Chinese Remainder Theorem: 2022/10/17

$G \times G'$ product group

$G \times G'$ product group.

$$(g_1, g_1')\cdot(g_2, g_2') = (g_1 g_2, g_1' g_2').$$

Identity: $(1, 1')$. Inverse: $(g, g')^{-1} = (g^{-1}, g'^{-1})$.

We identify G with $\{(g, 1') \in G \times G' \mid g \in G\}$.

G' with $\{(1, g') \in G \times G' \mid g' \in G'\}$

- we proved that under this identification. G, G' are normal subgroups of $G \times G'$.
- $|G \times G'| = |G| \times |G'|$.

- Subgroups

Q. Given a group G. can we identify G as a product of its subgroups H & K? (i.e. $G \cong H\times K$)
with some "natural" choice of isomorphism.

$$\begin{tikzcd} H\times K \arrow[rr, "f"] & & G \\ & H \arrow[ul, "h \mapsto (h,1)"] \arrow[ur, "h \mapsto h"'] & \end{tikzcd} \qquad \begin{tikzcd} H\times K \arrow[rr, "f"] & & G \\ & K \arrow[ul, "k \mapsto (1,k)"] \arrow[ur, "k \mapsto k"'] & \end{tikzcd}$$

so we with $f(h,1)=h$. $f(1,k)=k$.

If f is an isomorphism. $f(h,k)=f(h,1)f(1,k)=hk$.
(note $(h,k)=(h,1).(1,k)$)

- Theorem

Theorem. G is a group. H, K are subgroups of G.
$f: H\times K \to G$, $f(h,k)=hk$ is an isomorphism iff the following 3 conditions hold:

1. H, K are normal subgroups of G
2. $H\cap K=\{1\}$.
3. $G=HK=\{hk\in G \mid h\in H, k\in K\}$.

- Proof

1. $\Rightarrow$

Proof. If $f: H\times K \longrightarrow G$ is an isomorphism, then normal subgroups map to normal subgroups. Since $H\times\{1\}$ and $\{1\}\times K$ are normal subgroups in $H\times K$, their images, H and K, are normal subgroups in G.

The image of f is HK, and f is an isomorphism, so $HK=G$.

Suppose $H\cap K\neq\{1\}$, then there exists $g\in H\cap K$, $g\neq 1$. But then $f(g,1)=g=f(1,g)$, contradict to f is an isomorphism. We conclude $H\cap K=\{1\}$.

2. $\Leftarrow$

• f is injective $\in K$: $(h,k) \in \mathrm{Ker}(f) \iff f(h,k) = 1$

$\iff hk = 1$

$\iff h = k^{-1}$

$\quad\quad\quad\quad \in H \quad \in K$

so $h = k^{-1} \in H \cap K = \{1\}$

$h = k^{-1} = 1, \quad h = k = 1.$

The assumption $HK = G$ implies f is surjective.

It remains to check f is a homomorphism. $f((h_1, k_1)(h_{@}, k_2)) = f(h_1h_2, k_1k_2) = h_1h_2k_1k_2$. It suffices to prove $hk = kh$ for any $h \in H$ and $k \in K$. $hk = kh$ if and only if $hkh^{-1}k^{-1} = 1$. Observe that $hkh^{-1}k^{-1} = (hkh^{-1})k^{-1}$. K is a normal subgroup, so $hkh^{-1} \in K$, $hkh^{-1}k^{-1} \in K$. Similarly we can show $hkh^{-1}k^{-1} \in H$, and by the fact $H \cap K = \{1\}$, we conclude $hkh^{-1}k^{-1} = 1$, i.e., $hk = kh$.

• $G = H \times K$

Notation. If $f: H \times K \to G$. $f(h,k) = hk$ is an isomorphism.

we say G is the product of H and K, write $G = H \times K$

Example. $K_4 = \{1, a, b, c\}$. The Klein Four Group.

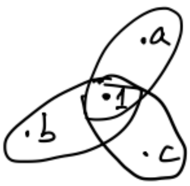
$\langle a \rangle = \{1, a\}$. $\langle b \rangle = \{1, b\}$

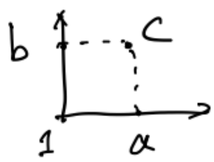
• K_4 abelian, so $\langle a \rangle$, $\langle b \rangle$ are normal subgroups.

• $\langle a \rangle \cap \langle b \rangle = \{1\}$

• $\langle a \rangle \langle b \rangle = \{1.1, 1.b, a.1, a.b\} = \{1, b, a, c\} = K_4$

so $K_4 = \langle a \rangle \times \langle b \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$





- Proposition

Prop. If r and s are relatively prime positive numbers.
then $C_{rs} \cong C_r \times C_s$ (C_k means cyclic group of order k)
(we can also write $\mathbb{Z}/rs\mathbb{Z} \cong \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z}$).

- Proof

Pf. $C_{rs} = \langle a \rangle$. $|a| = rs$.

