\cdot\varphi(y^{-1}) \underset{\varphi \text{ is hom}}{=} \varphi(\underbrace{xy^{-1}}_{\text{in } G})$$

$\therefore$ $ab^{-1} \in \varphi(G)$

QED

Isomorphisms

Def A group isomorphism is a function $\varphi : G \to G'$ between two groups which is both a homomorphism and a bijection:

$$\text{“iso} = \text{hom} + \text{bij”}$$

Lemma If $\varphi : G \to G'$ is an isomorphism, then $\varphi^{-1} : G' \to G$ is also an isomorphism.

Proof We know φ^{-1} is also a bijection, so enough to show φ^{-1} is a homomorphism.

Let $a', b' \in G'$. Write $a' = \varphi(a)$, $b' = \varphi(b)$

$$\Updownarrow \qquad \Updownarrow$$

$$\varphi^{-1}(a') = a \quad \varphi^{-1}(b') = b$$

Then:

$$\varphi^{-1}(a'b') = \varphi^{-1}(\varphi(a)\cdot\varphi(b)) \underset{\varphi \text{ is hom}}{=} \varphi^{-1}(\varphi(ab))$$

$$\underset{\text{since } \varphi^{-1}\circ\varphi = id_G}{=} ab = \varphi^{-1}(a')\cdot\varphi^{-1}(b')$$

$\boxtimes$

Def Two groups are said to be isomorphic if there is an isomorphism between them:

$$\underset{\substack{\uparrow \\ \text{iso} \\ (\backslash\text{cong})}}{G \cong G'} \iff (\exists\ \underset{\substack{\uparrow \\ \backslash\text{varphi } \varphi \\ \backslash\text{phi } \phi}}{\varphi} : G \to G' \text{ iso})$$