Last time

G a gp, $g \in G$

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

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

  a subgp

- If G is finite

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

$$= \{ e = g^0, \cdots, g^{k-1} \}$$

where $k = o(g)$

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

- If G is <u>cyclic</u> of

order n, $G \cong \mathbb{Z}_n = \langle 1 \rangle$

$=$

moreover the number of generators of $\mathbb{Z}_n$

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

$\Rightarrow$ If $n = p$ is prime

then any $0 \neq x \in \mathbb{Z}_p$

is a generator.

$\forall\, g \neq 0 \in \mathbb{Z}_p$

$\rightarrow \mathbb{Z}_p = \{e, g, 2g, \dots, (p-1)g\}$

$x = ng$

Prop: A subgp of a cyclic gp is cyclic.

Proof: Suppose $G = \langle g \rangle$ is cyclic of

order n, and $H \leq G$. $\#H = d$.

So $H = \{e = g^0, g^{k_1}, \ldots, g^{k_{d-1}}\}$

Now $d \mid n$ so $n = kd$ for some k. Since $\#H = d$

$g^{k_i d} = (g^{k_i})^d = e \quad \forall i$.

$\Leftrightarrow \quad k_i d = n m_i$ for some m_i

But then

$$k_i d = n m_i = k d m_i$$

$\Leftrightarrow \quad k_i = k m_i$

Thus each element in H is a power of g^k

So

$$H = \{e, g^k, (g^k)^2, \ldots, (g^k)^{d-1}\}$$

$= \langle g^k \rangle$. //

Lemma: If G, H are gps and $g \in G$ w/ $o(g) = n$ $h \in H$ w/ $o(h) = m$, then $o((g,h)) = \text{lcm}(n,m)$. (in $G \times H$).

Proof: $(g,h)^N = (e,e)$ ($\Rightarrow$)

$g^N = e \wedge h^N = e$

($\Leftarrow$) $o(g) \mid N \wedge o(h) \mid N$

So N must be a common multiple of n, m.

$\Rightarrow$ $o((g,h)) = \text{lcm}(n,m)$ //

Lemma: For $n, m \in \mathbb{N}$,

$$\gcd(n,m)\,\mathrm{lcm}(n,m) = n \cdot m.$$

Proof: Write $m = p_1^{a_1} \cdots p_s^{a_s}$, $n = q_1^{b_1} \cdots q_t^{b_t}$

$$\begin{cases} m = p_1^{k_1} \cdots p_r^{k_r} \\ n = p_1^{\ell_1} \cdots p_r^{\ell_r} \end{cases}$$

where $k_i, \ell_i \geq 0$

Then

$$\gcd(n,m) = p_1^{\max(k_1,\ell_1)} \cdots p_r^{\max(k_r,\ell_r)}$$

$$\mathrm{lcm}(n,m) = p_1^{\min(k_1,\ell_1)} \cdots p_r^{\min(k_r,\ell_r)}$$

$$\Rightarrow \quad \gcd(n,m) \cdot \mathrm{lcm}(n,m) = n \cdot m \;//$$

Corollary: $\mathbb{Z}_n \times \mathbb{Z}_m$ is cyclic iff $\gcd(n,m) = 1$.

(then $\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm}$)

Proof: Suppose $\gcd(n,m) = 1$.

Then $o((1,1)) = \operatorname{lcm}(n,m)$

$= nm / \gcd(n,m) = nm$

So $\mathbb{Z}_n \times \mathbb{Z}_m = \langle (1,1) \rangle$.

Conversely, if $\gcd(n,m) > 1$

then the order of every element in $\mathbb{Z}_n$ divides n and the order of each element in $\mathbb{Z}_m$ divides m

$\Rightarrow$ the order of each element in $\mathbb{Z}_n \times \mathbb{Z}_m$ divides $\operatorname{lcm}(n,m)$.

But $\operatorname{lcm}(n,m) = \frac{nm}{\gcd(n,m)}$

$< nm$

Then $\mathbb{Z}_n \times \mathbb{Z}_m$ is

not cyclic. //

Cor (Chinese remainder thm):

Suppose $n, m \in \mathbb{N}$ w/ $\gcd(n,m) = 1$.

