Math 210A Notes

Fall, 2025

Contents

1 Preliminaries **3**

1.1 Groups, Permutations and Cycle Decompositions 3

1.2 Orders of Permutations 5

1.3 Homomorphism and Isomorphism 6

1.4 Group Actions 8

1.5 Permutations and Group Actions 9

2 Subgroups **11**

2.1 Subgroups 11

Chapter 1

Preliminaries

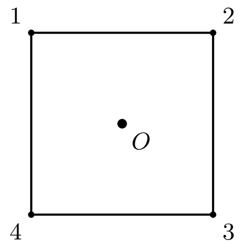
1.1 Groups, Permutations and Cycle Decompositions

Definition 1.1.1. (Group)
A group is an ordered pair $(G, *)$ where G is a set and $*$ is a mapping from $G \times G$ to G (called a binary operation) satisfying the following:

1. $\forall a, b, c \in G \quad a * (b * c) = (A * b) * c$ (associativity)
2. $\exists e \in G$ such that $e * a = a = a * e \quad \forall a \in G$ (identity element)
3. $\forall a \in G, \exists a^{-1} \in G$ such that $a * a^{-1} = e = a^{-1} * a$ (inverse element)

From now on we write $a * b = ab$.

Definition 1.1.2. (Permutations)
Let Ω be a nonempty set. The mapping $\sigma : \Omega \to \Omega$ is a permutation of Ω if σ is a bijection.



Here is a square centered at the origin. Take a copy of the square, move it around in 3-space, and lay it back down to cover the original square. This is called a rigid motion of the square, or a symmetry of the square. This creates a permutation of the vertices. How many symmetries are possible?

For the arbitrary symmetry of the square, we have 4 choices where to find 1. Once we know where vertex 1 is (say, vertex i), then vertex 2 can be one of 2 places. This gives 4 × 2 symmetries. Consider the regular n-gon centered at the origin. How many symmetries do we have? $2n$.

Fact 1. (Properties of Permutations)

1. Functional composition is associative. For mappings σ, τ, μ
$$\sigma \circ (\tau \circ \mu) = (\sigma \circ \tau) \circ \mu$$
2. The identity mapping on any set ($I(x) = x$) is a bijection of that set.
3. If σ is a bijection from a set Ω to Ω, then there is a bijection of Ω called σ^{-1} such that $\sigma \circ \sigma^{-1} = I = \sigma^{-1} \circ \sigma$.

Definition 1.1.3. (Order)
For $a \in G$, where G is a group, the order of a, denoted $|a|$, is the smallest positive integer k such that $a^k = e$ if such a k exists. If no such k exists, then we say a has infinite order and $|a| = \infty$.

Notation . (Cycle Decomposition)
A permutation σ of a set Ω can be written as a product of disjoint cycles. For example, if σ is a permutation of $\{1, 2, 3, 4, 5\}$ such that $\sigma(1) = 3$, $\sigma(3) = 1$, $\sigma(2) = 5$, $\sigma(5) = 2$, and $\sigma(4) = 4$, then we can write

$\sigma = (1\ 3)(2\ 5)(4)$. The order of a cycle is the number of elements in the cycle. The order of a permutation is the least common multiple of the orders of the disjoint cycles.

Example 1.1.1.
If $\sigma = (1\ 2)(3\ 2)$, then $\sigma(3) = 1$.
If $\mu = (3\ 2)(1\ 2)$, then $\mu(3) = 2$.
S_n is not abelian for $n \geq 3$.

1.2 Orders of Permutations

S_X refers to the set of all permutations on the set X. That is, the elements of S_X are bijections from X to itself. S_n refers to when $X = \{1, 2, \dots, n\}$.

Let $n = 5$. How many elements are in S_5? $5! = 120$. Why? Given a $\sigma \in S_5$, we have 5 choices for $\sigma(1)$, 4 for $\sigma(2)$, ... so there are $5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 5! = 120$ choices for σ. In general, there $n!$ elements in S_n.

S_5 : how many cycles of length 5 are in S_5?

$$\begin{tikzcd} (1\ 2\ 3\ 4\ 5) & (5\ 4\ 3\ 2\ 1) \\ (1\ 2\ 3\ 5\ 4) & \cancel{(2\ 3\ 4\ 5\ 1)} \arrow[ul, bend left] \end{tikzcd}$$

$\vdots$

There are 5! ways of filling in a blank 5-cycle. However, each 5-cycle is represented 5 ways, so we divide by 5. Thus there are $\frac{5!}{5} = 4! = 24$ distinct 5-cycles in S_5.How many

$$\begin{aligned} 4 \text{ cycles? } & \frac{5 \cdot 4 \cdot 3 \cdot 2}{4} = 30 \\ 3 \text{ cycles? } & \frac{5 \cdot 4 \cdot 3}{3} = 20 \\ 2 \text{ cycles? } & \frac{5 \cdot 4}{2} = 10 \\ 1 \text{ cycles? } & \frac{5}{1} = 5 \end{aligned}$$

