Recall

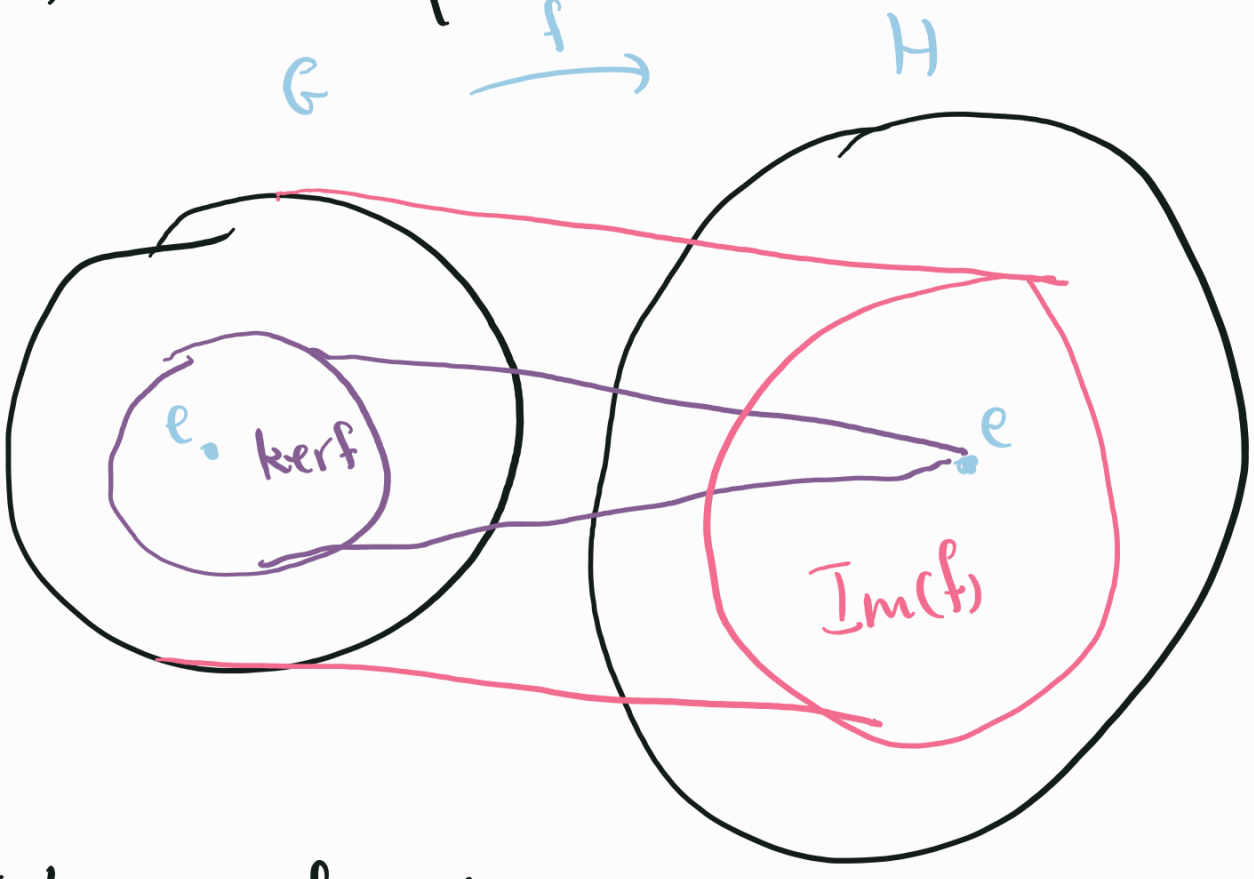
If $f: G \to H$ a gp map

(ie homomorphism)

$$H \geq Im(f) = \{ y \in H \mid \exists x \in G : f(x) = y \}$$

$$= \{ f(x) \mid x \in G \}$$

$$G \geq \ker(f) = \{ x \in G \mid f(x) = e \}$$



Note: • f is surj $\iff$ $Im\, f = H$

f is inj $\iff$

• f is inj $\Leftrightarrow$

$\ker(f) = \{e\}$:

If f is inj then

$\ker(f) = \{e\}$

conversely, if $\ker(f) = \{e\}$

and $x, x' \in G$ are s.th

$f(x) = f(x')$ then

$\Leftrightarrow$

$f(x') \cdot f(x)^{-1} = e$

$\Leftrightarrow$ $f(x' x^{-1}) = e$

$\Leftrightarrow$ $x' \cdot x^{-1} \in \ker(f)$

$\Leftrightarrow$ $x' \cdot x^{-1} = e$

$\Leftrightarrow$ $x' = x$

$\Rightarrow$ f is inj.