Then for all $r, s \in \mathbb{N}$

the system of equations

$$\begin{cases} x = r \pmod{n} \\ x = s \pmod{m} \end{cases}$$

has a unique solution.

Proof: Cosider $\cdot \mathbb{Z}_{nm} \to \mathbb{Z}_m$ ($\cdot \mathbb{Z}_{nm} \to \mathbb{Z}_n$)

$x \mapsto x \bmod n$

$$f : \mathbb{Z}_{nm} \longrightarrow \mathbb{Z}_n \times \mathbb{Z}_m$$

$$x \longmapsto (x \bmod n, x \bmod m)$$

$\langle g \rangle = \{g^0, \dots, g^k\} \to \langle h \rangle = \{h^0, \dots, h^k\}$, $g \mapsto h$

then f is a homomorphism

Clearly $\boxed{f(1) = (1,1)}$ $\quad o(1) = nm$, $\quad o((1,1)) = nm$

and $o((1,1)) = nm$

we get that f is bijective, hence

$$\mathbb{Z}_{nm} \cong \mathbb{Z}_n \times \mathbb{Z}_m .$$

Denote $[r]_n = r \pmod n$

$[s]_m = s \pmod m$

Since f is bijective

$((r]_n, [s]_m) \in \mathbb{Z}_n \times \mathbb{Z}_m$

has a unique $x \in \mathbb{Z}_{nm}$

s.th $x \bmod n = [r]_n$

$x \bmod m = [s]_m$ //

Classification of finite abelian gps

Convention $G = (G, \underset{=}{+}, 0)$

for abelian gp

$G \oplus H := G \times H$

$\mathbb{Z}_n$ Let $n = p_1^{n_1} \cdots p_k^{n_k}$

be the prime decomposition

of n $(n_i \geq 1)$

$s = p_1^{n_1}$ $t = p_2^{n_2} \cdots p_k^{n_k}$

$$\gcd(s,t) = 1$$

$$\Rightarrow \mathbb{Z}_h \cong \mathbb{Z}_{p_1^{n_1}} \oplus \mathbb{Z}_t$$

$$\cong \cdots \cong \mathbb{Z}_{p_1^{n_1}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{n_k}}$$

Def: For G a (finite) abelian gp and p a prime

$$G(p) = \{ a \in G \mid o(a) \text{ is a power of } p \}$$

$$= \{ a \in G \mid p^n a = 0 \text{ for some } n \}$$

- $G(p) \leq G$: if $a, b \in G(p)$

  Say $p^n a = 0$, $p^m b = 0$

  then $p^m(-b) = -p^m b = 0$

so $-b \in G(p)$

and $p^n p^m (a-b) = 0$

so $a - b \in G(p)$.

$G(p)$ is called the primary p-subgp of G.

Lemma: Let G be an abelian gp and $a \in G$ an element of finite order. Then

$$\boxed{a = a_1 + \dots + a_k}$$ where

$a_i \in G(p_i)$

w/ $p_1, \dots, p_k$ the distinct primes appearing in the decomposition of $o(a)$.

Proof: We use induction on k the

number of distinct primes that divide elements of finite order in G.

If $k=1$ $\quad a = p^t \Rightarrow a \in G(p)$

Now suppose for each $b \in G$ whose order is divisible by at most $k-1$ primes

$p_1, \ldots, p_{k-1}$,

$$b = b_1 + \cdots + b_{k-1}$$

w/ $b_i \in G(p_i)$.

If $a \in G$ s.t.h. $o(a)$ is divisible by k distinct primes

say $o(a) = p_1^{r_1} \cdots p_k^{r_k}$.

Let $m = p_2^{r_2} \cdots p_k^{r_k}$

$n = p_1^{r_1}$

$\Rightarrow o(a) = nm$

$\gcd(n,m) = 1$

$\Rightarrow \exists\, u, v \in \mathbb{Z}$ s.th (extended euclidean algo)

$mua + nva = a \iff mu + nv = 1$

(Bezout coeff.)

