Math 210A Notes

Fall, 2025

Contents

Chapter 1

Preliminaries

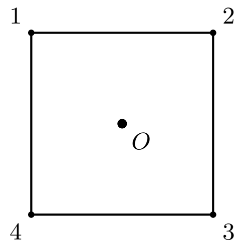
1.1 Groups, Permutations and Cycle Decompositions

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 1.1.1. (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 $X = \{1, 2, \ldots, n\}$.

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

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

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 1.3.1. 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. $\forall x \in G \quad |x| = |\phi(x)|$ (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. $g_1.(g_2.a) = (g_1 g_2).a \ \ \forall g_1, g_2 \in G$ (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 poperties 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 $g.a \ \ \forall g \in G$ 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 $\Psi(g) = \sigma_g \ \ \forall g \in G$. Let $a \in A$ and $g_1, g_2 \in G$. We want to show that $\Psi(g_1g_2) = \Psi(g_1) \circ \Psi(g_2)$. Since these are mappings in S_A, we will show that their values agree $\forall a \in A$. We have

$$\begin{aligned}\left(\Psi(g_1) \circ \Psi(g_2)\right)(a) &= \sigma_{g_1g_2}(a) \\ &= (g_1g_2).a \\ &= g_1.(g_2.a) \\ &= g_1.(\sigma_{g_2}(a)) \\ &= \sigma_{g_1}(\sigma_{g_2}(a)) \\ &= \sigma_{g_1} \circ \sigma_{g_2}(a) \\ &= \left(\Psi(g_1) \circ \Psi(g_2)\right)(a).\end{aligned}$$

   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: $\forall x, y \in H$, $x - y \in H$).

2.2 Centralizers and Normalizers, Stabilizers and Kernels

Definition 2.2.1. (Centralizers)
Let A be a nonempty subset of a group G. Define the centralizer of A in G to be the set

$$\begin{aligned} C_G(A) &= \{g \in G : gag^{-1} = g \quad \forall a \in A\} \\ &= \{g \in G : ga = ag \quad \forall a \in A\} \end{aligned}$$

The centralizer of A in G is the set of all elements in G which commute with every element in A.

Theorem 2.2.1. $C_G(A) \leq G$.

Proof. Let $a \in A$. Then

$$\begin{aligned} 1a1^{-1} &= (1a)1^{-1} \\ &= a1^{-1} \\ &= a1 \\ &= a \end{aligned}$$

Thus, $1 \in C_G(A)$.
Let $x, y \in C_G(A)$. Then $xax^{-1} = a$ and $yay^{-1} = a$. Note that

$$yay^{-1} = a \iff a = y^{-1} \tag{$*$}$$

Now

$$\begin{aligned} (xy^{-1})a(xy^{-1})^{-1} &= xy^{-1}a(y^{-1})^{-1}x^{-1} \\ &= x(y^{-1}ay)x^{-1} \\ &\overset{(*)}{=} xax^{-1} \\ &= a \end{aligned}$$

Hence, $xy^{-1} \in C_G(A)$. Furthermore, $C_G(A) \leq G$. □

Notation . If $A = \{a\}$, we write $C_G(a)$ instead of $C_G(\{a\})$.

Why was this unnecessary? From the homework, we know that G acts on the subset A by conjugation. That is, we have a mapping $(.) : G \times A \to A$ defined by $g.a = gag^{-1} \quad \forall g \in G, a \in A$ which satisfies both axioms of a group action.

Recall that the kernel of a group action is the kernel of the permutation representation of the group action (PRGA). The PRGA is the Homomorphism induced by the group action

$$\begin{aligned} \Psi : G &\to S_A \\ g &\mapsto \sigma_g \end{aligned}$$

Example 2.2.1. Find the kernel of G acting on $A \subset G$ by conjugation.

$$\begin{aligned} \{g \in G : g.a = a \quad \forall a \in A\} &= \left\{g \in G : gag^{-1} = a \quad \forall a \in A\right\} \\ &= C_G(A) \end{aligned}$$

Suppose that $A = G$. What is $C_G(G)$?

$$\left\{g \in G : gag^{-1} = a \quad \forall a \in G\right\}$$

This set is called the center of G denoted $Z(G)$. Since $Z(G)$ is a special case of $C_G(A)$, we know $Z(G) \leq G$.

