Lecture 6

recall definition: $S_n = \{\text{permutation of the set } \{1,2,\cdots,n\}\}$
S_n is a group. $|S_n| = n!$
If $\alpha \in S_n$, then $\alpha: \{1,\cdots,n\} \longrightarrow \{1,\cdots,n\}$ is a bijection function. And we can write $\alpha = \begin{bmatrix} 1 & 2 & \cdots & n \\ \alpha(1) & \cdots & & \alpha(n) \end{bmatrix}$

Cycle notation:
If $a_1,\cdots,a_n$ are distinct elements of $\{1,2,\cdots,n\}$. Then define $\alpha = (a_1,\cdots a_k) \in S_n$ by the following rule:
If $x = a_i$ for some i, $\alpha(x) = a_{i+1}$
If $x \neq a_i$ for some i, $\alpha(x) = x$

Facts
- If $\alpha = (a_1,\cdots,a_k)$ is a k-cycle in S_n, then $|\alpha| = k$.
- Every $\sigma \in S_n$ can be written as a product of disjoint cycles.
- disjoint cycles commute.
- If $\sigma \in S_n$ can be written as $\sigma = c_1 \cdots c_k$ where c_i are disjoint cycles. Then $|\sigma| = \{cm(|c_1|,|c_2|,\cdots,|c_k|)$
(least common multiple)

Definition: A transposition is a 2-cycle.
Theorem: Every element $\sigma \in S_n$ can be written as a product of transpositions.
Theorems: If $\sigma \in S_n$, and $\sigma = T_1 \times T_2 \times \cdots \times T_r$ are two different ways of writting $\sigma = P_1 P_2 \cdots P_s$ as a product of transpositions, then $r = s \bmod 2$

Definition: $\sigma \in S_n$ is even if σ can be written as product of an even number of transpositions.
Let $A_n = \{\sigma \in S_n \mid \sigma \text{ is even}\}$

Facts: — A_n is a subgroup of S_n
— $|A_n| = n!/2$

Q: Find the elements of A_6 of order 5
⇕
Find elements of S_6 of order 5 that happen to lie in A_6.
⇕
Permutations that are a product of a 1-cycle and a 5-cycle that disjoint from each other.

A: $6 \times 4!$ elements

CHAPTER 6 ISOMORPHISM

$\mu_4 = \{4\text{th roots of unity in } \mathbb{C}\}$
$\mathbb{Z}_4 = \{0,1,2,3\} \bmod 4$

Def: Let $G, \overline{G}$ be a pair of groups. A **group isomorphism** from G to $\overline{G}$ is a bijection $\phi: G \to \overline{G}$ s.t. $\forall a,b \in G$, $\phi(ab) = \phi(a)\phi(b)$

multiplication in G — multiplication in $\overline{G}$.

E.g.
Let's define $\phi: \underset{(G)}{\mathbb{Z}_4} \longrightarrow \underset{(\overline{G})}{\mu_4}$

$\phi(0)=1 \quad \phi(1)=i \quad \phi(2)=-1 \quad \phi(3)=-i$

- $\phi(1+1)=\phi(1)\phi(1)$
  $\phi(2)= i \cdot i = -1$
- $\phi(k)= e^{2\pi i \frac{k}{4}} = e^{2\pi i(\frac{k}{4})}$

$\phi(k+j) = e^{2\pi i(\frac{k+j}{4})} = e^{2\pi i \frac{k}{4}} \cdot e^{2\pi i \frac{j}{4}}$

E.g.
Define: $\phi : \mathbb{Z}_n \longrightarrow \mu_n$

$\phi(k) = e^{2\pi i \frac{k}{n}}$

Claim ϕ is an isomorphism

- Define $\psi : \mathbb{Z}_n \to \mu_n$
  $\psi(k) = e^{-2\pi i \frac{k}{n}}$
  verify ψ is an isomorphism but $\psi \neq \phi$

Fact: there will be $\phi(n) = \#\{k \mid 0 \le k < n, \gcd(k,n)=1\}$
$= |U(n)|$
distinct isomorphism.