How many distinct r-cycles $r \leq n$ are there in S_n? $\frac{n!}{r(n-r)!}$

$$\frac{n \cdot (n-1) \cdot (n-2) \cdots (n-r+1)}{r!}$$

How many distinct elements of the form (__)(___) disjoint in S_5?

$$\frac{5 \cdot 4}{2} \cdot \frac{3 \cdot 2 \cdot 1}{3} = 20$$

How many of the form (__)(__)?

$$\frac{\frac{5 \cdot 4}{2} \cdot \frac{3 \cdot 2}{2}}{2} = \frac{30}{2} = 15$$

How many distinct elements of the form (__)(___) in S_n?

$$\frac{n \cdot (n-1)}{2} \cdot \frac{(n-2)(n-3)(n-4)}{3}$$

How many distinct elements of the form (__)(__) in S_n?

$$\frac{\frac{n \cdot (n-1)}{2} \cdot \frac{(n-2)(n-3)}{2}}{2}$$

Definition 1.2.1. (Field)
$(F, +, \cdot)$ is a field if

1. $(F, +)$ is an abelian group with identity 0
2. $(F \setminus \{0\}, \cdot)$ is an abelian group with identity 1
3. Left and right distributive laws hold

The following are groups:

$$\begin{aligned} GL_n(F) &= \{\text{all } n \times n \text{ matrices with entries in } F \text{ and with non-zero determinants}\} \\ SL_n(F) &= \{\text{all } n \times n \text{ matrices with entries in } F \text{ and with determinant } 1\} \end{aligned}$$

1.3 Homomorphism and Isomorphism

In general, we can tell how similar groups are by the mappings we make between them where the mappings preserve the group structure of the domain.

Definition 1.3.1. (Homomorphism)
Let $(G, \star)$ and $(H, \diamond)$ be groups. A map $\Phi : G \to H$ is a homomorphism if for all $g_1, g_2 \in G$,

$$\Phi(g_1 \star g_2) = \Phi(g_1) \diamond \Phi(g_2)$$

We usually write

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

and we know that xy happens in G and $\Phi(x)\Phi(y)$ happens in H.

Example 1.3.1. $\pi : \mathbb{R}^2 \to \mathbb{R}$ by $\pi(x, y) = x \ \forall (x, y) \in \mathbb{R}^2$ is a homomorphism. Letting $(x_1, y_1), (x_2, y_2) \in \mathbb{R}^2$, we have

$$\begin{aligned} \pi((x_1, y_1) + (x_2, y_2)) &= \pi(x_1 + x_2, y_1 + y_2) \\ &= x_1 + x_2 \\ &= \pi(x_1, y_1) + \pi(x_2, y_2) \end{aligned}$$

Showing that π is indeed a homomorphism.
What elements are in the set $\left\{p \in \mathbb{R}^2 : \pi(p) = 0\right\} = K$?

$$K = \{(x, y) : x = 0\}$$

This is the kernel of π.

Definition 1.3.2. (Kernel)
Let G and H be groups and let $\Phi : G \to H$ be a group homomorphism. The kernel of Φ is

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

where e_H is the identity element in H.

Definition 1.3.3. (Isomorphism)
Let G and H be groups. A map $\Psi : G \to H$ is an isomorphism if

1. Ψ is a homomorphism
2. Ψ is bijective

If there exists an isomorphism $\Psi : G \to H$, we say that G and H are isomorphic, denoted $G \cong H$.
$\cong$ is an equivalence relation on any collection of groups.

Example 1.3.2. Let $k \in \mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$. Define $\phi_k : \mathbb{Q}^* \to \mathbb{Q}^*$ by $\phi_k(q) = kq$. We claim that ϕ is an isomorphism. Show that Φ_k is a homomorphism and a bijection:

1. Homomorphism:

$$\begin{aligned} \phi_k(q_1 + q_2) &= k(q_1 + q_2) \\ &= k(q_1 + q_2) \\ &= kq_1 + kq_2 \\ &= \phi_k(q_1) + \phi_k(q_2) \end{aligned}$$

2. Bijections:

- Injective: Suppose $\phi_k(q_1) = \phi_k(q_2)$. Then

$$\begin{aligned} & \phi_k(q_1) = \phi_k(q_2) \\ \iff & kq_1 = kq_2 \\ \iff & q_1 = q_2 && (k \neq 0) \end{aligned}$$

- Surjective: We want to show $\phi_k(\mathbb{Q}) = \mathbb{Q}$. Let $q \in \mathbb{Q}$. Since $k \neq 0$, $\frac{q}{k} \in \mathbb{Q}$. Then

$$\phi_k\left(\frac{q}{k}\right) = k \cdot \frac{q}{k} = q$$

  Thus ϕ_k is surjective.