Definition 2.2.2. (Normalizer)
Define $gAg^{-1} = \left\{gag^{-1} : a \in A\right\}$. We will define the normalizer of A in G to be the set

$$N_G(A) = \left\{g \in G : gAg^{-1} = A\right\}$$

We will prove $N_G(A) \leq G$, but not yet. Notice if $gag^{-1} = a \quad \forall a \in A$ then $gAg^{-1} = \{gag^{-1} : a \in A\} = \{a : a \in A\} = A$. Hence

$$C_G(A) \subseteq N_G(A)$$

Fact 2.2.1.

1. If G is abelian, then $Z(G) = G$ since every element commutes with every other element. That is,

$$\begin{aligned} \forall a, b \in G \;\; ab = ba &\iff a = bab^{-1} \;\; \forall a, b \in G \\ &\implies b \in Z(G) \;\; \forall b \in G \end{aligned}$$

   Similarly, $C_G(A) = N_G(A) = G$.

2. Consider $A = \{1, (1\ 2)\} \subseteq S_3$. Find $C_{S_3}(A)$. Notice that 1 commutes with everything in S_3, specifically 1 and $(1\ 2)$. Also,

$$(1\ 2)(1\ 2)(1\ 2)^{-1} = (1\ 2)$$

   so $(1\ 2) \in C_{S_3}(A)$. Hence, $A \leq C_{S_3}(A)$.

   Theorem 2.2.2. (Lagrange's Theorem)
   Let G be a finite group ($|G| \in \mathbb{N}$) and let $H \leq G$. Then

$$|H| \text{ divides } |G|$$

   Since $|A| = 2$ and $A \leq C_{S_3}(A)$, we know $2\big||C_{S_3}(A)|$ since $C_{S_3}(A) \leq S_3$.

$$\left.\begin{aligned} &|C_{S_3}(A)|\big||S_3| = 3! = 6 \\ &|A|\big||C_{S_3}(A)| \end{aligned}\right\} \implies |C_{S_3}(A)| \in \{2, 6\}$$

   . Thus, $C_{S_3} = A$ or $C_{S_3}(A) = S_3$. Well,

$$\begin{aligned} (1\ 2)(1\ 2\ 3) &= (2\ 3) \\ (1\ 2\ 3)(1\ 2) &= (1\ 3) \end{aligned}$$

   so $(1\ 2\ 3) \notin C_{S_3}(A)$. It follows that $|C_{S_3}(A)| = 2 \implies C_{S_3}(A) = A$.

Let G be a group acting on a set S. That is, there is a mapping

$$(.,.) : G \times S \to S$$

denoted by $g.a \quad \forall a \in S$ with $g_1.(g_2.a) = (g_1 g_2).a$ and $1.a = a \quad \forall a \in S, g_1, g_2 \in G$.

Definition 2.2.3. (Stabilizers)
If G is a group acting on a set S and $s \in S$, then we define the stabilizers of s in G to be the set

$$G_s = \{g \in G : g.s = s\}$$

Theorem 2.2.3. $G_s \leq G$.

Proof. Since G acts on S we know that $1.s = s$. Hence $1 \in G_s \implies G_s \neq \emptyset$. Let $x, y \in G_s$. Then

$$\begin{aligned} s = 1.s &= (y^{-1}y).s \\ &= y^{-1}.(y.s) \\ &= y^{-1}.s \qquad \text{(since } y \in G_s\text{)} \end{aligned}$$

Hence $y^{-1} \in G_s$. Furthermore,

$$\begin{aligned} (xy).s &= x.(y.s) \\ &= x.s \\ &= s \end{aligned}$$

Hence $xy \in G_s$. Thus, $G_s \leq G$. □

Now to show $N_G(A)$ where $A \subseteq G$ is a subgroup of G. To that end, let $S = \mathcal{P}(G)$, the power set of G, and define a map

$$G \times S \to S \text{ by } g.B = gBg^{-1} = \left\{gbg^{-1} : \forall g \in G, B \in \mathcal{P}(G)\right\}$$

