MATH 3030 ALGEBRA I

Lecture 4

Cayley's Theorem

Let X be a nonempty set.

Let S_X be the set of all bijective maps $\sigma : X \to X$.
(permutations)

Recall that S_X is a group under composition of maps.

We call S_X the group of permutations of X or
the symmetric group on X.

Thm (Cayley) Every group is isomorphic to a group of permutations.
More precisely, for any group G, $\exists X \neq \emptyset$ s.t. G is isomorphic to a subgroup of $(S_X, \circ)$. Also, X is finite if G is finite.

(Slogan: groups are "symmetries".)

<u>Pf</u>: The idea is to define a 1-1 homomorphism $\phi : G \hookrightarrow S_G$.

Let $g \in G$. Define
$$\begin{aligned} \lambda_g : G &\longrightarrow G \\ a &\longmapsto ga \end{aligned}$$

Now,

λ_g is 1-1: $g a_1 = g a_2 \Rightarrow g^{-1} g a_1 = g^{-1} g a_2 \Rightarrow a_1 = a_2$

λ_g is onto: $\forall b \in G$, let $a = g^{-1} b \in G$. Then $\lambda_g(a) = b$.

Hence $\lambda_g \in S_G$ and we set $\phi(g) = \lambda_g$.

ϕ is a homomorphism:
$$\begin{aligned} \phi(g_1 g_2) = \lambda_{g_1 g_2} : G &\longrightarrow G \\ a &\longmapsto g_1 g_2 a \end{aligned}$$

and
$$\begin{aligned} \lambda_{g_1} \circ \lambda_{g_2} : G &\xrightarrow{\lambda_{g_2}} G \xrightarrow{\lambda_{g_1}} G \\ a &\longmapsto g_2 a \longmapsto g_1 g_2 a \end{aligned}$$

$$\Rightarrow \phi(g_1 g_2) = \lambda_{g_1 g_2} = \lambda_{g_1} \circ \lambda_{g_2} = \phi(g_1) \circ \phi(g_2)$$

ϕ is 1-1 : $\lambda_{g_1} = \lambda_{g_2} \Rightarrow \lambda_{g_1}(e) = \lambda_{g_2}(e) \Rightarrow g_1 = g_2$

The Thm now follows from the previous lemma. #

Rmk : $\phi : G \hookrightarrow S_G$ is called the left regular representation of G.
$g \longmapsto \lambda_g$

We can also define

$\psi : G \hookrightarrow S_G$ where $\mu_g : G \to G$ is defined by
$g \longmapsto \mu_g$

$\mu(a) = ag^{-1}$

This is called the right regular representation of G.

Group actions

Def Let X be a nonempty set and let G be a group. An action of G on X or a G-action on X is a map

$$\begin{aligned} G \times X &\longrightarrow X \\ (g, x) &\longmapsto g \cdot x \end{aligned}$$

s.t. (1) $e \cdot x = x \quad \forall x \in X$

(2) $(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x) \quad \forall x \in X \;\&\; \forall g_1, g_2 \in G$

Under these conditions, we call X a G-set.

Rmk: Informally, we denote a G-action on X by $G \curvearrowright X$.

Prop An action of G on X is equivalent to a group homomorphism

$$\rho : G \longrightarrow S_X$$

where S_X is the group of permutations of X under composition.

Pf: Given an action of G on X: $G \times X \longrightarrow X$

$$(g, x) \longmapsto g \cdot x \, .$$

For $g \in G$, define $\rho(g) : X \longrightarrow X$ by

$$x \longmapsto g \cdot x$$

$\rho(g)$ is 1-1 : $g \cdot x = g \cdot y \Rightarrow g^{-1} \cdot (g \cdot x) = g^{-1} \cdot (g \cdot y)$

$\Rightarrow (\cancel{g^{-1} \cdot g})^{e} \cdot x = (\cancel{g^{-1} \cdot g})^{e} \cdot y$ by (2)

$\Rightarrow x = y$ by (1)

$\rho(g)$ is onto: $\forall x \in X$, let $y := g^{-1}\cdot x$. Then

$$\rho(g)(y) = g\cdot y = g\cdot(g^{-1}\cdot x) \underset{\text{by }(2)}{=} (\cancelto{e}{g\cdot g^{-1}})\cdot x \overset{\text{by }(1)}{=} x$$