$\ker \phi_k = \{0\}$ since $\phi_k(q) = 0 \iff kq = 0 \iff q = 0$.

Fact 2. Suppose $G \cong H$, that is there exists $\phi : G \to H$ which is a homomorphic bijection. Then

1. $|G| = |H|$
2. G is abelian if and only if $|H|$ is abelian
3. $\forall x \in G \;\; |x| = |\phi(x)|$ (Corresponding elements have the same order)

1.4 Group Actions

There are many examples of groups acting on sets. For instance, consider an element in S_5, call it σ. σ is a permutation of $\{1,2,3,4,5\}$ and it is also an element of a group

$$\sigma = (1\ 2\ 3\ 4\ 5)$$
$$\sigma(5) = 4$$

We say that σ is acting on the set $\{1,2,3,4,5\}$.

Consider the set of all 2×2 matrices with elements in $\mathbb{R}$. Let $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ and let $k \in \mathbb{R}$. Then $kA = \begin{bmatrix} k & 2k \\ 3k & 4k \end{bmatrix}$. We say that $\mathbb{R}$ is acting on the set of all 2×2 matrices with elements in $\mathbb{R}$.

Definition 1.4.1. (Group Action)
Let G be a group and A be a set. A group action of G on A is a map from $G \times A$ to A (written $g.a \;\; \forall g \in G, a \in A$) such that

1. $g_1.(g_2.a) = (g_1g_2).a \;\; \forall g_1, g_2 \in G$ (Compatability)
2. $1.a = a$ (or $e.a = a$) $\quad \forall a \in A$ (Identity)

Example 1.4.1. Let $G = S_n$. Let's verify that S_n acts on the set $\{1,2,...,n\}$. Define the group action

$$\sigma.a = \sigma(a) \;\; \forall \sigma \in S_n, a \in \{1,2,...,n\} \tag{$*$}$$

Then let $\sigma_1, \sigma_2 \in S_n$ and $a \in \{1,2,...,n\}$. We have

$$\begin{aligned} \sigma_1.(\sigma_2.a) &= \sigma_1.(\sigma_2(a)) \\ &= \sigma_1(\sigma_2(a)) \\ &= (\sigma_1 \circ \sigma_2)(a) \\ &= (\sigma_1 \circ \sigma_2).a \end{aligned} \tag{I}$$

To verify the identity property, recall that the identity map, denoted I, is the identity of S_n and

$$I(a) = a \;\; \forall a \in \{1,2,...,n\}$$

That is,

$$I.a = I(a) = a \;\; \forall a \in \{1,2,...,n\} \tag{II}$$

By (I) and (II), S_n acts on the set $\{1,2,...,n\}$ by the group action defined in $(*)$.

Example 1.4.2. A vector space over a field F is a set V with two binary operations vector addition and scalar multiplication, and other popperties including

- $a(bv) = (ab)v \;\; \forall a, b \in F, v \in V$ (Compatability)
- $1v = v \;\; \forall v \in V$ where 1 is the multiplicative identity in F (Identity)

Since F is not a group with respect to multiplication, we must say that $F^* = F \setminus \{0\}$ acts on V.

1.5 Permutations and Group Actions

Let G be a group acting on a set S. That is, define a mapping $G \times S \to S$ denoted by $g.a \quad \forall g \in G$ and $a \in S$. Fix $g \in G$. Then this defines a map σ_g such that $\sigma_g : S \to S$ by $\sigma_g(a) = g.a$

Example 1.5.1. Take $G = \mathbb{R} \setminus \{0\}$ with respect to multiplication. Let $S = M_2(\mathbb{R})$.

$$\begin{aligned} \sigma_{\sqrt{2}}(A) &= \sqrt{2}.A \\ &= \sqrt{2}\begin{bmatrix} a & b \\ c & d \end{bmatrix} \\ &= \begin{bmatrix} \sqrt{2}a & \sqrt{2}b \\ \sqrt{2}c & \sqrt{2}d \end{bmatrix} \end{aligned}$$

For $\begin{bmatrix} 1 & \pi \\ e & \ln(2) \end{bmatrix}$, we have

$$\sigma_{\sqrt{2}}\begin{bmatrix} 1 & \pi \\ e & \ln(2) \end{bmatrix} = \begin{bmatrix} \sqrt{2} & \sqrt{2}\pi \\ \sqrt{2}e & \sqrt{2}\ln(2) \end{bmatrix}$$

What is the range of $\sigma_{\sqrt{2}}$? $M_2(\mathbb{R})$.

