Last class.

Theorem: Assume $\gcd(s,t) = 1$

$\Rightarrow U(st) \cong U(s) \oplus U(t)$

Proof. already showed last time:

If $\Phi: x \in U(st) \mapsto (x \bmod s,\ x \bmod t)$

then $\Phi(xy) = \Phi(x)\Phi(y)$

still to show:

1-1 and onto:

assume $\Phi(x) = \Phi(y)$

$\Rightarrow$ $x \bmod s = y \bmod s$, $x \bmod t = y \bmod t$ $\Rightarrow$ $s \mid (x-y)$, $t \mid (x-y)$

$\operatorname{lcm}(s,t) \mid (x-y)$

But $\operatorname{lcm}(s,t) = \dfrac{st}{\gcd(s,t)} = st$

$\Rightarrow \quad st \mid x-y \quad \Leftrightarrow \quad x \bmod st = y \bmod st$

i.e. x and y same in $U(st)$

onto follows from Φ being $1\text{-}1$ and from

$|\Phi(U(st))| = |U(st)| = \phi(st) = \phi(s)\,\phi(t) =$

(Φ is H; ϕ = Euler ϕ function; $\phi(st) = \phi(s)\,\phi(t)$ ← fact from number theory)

$= \#\{0 \le j < st,\ \gcd(j, st) = 1\}$

$= |U(s)|\,|U(t)| = |U(s) \oplus U(t)|$

As $\Phi(U(st)) \subset U(s) \oplus U(t) \Rightarrow$ equality.

Example: $U(15) \cong U(3) \oplus U(5)$

$\cong \mathbb{Z}_2 \oplus \mathbb{Z}_4$

Remark: (1) One can show

$U(p^n) \cong \mathbb{Z}_{(p-1)p^{n-1}}$ cyclic for $p > 2$

$U(2^n) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{2^{n-2}}$

Can use this to determine structure of $U(n)$ for any n.

e.g. $U(120) = U(2^3 \cdot 3 \cdot 5)$

$\cong U(2^3) \oplus U(3) \oplus U(5)$

$\cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4$

(2) If $n = pq$ p, q primes

$\Rightarrow \mathcal{U}(n) \cong \mathcal{U}(p) \oplus \mathcal{U}(q)$

$\cong \mathbb{Z}_{p-1} \oplus \mathbb{Z}_{q-1}$

in particular $|\mathcal{U}(n)| = (p-1)(q-1)$

If we know prime factorization $n = pq$

$\Rightarrow$ easy to calculate $|\mathcal{U}(n)| = (p-1)(q-1)$

$\Rightarrow$ " " " $j^m \bmod n$ for large m

(because $j^{(p-1)(q-1)} = 1 \bmod n$ $\forall j \in \mathcal{U}(n)$)

If we do not know prime factorization

$j^m \bmod n \stackrel{?}{=}$ hard

Key ingredient for RSA encryption (see book for details Chapter 8, p. 165)

Chapter 10 Homomorphisms

Def. G, H groups

A map $\Phi: G \to H$ is called a homomorphism if $\Phi(ab) = \Phi(a)\Phi(b)$ for all $a, b \in G$

Remark: unlike an isom., a homomorphism need not be 1-1 or onto.

Examples:

(1) Every isom. is a homom.

(2) $G = GL(2, \mathbb{R})$, $H = \mathbb{R}^* = (\mathbb{R} \setminus \{0\}, \cdot)$

Then $\Phi(A) = \det(A)$ for $A \in GL(2, \mathbb{R})$ is a homom.

proof: $\Phi(AB) = \det(AB) = \det(A)\det(B) = \Phi(A)\Phi(B)$ ✓ (lin. algebra)

(3) $G = S_n$ $H = \mathbb{Z}_2$

recall: A perm. π is called odd/even

if $\pi = s_1 s_2 \dots s_k$ where each s_i is a 2-cycle

such that k is odd/even.

Define $\Phi: S_n \to \mathbb{Z}_2$

$$\pi \to \begin{cases} 0 & \text{if } \pi \text{ even} \\ 1 & \text{if } \pi \text{ odd} \end{cases}$$

check hom. property case by case

let $\pi = s_1 \dots s_k$, $\sigma = t_1 \dots t_\ell$ s_i, t_j 2-cycles

check for all 4 cases k, ℓ odd/even that hom. prop. satisfied.

e.g. k odd, ℓ even $\Rightarrow$ $k+\ell$ odd

$\Phi(\pi) = 1$, $\Phi(\sigma) = 0$

$\pi\sigma = \underbrace{s_1 s_2 \dots s_k t_1 t_2 \dots t_\ell}_{k+\ell \text{ cycles}}$ odd perm. $\Rightarrow \Phi(\pi\sigma) = 1 = \Phi(\pi) + \Phi(\sigma)$

add. notation for $\mathbb{Z}_2$

Properties of Homomorphisms (see book Th. 10.1)

Let $\Phi: G \to H$ be a homom.

e_G and e_H identities of G and H

① $\Phi(e_G) = e_H$

② $\Phi(g^n) = \Phi(g)^n$

} proofs exactly same as for isomorphisms

②' $\Phi(g^{-1}) = \Phi(g)^{-1}$

(proof: $\Phi(g^{-1})\,\Phi(g) = \Phi(g^{-1}g) = \Phi(e_G) = e_H$

↑ hom. prop

simil. $\Phi(g)\,\Phi(g^{-1}) = \ldots = e_H$

by uniqueness of inverse $\Phi(g^{-1})$ must be the inverse of $\Phi(g)$

"$\Phi(g)^{-1}$

③ ord $\Phi(g)$ | ord (g)

proof. let $n = \text{ord}(g)$: $\Phi(g)^n = \Phi(g^n) = \Phi(e_G) = e_H$

$\Rightarrow \text{ord}\,\Phi(g) \mid n$.

Remark: For homom. Φ $\text{ord}\,\Phi(g)$ can be smaller than $\text{ord}(g)$

example: $\text{ord}(123) = 3$

but $\Phi: S_3 \to \mathbb{Z}_2$ as in Ex. 3

we have $\Phi(123) = 0$ in $\mathbb{Z}_2$ $\quad \text{ord}(0) = 1 \neq \text{ord}(123) = 3$

↑ even permutation

Def. $\Phi : G \to H$ hom.

we define the kernel of Φ by

$$\ker \Phi = \{ g \in G, \ \Phi(g) = e_H \}$$

Ex. $\Phi : S_n \to \mathbb{Z}_2$

$$\ker \Phi = \{ \pi \in S_n, \ \Phi(\pi) = 0 \bmod 2 \}$$
$$= \{ \pi \in S_n, \ \pi \text{ evens} \}$$
$$= A_n .$$

Lemma (a) $\ker \Phi$ is a normal subgroup of G

(b) $\Phi(a) = \Phi(b) \iff a \ker \Phi = b \ker \Phi$

Proof. @ subgroup test

$g, h \in K \Rightarrow \Phi(g) = e_H = \Phi(h)$

$\Rightarrow \Phi(gh) = \Phi(g)\Phi(h) = e_H e_H = e_H$

$\Rightarrow gh \in \ker \Phi$

$g \in \ker \Phi$: $\Phi(g^{-1}) = \Phi(g)^{-1} = e_H^{-1} = e_H$

$\Rightarrow g^{-1} \in \ker \Phi$