Let's prove this defines a group action. Let $g_1, g_2 \in G$ and $B \in \mathcal{P}(G)$. Well,

$$1.B = \left\{1b1^{-1} : b \in B\right\} = \{b : b \in B\} = B$$

so the identity axiom holds. Furthermore,

$$\begin{aligned}
(g_1g_2).B &= (g_1g_2)B(g_1g_2)^{-1} \\
&= \left\{(g_1g_2)b(g_1g_2)^{-1} : b \in B\right\} \\
&= \left\{(g_1g_2)b(g_2^{-1}g_1^{-1}) : b \in B\right\} \\
&= \left\{g_1(g_2bg_2^{-1})g_1^{-1} : b \in B\right\} \\
&= \left\{g_1b'g_1^{-1} : b' \in g_2Bg_2^{-1}\right\} \\
&= g_1\left(g_2Bg_2^{-1}\right)g_1^{-1} \\
&= g_1\left(g_2.B\right)g_1^{-1} \\
&= g_1.(g_2.B)
\end{aligned}$$

Hence, we have defined a group action. Now, back to showing that $N_G(A) \leq G$ $(A \subseteq G)$.

Recall, $G_s = \{g \in G : g.s = s\}$. Given our new group action G acting on $\mathcal{P}(G)$ by conjugation, we have

$$\begin{aligned}
G_a &= \{g \in G : g.A = A\} \\
&= \left\{g \in G : gAg^{-1} = A\right\} \\
&= N_G(A)
\end{aligned}$$

We can then deduce that $N_G(A) \leq G$ as $G_A \leq G$.

2.3 Cyclic Groups

Definition 2.3.1. (Cyclic Group)
A group H is cyclic if H is generated by a single element. That is,

$$\exists x \in H \text{ such that } H = \{x^n : n \in \mathbb{Z}\}$$

$$(\exists x \in H \text{ such that } H = \{nx : n \in \mathbb{Z}\} \text{ using additive notation})$$

We write $< x >= H$ (x generates H).

Example 2.3.1.

1. $\mathbb{Z} =< 1 >=< -1 >$
2. The rotations in D_{2n} are generated by r ($360/n$ clockwise rotation)
3. $U_4 = 1, -1, i, -i =< i >$

Note . If $H =< x >= \{x^n : n \in \mathbb{Z}\}$, we define

$$x^0 = 1$$
$$x^{-n} = (x^n)^{-1} = (x^{-1})^n \text{ for } n > 0$$

Proposition 2.3.1. If $H =< x >$, then $|H| = |x|$. If one side of this equality is infinity, then so is the other. More specifically,

1. If $|x| = n < \infty$, then $x^n = 1$ and $1, x, x^2, ..., x^{n-1}$ are all the distinct elements of H.
2. If $|x| = \infty$, then $x^n \neq 1$ when $n \neq 0$ and $x^a \neq x^b$ for all $a \neq b \in \mathbb{N}$.

Proof. Let $|x| = n$.

1. Consider the case where $n < \infty$. Consider the elements $1, x, x^2, ..., x^{n-1}$ and suppose $x^a = x^b$ where $0 \leq a < b < n$. Then

$$\begin{aligned} x^a = x^b &\implies 1 = x^b x^{-a} \\ &\implies 1 = x^{b-a} \end{aligned}$$

   Since $b - a > 0$, this contradicts n being the order of x. Thus, all the $1, x, x^2, ..., x^{n-1}$ are distinct. Also, $x^n = 1$ as $n = |x|$. Thus H contains at least n elements. It remains to show we have all of them.
   Let $t \in Z$ such that $x^t \in H$. By the division algorithm, there exitst $q, r \in \mathbb{Z}$ such that

$$t = qn + r \text{ where } 0 \leq r < n$$

   Then

$$\begin{aligned} x^t = x^{qn+r} &= x^{qn} x^r \\ &= (x^n)^q x^r \\ &= 1^q x^r \\ &= x^r \in \left\{1, x, x^2, ..., x^{n-1}\right\} \text{ since } 0 \leq r < n \end{aligned}$$

   Hence, $H = \left\{1, x, x^2, ..., x^{n-1}\right\}$.