Example : $f : \mathbb{Z}_5 \longrightarrow \mathbb{Z}_{10}$

$f(x) = 2x \pmod{10}$

gp map : $x, y \in \mathbb{Z}_5$

$$f(x+y \pmod 5) = 2(x+y) \bmod 10$$

$$= 2x \bmod 10 + 2y \bmod 10$$

$$= f(x) + f(y)$$

$$\mathbb{Z}_{10} \geq Im(f) = \{0, 2, 4, 6, 8\}$$

$$\ker(f) = \{0\} \Rightarrow f \text{ is inj}$$

$$\bar{f} : \mathbb{Z}_5 \longrightarrow Im(f)$$

$\bar{f}$ is inj + surj

+ $\bar{f}$ is a gp map

$$\Rightarrow \mathbb{Z}_5 \cong Im(f)$$

2.

$+_{mod 5}$	0	1	2	3	4
0					
1					
2					
3					
4					

$+_{mod 10}$	0	2	4	6	8
0					
2					
4					
6					
8					

Last time: if $f: G \to H$ is a gp map then

$$G/\ker(f) \xrightarrow{\cong} \mathrm{Im}(f)$$

Thm

Def: Let G be a gp and $g \in G$. The order of g, denoted $O(g)$ is the minimal positive integer n s.th $g^n = e$.

If no such n exists, we set $O(g) = \infty$.

Note: if G is finite

$$\forall\, g \in G \qquad O(g) < \infty$$

Recall: if $m, n \in \mathbb{N}$,

their least common multiplier

is $\operatorname{lcm}(m,n)$ is minimal

n. number l s.th $m \mid l$ and

$n \mid l$.

If we write

$$\mathcal{P}_m = \{ p \text{ primes} \mid p \leq m \}$$

if $p \mid m \Rightarrow \mathcal{P}_{m/p}$

$$\rightsquigarrow \quad m = p_1^{s_1} \cdots p_k^{s_k}$$

where $p_1, \ldots, p_k$ are primes.

$$n = p_1^{t_1} \cdots p_k^{t_k}$$

where $s_i, t_i \geq 0$

Then $\operatorname{lcm}(m,n)$

$$= p_1^{\min(s_1,t_1)} \cdot \ldots \cdot p_k^{\min(s_k,t_k)}$$

Thm (Cauchy): If G is a finite abelian gp and p a prime s.th $p \mid \#G$. Then $\exists\, g \in G$ w/ $o(g) = p$ (ie $g^p = e$).

Proof: Assume by contradiction that $\nexists\, g \in G$ w/ $o(g) = p$. Then there is no element in G of order divisible by p:

if $g^r = e$ & $p \mid r$

then $\left(g^{r/p}\right)^p = g^r = e$.

Let $G = \{g_1, \ldots, g_n\}$ and let

$m_i = o(g_i)$ $(\Rightarrow \forall i \;\; p \nmid m_i)$

Let $m = \operatorname{lcm}_{i=1,\dots,n}(m_i)$ then $m_i \mid m$

$\forall m$, Furthermore $g_i^m = e$.

For $n \in \mathbb{N}$, write

$$g^{-n} := (g^{-1})^n$$

Then we can define:

$$f : \overbrace{\mathbb{Z}_m \times \dots \times \mathbb{Z}_m}^{n\text{-times}} \longrightarrow G$$

$$f(a_1, \dots, a_n) := g_1^{a_1} \cdot \dots \cdot g_n^{a_n}$$

then f is gp map:

$$f\big((a_1, \dots, a_n) + (b_1, \dots, b_n)\big) \overset{\checkmark}{=} f(a_1, \dots, a_n) \cdot f(b_1, \dots, b_n)$$

$$\Big\| \qquad \Big\|$$

$$f(a_1 + b_1, \dots, a_n + b_n)$$

$$\| $$

$$g_1^{a_1+b_1} \cdots g_n^{a_n+b_n} =$$

$$g_1^{a_1} g_1^{b_1} \cdots g_n^{a_n} g_n^{b_n} =$$

$$f(a_1, \ldots, a_n) \cdot f(b_1, \ldots, b_n).$$

Note: f is surj: $(\mathbb{Z}_m)^n \xrightarrow{f} G$

i $\qquad\qquad$ $\{g_1, \ldots, g_n\}$

$$f(0, \ldots, 0, \underset{i}{1}, 0, \ldots, 0) = g_i$$

$$\Rightarrow \quad (\mathbb{Z}_m)^n / \ker(f) \cong G$$

$\Im m(f) = G$

$\uparrow =$

By Lagrange

$$\#\ker(f) \cdot \# G = \#(\mathbb{Z}_m)^n = m^n$$

$$\Rightarrow \quad \# G \mid m^n$$

$\Rightarrow$ $p \mid \# G$ and $p \nmid m$

But

so $p \nmid m^n$ -

contradiction. //

Hasse-Weil

$$\#E(\mathbb{F}_p) \sim p$$

$\#\langle P \rangle = q$ if q a prime s.th

$\langle P \rangle \leq E(\mathbb{F}_p) \to q \mid \#E(\mathbb{F}_p)$

$\Leftarrow$ Cauchy $\Rightarrow$ $\exists\, P \in E(\mathbb{F}_p)$

$\to q \cdot P := \underbrace{P + P \cdots + P}_{q\text{-times}} = O$

$p \mid \#G \Rightarrow O(g) = p$

Generally: If $g \in G$ of order n, then $H = \{e = g^0, g, \cdots, g^{n-1}\}$

if $1 \leq k < l \leq n$

then $g^k \neq g^l$ $\quad g^k \cdot g^l = g^{k+l}$

otherwise

since

$$g^{l-k} = e \quad \text{so}$$

$$o(g) \leq l-k < n$$

H is a subgp of G:

$$\rightarrow (g^k)^{-1} = g^{n-k}$$

$$\text{且} \quad \underline{H} =: \langle g \rangle = \{ e, g, \cdots, g^{n-1} \}$$