Hence this defines a map

$$\rho : G \longrightarrow S_X .$$

Now ρ is a homomorphism

$$\iff \quad \rho(g_1 g_2) = \rho(g_1)\circ\rho(g_2) \quad \forall g_1, g_2 \in G$$

$$\iff \quad \rho(g_1 g_2)(x) = \rho(g_1)\big(\rho(g_2)(x)\big) \quad \forall g_1, g_2 \in G \ \& \ \forall x \in X$$

$$\iff \quad (g_1 g_2)\cdot x = g_1\cdot(g_2\cdot x) \quad \forall g_1, g_2 \in G \ \& \ \forall x \in X$$

which is condition (2) in the definition of a G-action.

This shows that a G-action on X gives rise to a group homomorphism $\rho : G \longrightarrow S_X$.

Conversely, given a homomorphism $\rho : G \longrightarrow S_X$, we can define a map

$$G \times X \longrightarrow X$$
$$(g, x) \longmapsto g.x := \rho(g)(x)$$

(1) : $e.x = \rho(e)(x) = id_X(x) = x \quad \forall x \in X$

(2) : $\forall g_1, g_2 \in G$, we have

since ρ is a homomorphism

$$(g_1 g_2).x = \rho(g_1 g_2)(x) = (\rho(g_1) \circ \rho(g_2))(x) = g_1.(g_2.x)$$

for all $x \in X$.

Hence this is an action of G on X. #

Examples

- For any set $X \neq \emptyset$ and any group G, $G \curvearrowright X$ by $g \cdot x = x$ $\forall x \in X$ $\forall g \in G$.
  This is called the trivial action.
- $S_n \curvearrowright I_n = \{1, 2, \ldots, n\}$
- $D_n \curvearrowright$ the regular n-gon Δ_n
- $GL_n(\mathbb{R}) \curvearrowright \mathbb{R}^n$ (or more generally, $GL(V) \curvearrowright V$)

$$GL_n(\mathbb{R}) \times \mathbb{R}^n \longrightarrow \mathbb{R}^n$$
$$(A, \vec{x}) \longmapsto A\vec{x}$$

(view $\vec{x}$ as a column vector)

Similarly, $SL_n(\mathbb{R}) \curvearrowright \mathbb{R}^n$, $O_n \curvearrowright \mathbb{R}^n$; $GL_n(\mathbb{C}) \curvearrowright \mathbb{C}^n$, $SL_n(\mathbb{C}) \curvearrowright \mathbb{C}^n$, etc.

- If V is a vector space $/\mathbb{R}$ (or $\mathbb{C}$ or any field F)
  $\mathbb{R}^\times$ (or $\mathbb{C}^\times$ or $F^\times$) acts on V by scalar multiplication.

- $G \curvearrowright G$

$$\begin{aligned} G \times G &\longrightarrow G \\ (g, x) &\longmapsto gx \end{aligned} \qquad \left(\text{or} \quad \begin{aligned} G &\xrightarrow{\sigma} S_G \\ g &\longmapsto \left(\sigma_g : \begin{aligned} G &\to G \\ x &\mapsto gx \end{aligned} \right) \end{aligned} \right)$$

remember Cayley's thm ? — left action; similarly, have right action.

- If $H < G$ & $G \curvearrowright X$, there is an induced action of H on X by restriction.

- $\boxed{\text{Conjugate action}}$ $G \curvearrowright G$

$$\begin{aligned} G \times G &\longrightarrow G \\ (g, x) &\longmapsto gxg^{-1} \end{aligned} \qquad \left(\text{or} \quad \begin{aligned} G &\xrightarrow{i} \mathrm{Aut}(G) \\ g &\longmapsto \left(i_g : \begin{aligned} G &\to G \\ x &\mapsto gxg^{-1} \end{aligned} \right) \end{aligned} \right)$$

- G also acts on the set $X := \{H \mid H < G\}$ of all subgroups of G by conjugation. Then $H < G$ is normal iff it's a fixed point of this action.

Def: Let $G \times X \to X$ be a G-action on X.

We say the action is faithful if $g \cdot x = x \ \forall x \in X$ implies $g = e$.

(i.e. $\rho : G \to S_X$ is injective or $\mathrm{Ker}(\rho) = \{e\}$)

We say the action is transitive if

$$\forall x_1, x_2 \in X, \ \exists g \in G \ \text{ s.t. } \ x_2 = g \cdot x_1$$

e.g.