Since $o(a) = nm$, $n = p_1^{r_1}$

$p_1^{r_1} \cdot mua = nm(ua) = 0$

$\Rightarrow mua \in G(p_1)$

also

$n(nva) = v(mna) = 0$

so $o(nva)$ divides

$p_2^{r_2} \cdots p_k^{r_k}$

By inductive hypothesis

$$nva = a_2 + \cdots + a_k$$

w/ $a_i \in G(p_i)$ $i = 2, \ldots, k$.

Then $a = mva + nva$

$$= mva + a_2 + \cdots + a_k \quad //$$

$a_1 \in G(p_1)$

Thm: Let G be a finite abelian gp w/ $\#G = p_1^{r_1} \cdots p_k^{r_k}$ its prime decomposition.

Then $$G \cong G(p_1) \oplus \cdots \oplus G(p_k)$$

obs: $\to$ $\#G(p) = p^n$ for some n. If $p' \mid \#G(p)$

$G(p) \cong \mathbb{Z}_{p^n}$ ✗

$G(p) \cong \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_{p^{n-2}}$

$(1, 0, 0)$

$\mathbb{Z}_{nm} \cong \mathbb{Z}_n \oplus \mathbb{Z}_m$

$\iff (n, m) = 1$

Proof: For $a \in G$, $o(a) \mid \#G$

hence the prime in the decomposition of a are a subset of $\{p_1, \dots, p_k\}$. We can write

$(*)$ $a = a_1 + \dots + a_k$ w/

$a_i \in G(p_i)$ $i = 1, \dots, k$

We claim that the sum $(*)$

is unique: suppose that also

(**) $a = b_1 + \cdots + b_k$ w/

$b_i \in G(p_i)$, $i = 1, \ldots, k$.

Then

(Δ) $a_1 - b_1 = (b_2 - a_2) + \cdots + (b_k - a_k)$

$\uparrow$ $G(p_1)$ $\quad$ $\uparrow$ $G(p_2)$ $\quad$ $\uparrow$ $G(p_k)$.

$\Rightarrow \exists\ s_i \geq 0$ s.t.h

$o(b_i - a_i) = p_i^{s_i} \Leftrightarrow p_i^{s_i}(b_i - a_i) = 0$

If we set $m = p_2^{s_2} \cdots p_k^{s_k}$

then $m \cdot (b_i - a_i) = 0$

for $i = 2, \ldots, k$.

by (Δ) $m \cdot (a_1 - b_1) = 0$

$\Rightarrow$ the order of

$G(p_1) \ni (a_1 - b_1)$ divides

$$\underline{\underline{m}} = p_2^{s_2} \cdots p_k^{s_k}$$

So if $\sigma(a_1 - b_1) = p_1^{s_1}$

then $s_1 = 0$

so $a_1 = b_1$

Similarly $a_i = b_i \quad \forall i$.

We now define

$$f: \underset{\cup}{G} \longrightarrow G(p_1) \oplus \cdots \oplus G(p_k)$$

$$a = a_1 + \cdots + a_k \longmapsto (a_1, \ldots, a_k)$$

uniqueness of $a = a_1 + \cdots + a_k$

says that f is injective

f is surj since if

$(a_1, \ldots, a_k)$ then

$a = a_1 + \ldots + a_k$ and

$f(a) = (a_1, \ldots, a_k)$

f is a homomorphism

$a = a_1 + \ldots + a_k$

$b = b_1 + \ldots + b_k$

$\Rightarrow \quad a + b = \underbrace{(a_1 + b_1)}_{G(p_1)} + \ldots + \underbrace{(a_k + b_k)}_{G(p_k)}$

$\Rightarrow \quad f(a+b) = (a_1 + b_1, \ldots, a_k + b_k)$

$= (a_1, \ldots, a_k) + (b_1, \ldots, b_k)$

$= f(a) + f(b).$

So f is an iso. //