Consider $\langle a^s \rangle$ and $\langle a^r \rangle$.

$|a^s| = r$, $|a^r| = s$

$(a^s)^k = 1 \Leftrightarrow a^{sk} = 1 \Leftrightarrow rs \mid sk \Leftrightarrow r \mid k$.

- $\langle a^s \rangle$ & $\langle a^r \rangle$ are normal subgroups. since C_{rs} is abelian.
- $\langle a^s \rangle \cap \langle a^r \rangle = \{1\}$ since $\gcd(|a^s|, |a^r|) = 1$:

Lemma. If H and K are subgroups of G. with $|H|, |K|$ relatively prime. then $H \cap K = \{1\}$.

Pf. $H \cap K$ is a subgroup of H. so $|H \cap K|$ divides $|H|$.
similarly, it divides $|K|$.
$\gcd(|H|, |K|) = 1$. so $|H \cap K| = 1$. $H \cap K = \{1\}$.

- $\langle a \rangle = \langle a^s \rangle \cdot \langle a^r \rangle$

only need to verify $\langle a \rangle \leq \langle a^s \rangle \langle a^r \rangle$.

$\gcd(s, r) = 1$. so $\exists k, l \in \mathbb{Z}$. $1 = ks + lr$

Then for any $m \in \mathbb{Z}$. $m = mks + mlr$

$$a^m = a^{mks+mlr} = (a^s)^{mk} \cdot (a^r)^{ml} \in \langle a^s \rangle \cdot \langle a^r \rangle$$

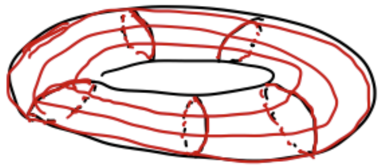
We conclude $C_{rs} = \langle a^s \rangle \times \langle a^r \rangle \cong C_r \times C_s$.

Interpretation: $\gcd(r,s)=1$.

6	12	3	9	15
11	2	8	14	5
1	7	13	4	10

s (rows), r (columns)

identify opposite edges to form a torus



By going "upper-right", we can visit all the squares.

Chinese Remainder Theorem

Chinese Remainder Theorem (Sun Zi Suan Jing) $\gcd(r,s)=1$.

The function $f: \mathbb{Z}/rs\mathbb{Z} \to \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z}$ is an isomorphism.

$$k \bmod rs \mapsto (k \bmod r,\ k \bmod s).$$

In practice, it means. the system of congruence equations

$$\begin{cases} x \equiv a \pmod{r} \\ x \equiv b \pmod{s} \end{cases}$$

has unique solution up to congruence mod rs.

$\gcd(r,s)=1$. so $\exists\, k,l$. $\boxed{kr+ls=1} \Rightarrow \begin{cases} ls \equiv 1 \pmod{r} \\ kr \equiv 1 \pmod{s} \end{cases}$

to find k,l. need to apply "Euclidean algorithm"

Let $\boxed{x = als + bkr.}$ $\leftarrow$ solution

$x \equiv als \equiv a \pmod{r}$

$x \equiv bkr \equiv b \pmod{s}$

Remarks ① This can be generalized to more equations:

$r_1, r_2, \ldots, r_n$ are pairwisely relatively prime

Then $\begin{cases} x \equiv a_1 \pmod{r_1} \\ x \equiv a_2 \pmod{r_2} \\ \vdots \\ x \equiv a_n \pmod{r_n} \end{cases}$ has unique solution, up to congruence mod $r_1 r_2 \cdots r_n$.

Correspondingly.

$$\underline{\mathbb{Z}/r_1 r_2 \cdots r_n\mathbb{Z} \cong \mathbb{Z}/r_1\mathbb{Z} \times \mathbb{Z}/r_2\mathbb{Z} \times \cdots \times \mathbb{Z}/r_n\mathbb{Z}}.$$

②. The isomorphism $f: \mathbb{Z}/rs\mathbb{Z} \xrightarrow{\cong} \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z}$ $\gcd(r,s)=1$.

is an isomorphism of "<u>rings</u>"

③ If $\gcd(r,s) \neq 1$. you can prove that

$\mathbb{Z}/rs\mathbb{Z}$ is not isomorphic to $\underline{\mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z}}$.

(idea: try to show in $\mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z}$ <u>there's no element of order rs</u>).

- $(g, g') \in G \times G'$. $|g| = m$, $|g'| = n$. What is $|(g,g')|$?

$$\underline{(g,g')^k} = (1, 1') \iff (g^k, g'^k) = (1, 1')$$
$$\iff \begin{cases} g^k = 1 \\ g'^k = 1 \end{cases}$$
$$\iff |g| \mid k,\ |g'| \mid k$$
$$\iff k \text{ is a common multiple of } m \,\&\, n.$$

So $\underline{\boxed{|(g,g')| = \mathrm{lcm}(m,n)}}$