- $S_n \curvearrowright I_n$ is faithful and transitive.
- $D_n \curvearrowright \{\text{vertices of } \Delta n\}$ is faithful and transitive.
- $GL_n(\mathbb{R}) \curvearrowright \mathbb{R}^n$ is faithful but not transitive.
- The left and right regular representations are faithful.
- The conjugate action $G \curvearrowright G$ is faithful iff $Z(G) = \{e\}$.

For a G-set X, we consider the following.

I) Let $g \in G$. Define

$$X_g := \{ x \in X \mid g \cdot x = x \}$$

This is the subset of X fixed by g.

We call $x \in X_g$ a fixed point of g or we say g fixes x.

The set

$$X_G := \bigcap_{g \in G} X_g = \{ x \in X \mid g \cdot x = x \ \forall g \in G \}$$

is called the set of fixed points of the G-action.

e.g.
- For $S_n \curvearrowright I_n$, the fixed point set $= \emptyset$
- For the conjugate action $G \curvearrowright G$, the fixed point set is

$$G_G = \{ x \in G \mid g x g^{-1} = x \ \forall g \in G \} = Z(G)$$

II) Let $x \in X$

Prop Define $G_x = \{g \in G \mid g \cdot x = x\}$. Then $G_x < G$

Pf: Let $g_1, g_2 \in G_x$. Then $g_1 \cdot x = g_2 \cdot x = x$

So $g_2^{-1} \cdot x = g_2^{-1} \cdot (g_2 \cdot x) = x$.

And $(g_1 g_2^{-1}) \cdot x = g_1 \cdot (g_2^{-1} \cdot x) = g_1 \cdot x = x$. Hence $g_1 g_2^{-1} \in G_x$. #

We call G_x the stabilizer (or isotropy subgroup) of $x \in X$.

e.g. • For $S_n \curvearrowright I_n$, $S_n > (S_n)_k \cong S_{n-1}$ for any $k \in I_n = \{1, 2, \dots, n\}$

• For the conjugate action $G \curvearrowright G$, the stabilizer of $x \in G$

$$Z_G(x) := G_x = \{g \in G \mid gx = xg\}$$

is also called the centralizer of $x \in G$.

III) Let $x \in X$. Define

$$G\cdot x = \{g\cdot x \mid g \in G\} \subset X$$ (We also denote $G\cdot x$ by $\bar{x}$)

This is called the orbit of x under the G-action.

Define a relation on X by

$x_1 \sim x_2$ iff $\exists g \in G$ s.t. $g\cdot x_1 = x_2$

Then $\sim$ is an equivalence relation and the equivalence classes are precisely the orbits in X under the G-action. (check this!)

Rmk $G \curvearrowright X$ is transitive $\Leftrightarrow$ # of orbits $= 1$

e.g. orbits of the cyclic subgroup $\langle\sigma\rangle < S_n$ on $I_n = \{1, 2, \ldots, n\}$ give the cycle decomposition of σ;

$\langle\sigma\rangle \curvearrowright I_n$ transitive iff σ is a cycle of length n.

Prop For an action $G \curvearrowright X$, we have

(1) $|G\cdot x| = [G : G_x]$ $\forall x \in X$.

(2) Hence, if $|X| < \infty$ and $G\cdot x_1, \dots, G\cdot x_n$ are all the distinct orbits in X with $|G\cdot x_i| > 1$, then

$$|X| = |X_G| + \sum_{i=1}^{n} [G : G_{x_i}]. \qquad \text{(class equation)}$$

Pf: Define a map

$$\zeta : G\cdot x \longrightarrow \{\text{left cosets of } G_x \text{ in } G\}$$
$$g\cdot x \longmapsto gG_x$$

ζ is well-defined: $g_1\cdot x = g_2\cdot x \Leftrightarrow (g_2^{-1}g_1)\cdot x = x \Leftrightarrow g_2^{-1}g_1 \in G_x$

& 1-1 $\qquad \Leftrightarrow g_1G_x = g_2G_x$

ζ is clearly onto. This proves (1).