E.g. $\alpha: \mathbb{R} \to \mathbb{R}_{>0} \quad \alpha(x) = 2^x$

Claim: α is an isomorphism
α is a bijection because it has 2-sided inverse $\alpha^{-1}: \mathbb{R}_{>0} \to \mathbb{R}$
$y \longmapsto \log_2(y)$

And we need to check that $\alpha(x+y) = \alpha(x)\alpha(y)$
i.e. $2^{x+y} = 2^x 2^y$. but this is clear.

Example: let G be a cyclic group with generator a. Then $G = \langle a \rangle$. If G is infinite, then G is isomorphic to $\mathbb{Z}$.

Consider $G=\{a^k \mid k\in\mathbb{Z}\}$
Since G is infinite, $a^k=a^j$ iff $k=j$
So define $\phi: G\to\mathbb{Z}$ by $\phi(a^k)=k$
Then ϕ is clearly a bijection and $\phi(a^k a^l)=\phi(a^{k+l})=k+l=\phi(a^k)\phi(a^l)$
Similarly, if $|G|=n<\infty$, then define $\phi: G\to\mathbb{Z}_n$ by $\phi(a^k)=k\in\mathbb{Z}_n$
Since $a^k=a^j$ in G iff $k=j \bmod n$. ϕ is well defined and $\phi(a^k a^j)=\phi(a^{k+l})=k+l=\phi(a^k)\phi(a^l)$

Punchline: "up to isomorphism" i.e. considering isomorphic groups to be the same. $\mathbb{Z}_n$ and $\mathbb{Z}$ are the only cyclic groups.

Non-example: Define $f:\mathbb{R}\to\mathbb{R}$ by $f(x)=x^3$
f is not a isomorphism because $(x+y)^3\neq x^3+y^3$.
If it were isomorphic, we would need $f(x+y)=f(x)+f(y)\ \forall x,y\in\mathbb{R}$.

Cayley's Theorem: Every group is a subgroup of a symmetric group. $\Leftrightarrow$ every group is isomorphic to some permutation group.

Proof: Let G be a group. Let's consider G as a set.
Let permutation$(G)=\{$all permutations of $G\}=\{$bijections $\alpha: G\to G\}$
$\forall g\in G$, we can define $T_g\in \text{Perm}(G)$ by
$T_g(h)=gh\ \forall h\in G$

ex: T_g is a bijection.

Let $\overline{G}=\{T_g \mid g\in G\}\subseteq \text{Perm}(G)$
Define $\phi: G\to\overline{G}$ by $\phi(g)=T_g$
Ex: $T_{gh}=T_gT_h$. So $\phi(gh)=T_{gh}=T_gT_h=\phi(g)\phi(h)$
ϕ is a bijection.

Properties of isomorphic groups

Let $\phi: G\to\overline{G}$ be an isomorphism.
① $\phi(e)=e \longrightarrow e$ in $\overline{G}$
↳ e in G
② $\forall a\in G,\ \phi(a^n)=[\phi(a)]^n$
③ $\forall a,b\in G,\ ab=ba$ iff $\phi(a)\phi(b)=\phi(b)\phi(a)$ in $\overline{G}$.
④ $G=\langle G\rangle$ iff $\overline{G}=\langle\phi(a)\rangle$
- $|G|=|\overline{G}|$
- If $\phi: G\to\overline{G}$ is an isomorphism. Then $\phi^{-1}:\overline{G}\to G$ is also an isomorphism.

Antumorphisms (self-morphisms)
Def: An automorphism of G is an isomorphism $\alpha: G\to G$.
i.e. $\alpha(ab)=\alpha(a)\alpha(b)\ \forall a,b\in G$

E.g. $\phi:\mathbb{Z}\to\mathbb{Z}$ by $\phi(n)=-n$
$\phi(n+m)=-(n+m)=(-n)+(-m)=\phi(n)+\phi(m)$

E.g. $\phi:\mathbb{C}\to\mathbb{C}$

$\phi(\bar{z}) = \overline{\bar{z}}$
$\phi(z+u) = \overline{z+u} = \bar{z} + \bar{u} = \phi(z) + \phi(u)$

E.g. Let G be any group. Then $id_G : G \to G$ is an isomorphism.