Asserttion 1.

1. σ_g as defined is a permutation of the set S.
2. For the sake of notation, we change the name of our set to A. The map from G to S_A defined by $g \mapsto \sigma_g$ is a homomorphism.

Proof.

1. Let $g \in G$ be given and σ_g be defined as above. Clearly, σ_g is a mapping from $S \to S$. We will show that σ_g is a bijection by showing it has a two-sided inverse. Let $a \in S$ and note $g^{-1} \in G$ since G is a group. Then

$$\begin{aligned} \left(\sigma_{g^{-1}} \circ \sigma_g\right)(a) &= \sigma_{g^{-1}}(\sigma_g(a)) \\ &= \sigma_{g^{-1}}(g.a) \\ &= g^{-1}.(g.a) \\ &= (g^{-1}g).a \\ &= e.a \\ &= a. \end{aligned}$$

We see that $\sigma_{g^{-1}} \circ \sigma_g$ is the identity mapping from $S \to S$. To show that $\sigma_g \circ \sigma_{g^{-1}}$ is also the identity map from $S \to S$ is analogous. Thus we have a two-sided inverse as desired. Hence, σ_g is a permutation of S as desired. That is, σ_g is an element of the symmetric group of S.

2. Let $\Psi : G \to S_A$ be defined by $\Psi(g) = \sigma_g \quad \forall g \in G$. Let $a \in A$ and $g_1, g_2 \in G$. We want to show that $\Psi(g_1 g_2) = \Psi(g_1) \circ \Psi(g_2)$. Since these are mappings in S_A, we will show that their values agree $\forall a \in A$. We have

$$\begin{aligned} \left(\Psi(g_1) \circ \Psi(g_2)\right)(a) &= \sigma_{g_1 g_2}(a) \\ &= (g_1 g_2).a \\ &= g_1.(g_2.a) \\ &= g_1.(\sigma_{g_2}(a)) \\ &= \sigma_{g_1}(\sigma_{g_2}(a)) \\ &= \sigma_{g_1} \circ \sigma_{g_2}(a) \\ &= \left(\Psi(g_1) \circ \Psi(g_2)\right)(a). \end{aligned}$$

Hence, Ψ is a homomorphism as desired.

□

If we have a homomorphism, then we have a kernel.

Definition 1.5.1. (Kernel of a Group Action)
For a group G acting on a set A, the kernel of the group action is

$$\{g \in G : g.a = a \quad \forall a \in A\}$$

Chapter 2

Subgroups

2.1 Subgroups

Definition 2.1.1. (Subgroup)
Let G be a group. The subset H of G is called a subgroup of G if

1. H is nonempty.
2. $\forall x, y \in H$, $x^{-1} \in H$ and $xy \in H$.

Notation . IF H is a subgroup of G, we write $H \leq G$.

Example 2.1.1.

1. $\mathbb{Z} \leq \mathbb{Q}$ with respect to $(+)$.
2. All groups have two subgroups: $H = G$ and $H = \{1\}$.
3. $2\mathbb{Z} \leq \mathbb{Z}$ with respect to $(+)$.
4. Let $G = D_{2n}$ and let r be a $360°/n$ clockwise rotation of the n-gon about the origin. Then $\left\{1, r, r^2, r^3, ..., r^{n-1}\right\}$ forms a subgroup of D_{2n}.
5. Nonexample: $H = \{1, -1\} \subseteq \mathbb{Z}$ forms a group with respect to multiplicaiton, but H is not a subgroup of $\mathbb{Z}$ since $\mathbb{Z}$ is a group with respect to addition, NOT multiplicaiton.
6. $\mathbb{Z}/5\mathbb{Z}$ is not a subgroup of $\mathbb{Z}/6\mathbb{Z}$ since $\mathbb{Z}/5\mathbb{Z} \not\subseteq \mathbb{Z}/6\mathbb{Z}$.

$$\begin{aligned} \mathbb{Z}/6\mathbb{Z} &= \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\} \text{ is an additive group} \\ (\mathbb{Z}/6\mathbb{Z})^* &= \{\bar{1}, \bar{5}\} \text{ is a multiplicative group with all elements coprime to 6} \\ (\mathbb{Z}/9\mathbb{Z})^{**} &= \{\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}\} \text{ is a multiplicative group with all elements coprime to 9} \end{aligned}$$

Proposition 2.1.1. (Subgroup Criterion)
A subset H of a group G is a subgroup of G if and only if

1. $H \neq \emptyset$.
2. $\forall x, y \in H$, $xy^{-1} \in H$ (in additive notation: $\forall x, y \in H$, $x - y \in H$).