(2) follows from (1) and the observation that

$$|G\cdot x| = 1 \Leftrightarrow g\cdot x = x \ \forall g \in G \Leftrightarrow x \in X_G. \ \#$$

e.g. $S_n \curvearrowright I_n$ is transitive $\Rightarrow |I_n| = n = [S_n : S_{n-1}]$

Conjugate action

$$\begin{aligned} G \times G &\longrightarrow G \\ (g,x) &\longmapsto gxg^{-1} \end{aligned} \qquad \text{or} \qquad \begin{aligned} i : G &\longrightarrow \mathrm{Aut}(G) \\ g &\longmapsto \left(\begin{aligned} i_g : G &\longrightarrow G \\ x &\longmapsto gxg^{-1} \end{aligned} \right) \end{aligned}$$

- The orbit of $x \in G$: $\bar{x} = G \cdot x = \{ gxg^{-1} \mid g \in G \}$ is called the conjugacy class of x (cf. similar matrices in linear algebra)
- The stabilizer of $x \in G$: $Z_G(x) := G_x = \{ g \in G \mid gxg^{-1} = x \}$ is called the centralizer of x
- Each $i_g \in \mathrm{Aut}(G)$ is called an inner automorphism of G; the set of all inner automorphisms is denoted by $\mathrm{Inn}(G)$.

  We have $\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$ and the quotient $\mathrm{Out}(G) := \mathrm{Aut}(G)/\mathrm{Inn}(G)$ is called the outer automorphism group of G.

e.g. • For abelian groups, the conjugate action is trivial.

• In S_n, two permutations are conjugate iff they have the same cycle type (why?)

For example, in S_4, there are 5 conjugacy classes:

conj. class	$\overline{(1\ 2\ 3\ 4)}$	$\overline{(1\ 2\ 3)}$	$\overline{(1\ 2)}$	$\overline{(1)}$	$\overline{(1\ 2)(3\ 4)}$
size	$3\cdot 2=6$	$4\cdot 2=8$	$\binom{4}{2}=6$	1	$\frac{1}{2}\cdot\binom{4}{2}=3$

In general, # of conjugacy classes in $S_n = p(n) =$ # of partitions of n.

Cor Let G be a finite group.

(1) $|\bar{x}| = [G : Z_G(x)]$.

(2) Let $\bar{x}_1, \dots, \bar{x}_n$ ($x_i \in G$) be all the distinct conjugacy classes of G with $|\bar{x}_i| > 1$. Then

$$|G| = |Z(G)| + \sum_{i=1}^{n} [G : Z_G(x_i)]$$

This is called the class equation of G.

As an application, we have

Prop If G is a finite group of order p^r where p is a prime and $r \in \mathbb{Z}_{>0}$, then $Z(G)$ is nontrivial.

Pf: By the class equation, we have

$$|G| = |Z(G)| + \sum_{i=1}^{n} [G : Z_G(x_i)]$$

where $\bar{x}_1, \dots, \bar{x}_n$ are all the distinct conjugacy classes of G with $|\bar{x}_i| > 1$.

Since $[G : Z_G(x_i)] \,\big|\, |G| = p^r$ & $[G : Z_G(x_i)] = |\bar{x}_i| > 1$, we have $p \,\big|\, [G : Z_G(x_i)]$

Hence, $|Z(G)| = |G| - \sum_i [G : Z_G(x_i)]$ is divisible by p.

In particular, $Z(G)$ cannot be trivial. #

Cor If $|G| = p^2$ where p is prime, then G is abelian.

Pf: If $Z(G) = G$, then G is abelian.

Otherwise, $|Z(G)| = p \Rightarrow |G/Z(G)| = p$.

So $G/Z(G)$ is cyclic and hence G is abelian (by Q.37 in Ex 15). #

Cor If $|G| = p^3$ where p is prime, then either

- G is abelian, or
- G is nonabelian with $Z(G) \cong \mathbb{Z}_p$ and $G/Z(G) \cong \mathbb{Z}_p \times \mathbb{Z}_p$

Pf: If $Z(G) = G$ then G is abelian.

If $|Z(G)| = p^2$ then $G/Z(G)$ is cyclic and G is again abelian

So if G is nonabelian, then we must have $|Z(G)| = p$

In this case, $G/Z(G)$ cannot be cyclic, so $G/Z(G) \cong \mathbb{Z}_p \times \mathbb{Z}_p$. #

Rmk: When $|G| = p^3$, there are exactly 2 nonabelian groups.

For example, when $|G| = 2^3 = 8$, the 2 nonabelian groups are D_4 and $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ – the quaternion group.