Special type of isomorphism: inner automorphism.
Let G be any group. and let $a \in G$ be any element. Then define $\phi_a : G \to G$ by $\phi_a(g) = aga^{-1}$ (conjugation by a). Then ϕ_a is an automorphism.
Proof: ϕ_a is a bijection because $(\phi_a)^{-1} = \phi_{a^{-1}}$
$\phi_{a^{-1}} \circ \phi_{a^{-1}} = \phi_{a^{-1}}(aga^{-1}) = a^{-1}g\,a^{-1}(a^{-1})^{-1} = g$
Similarly $\phi_a \circ \phi_{a^{-1}} = id_G$
And $\forall x, y \in G$, $\phi_a(xy) = axya^{-1} = axa^{-1}aya^{-1} = (axa^{-1})(aya^{-1})$
$= \phi_a(x) \cdot \phi_a(y)$

- Let $Aut(G) = \{\text{automorphisms of } G\}$
- Let $Inn(G) = \{\text{inner automorphisms of } G\}$

Theorem: $Aut(G)$ is a group under composition.
Theorem: $Inn(G)$ is a group under composition.

Pf: key points: $\phi_a \circ \phi_b = \phi_{ab}$
$(\phi_a)^{-1} = \phi_{a^{-1}}$

Fact $Inn(G) \leq Aut(G)$

E.g. What is $Inn(\mathbb{Z}_5)$?
Let $a \in \mathbb{Z}_5$. The inner automorphism corresponding to $a \in \mathbb{Z}_5$ is
$\phi_a : \mathbb{Z}_5 \to \mathbb{Z}_5$.
$\phi_a(k) = "aka^{-1}" = a + k + (-a) = k$
So $Inn(G)$ is just the identity automorphism.

Thm: If G is Abelian, $Inn(G)$ is just the identity automorphism.

proof: $a \in G$, $aga^{-1} = a\,a^{-1}g = g$

E.g. What's $Inn(D_4)$?
recall $D_4 = \{R_0, R_{90}, R_{180}, R_{270}, V, H, D, D'\}$
What's ϕ_{R_0}?
$\phi_{R_0}(H) = R_0 H R_0^{-1} = H$
In fact, $\phi_{R_0} = id_{D_4}$
$\phi_{R_{90}}(H) = R_{90} H R_{90}^{-1} = R_{90} H R_{270} = V$

$\phi_{R_{90}}(R_0) = R_0$	$\phi_{R_{90}}(H) = V$
$\phi_{R_{90}}(R_{90}) = R_{90}$	$\phi_{R_{90}}(V) = H$
$\phi_{R_{90}}(R_{180}) = R_{180}$	$\phi_{R_{90}}(D) = D'$
$\phi_{R_{90}}(R_{270}) = R_{270}$	$\phi_{R_{90}}(D') = D$

E.g. What's $Aut(\mathbb{Z}_{10})$?
Sps $\alpha : \mathbb{Z}_{10} \to \mathbb{Z}_{10}$. Then $\alpha(k) = \alpha(1+\cdots+1) = k\alpha(1)$
So α is determined by $\alpha(1)$
So we just have to decide what are the possibilities for $\alpha(1)$.

We saw that: If $G=\langle G\rangle$. and $\psi: G \to \overline{G}$ is isomorphism. that $\overline{G}=\langle \phi(a)\rangle$

So in our example of $\mathbb{Z}_{10}$, we must have $\langle \alpha(1)\rangle = \mathbb{Z}_{10}$.

So $\alpha(1) \in \{1,3,7,9\} = U(10)$

Exercise: prove $\exists$ 4 automorphisms of $\mathbb{Z}_{10}$.

one with $\alpha(1)=1$, one with $\alpha(1)=3$, $\cdots$ 7, $\cdots$, 9.

So in general, consider $Aut(\mathbb{Z}_n)$ if $\alpha \in Aut(\mathbb{Z}_n)$. then α is determined by $\alpha(1)$ as before.

All as before, α will be an automorphism iff $\alpha(1) \in U(n)$

Fact: $\forall p \in U(n)$, $\exists$ a unique automorphism α_p s.t. $\alpha_p(1)=p$. In fact, we can write an explicit formula for α_p.

$$\alpha_p(k) = pk \quad \forall k \in \mathbb{Z}_n$$

Thm: The function $A: U(n) \to Aut(\mathbb{Z}_n)$

$A(p)=\alpha_p$

is an isomorphism.

Ch 6 Practice Problems

1/1, 2/2, 4/4, 5/5, 9/9, 11/11

need examples: 4, 5, 6, 7