Example: $\mathbb{Z}_{10}$ has a subgp of order 5

eg $H = \{0, 2, 4, 6, 8\} \leq \mathbb{Z}_{10}$

Def: Let G be a gp and $g \in G$.

(1) $\langle g \rangle = \{ g^n \mid n \in \mathbb{Z} \}$

the gp generated by g ($g^{-n} := (g^{-1})^n$.)

(2) G is called cyclic if

$\exists\, g \in G$ s.th

$$G = \langle g \rangle.$$

Rem: If G is finite

then $g \in G$ must have a finite order so

$$\langle g \rangle = \{ g^n \mid n \in \mathbb{Z} \}$$
$$= \{ e = g^0, g, \cdots, g^{n-1} \}$$

bcs $g^{n+k} = g^k$

$$g^{-k} = (g^k)^{-1} = g^{n-k}$$

Examples

(1) $\mathbb{Z}_n = \langle 1 \rangle$

(2) $\mathbb{Z} = \langle 1 \rangle = \{ \underline{n} \cdot 1 \mid \underline{n} \in \mathbb{Z} \}$

$= \langle -1 \rangle = \{ n \cdot (-1) \mid n \in \mathbb{Z} \}$

$g = e$

(3) $\mathbb{Z}_2 \times \mathbb{Z}_3 = \langle (1,1) \rangle$

$0 \cdot (1,1) = (0,0)$

$1 \cdot (1,1)$

$2 \cdot (1,1) = (1,1) + (1,1) = (2,2) = (0,2)$

$3(1,1) = (1,1) + (1,1) + (1,1) = (1,3) = (1,0)$

$4 \cdot (1,1) = (0,1)$

$5 \cdot (1,1) = (1,2)$.

$(G, \circ, e)$

$$g^n = \overbrace{g \cdot g \cdot \ldots \cdot g}^{n\text{-times}}$$

$(G, +, 0)$

$$n \cdot g = \overbrace{g + \ldots + g}^{n\text{ times}}$$

---

obs: If G is cyclic then it is abelian:

$$G = \langle g \rangle = \{ g^n \mid n \in \mathbb{Z} \}$$

$$g^k \cdot g^l = g^l \cdot g^k$$

Prop: For any $n \in \mathbb{N}$ there exists a cyclic gp of order n and it is unique up to isomorphism.

Proof: $\mathbb{Z}_n$ is cyclic ($\mathbb{Z}_n = \langle 1 \rangle$).

If $G = \langle g \rangle$ is a cyclic gp of order n. Then

$$G = \{g^0, g^1, \dots, g^{n-1}\}$$

Define $f : \mathbb{Z}_n \to G$ by $f(k) = g^k$

$\{0, \dots, n-1\}$

f is a gp map:

$$f(k+k') \overset{?}{=} f(k) \cdot f(k')$$

$$g^{k+k'} = g^k \cdot g^{k'}$$

$\Rightarrow$ f is an iso //

Prop: An element $k \in \mathbb{Z}_n$ is a generator ($\langle k \rangle = \mathbb{Z}_n$) iff

$\gcd(n,k) = 1$ ("coprime") $\Leftrightarrow$ $\{0, k, 2k, \dots, (n-1)k\}$

Proof: k is a generator iff

$$\mathbb{Z}_n = \{0, k, \dots, (n-1)\cdot k\}$$

if $r = \gcd(n,k) > 1$ then

$n = r \cdot s \quad k = r \cdot t \quad (s < n)$

$\Rightarrow s \cdot k = s \cdot r \cdot t = nt = 0 \pmod n$

$\Rightarrow$ k cannot have order n.

Conversly, if $r = \gcd(n,k) = 1$

i.e. that the numbers

we claim that the

$0, k, 2k, \ldots, (n-1)k$ are

distinct: otherwise if

$s, t < n$ $\quad sk \equiv tk \pmod{n}$

$$(s-t)k = nx$$

and since $k \nmid n \Rightarrow k \mid x$

But then $(s-t)k = nx = n \cdot k \cdot y$

for some y

$$\text{so} \quad s-t = ny \equiv 0 \pmod{n}$$

$$\Rightarrow \quad s = t \quad . \quad //$$

Def: For $n \in \mathbb{N}$ the Euler

totient function is

$$\varphi(n) = \#\{k \mid 1 \le k \le n \wedge \gcd(n,k) = 1\}$$

$\Rightarrow$ $\varphi(n)$ is also the

number of distinct

generators of $\mathbb{Z}_n$.