2. Next, suppose $|x| = \infty$ (no positive powers of x is the identity). For the sake of contradiction, if $x^a = x^b$ with $a < b$ then $x^{a-b} = 1$, a contradiction. So distinct powers of x give distinct elements of H. It follows that $|H| = \infty$.

□

Proposition 2.3.2. Let G be a group and let $x \in G$. Let $m, n \in \mathbb{Z}$. If $x^n = 1$ and $x^m = 1$, then $x^d = 1$ where $d = \gcd(m, n)$. In particular, if $x^m = 1$ for some $m \in \mathbb{Z}$ then $|x||m$.

Proof. Let m, n, d be defined as above. Then by the Euclidean algorithm

$$\exists x_0, y_0 \in \mathbb{Z} \text{ such that } d = mx_0 + ny_0$$

Then

$$\begin{aligned} x^d &= x^{mx_0+ny_0} \\ &= (x^m)^{x_0}(x^n)^{y_0} \\ &= 1^{x_0}1^{y_0} \\ &= 1 \end{aligned}$$

To prove the second assertion, let $x^m = 1$ and $n = |x|$. Then $x^n = 1$ by definition of order.

Case 1: If $m = 0$ then certainly $n|m$.

Case 2: Let $m \neq 0$. We know $n < \infty$ since $x^m = 1$. Let $d = \gcd(m, n)$ and hence by the first assertion $x^d = 1$. Since $0 < d \leq n$ and n is the smallest positive integer such that $x^n = 1$, we have that $n = d$. By definition,

$$d|m \implies n|m \text{ as desired.}$$

□

Theorem 2.3.1. (Cyclic Groups Isomorphisms)

1. Any infinite cyclic group $< x >$ is isomorphic to $\mathbb{Z}$ (with the mapping $\phi : \mathbb{Z} \to < x >$, $k \mapsto x^k$).
2. If $< x >$ and $< y >$ are cyclic groups both with order $n < \infty$, then

$$\begin{gathered} \phi :< x > \to < y > \\ x^k \mapsto y^k \end{gathered}$$

   is a well-defined isomorphism.

We will use multiplicative notation when describing an arbitrary cyclic group of order $n \in \mathbb{N}$, and denote this group $\mathbb{Z}_n$. NOT to be confused with the additive group $\mathbb{Z}/n\mathbb{Z}$, which is cyclic of order n. Most times we will refer to an infinite cyclic group as $\mathbb{Z}$.

Proposition 2.3.3. (The Order of x^a in a Cyclic Group)
Let G be a group and let $x\imath 9nG$. Let $a \in \mathbb{Z} - \{0\}$.

1. If $|x| = \infty$, then $|x^a| = \infty$.
2. If $|x| = n < \infty$, then $|x^a| = \frac{n}{\gcd(n,a)}$.

In particular, $|x^a| = \frac{n}{a}$ when $a|n$ ($a \in \mathbb{N}$).

Proof. We start with the following claim: Let $a, n, \in \mathbb{Z}$ not both zero.

$$\text{If } \gcd(a, n) = d \text{ then } \gcd(\frac{a}{d}, \frac{n}{d}) = 1$$

> **Proof.** Let a, n and d be as defined. Then there exists $x_0, y_0 \in Z$ such that
>
> $$d = ax_0 + ny_0$$
>
> It follows that
>
> $$1 = \frac{a}{d}x_0 + \frac{n}{d}y_0$$
>
> Since $\gcd(\frac{a}{d}, \frac{n}{d})$ divides $\frac{a}{d}$ and $\frac{n}{d}$, $\gcd(\frac{a}{d}, \frac{n}{d})$ divides the right-hand side, so $\gcd(\frac{a}{d}, \frac{n}{d})|1$. Thus, $\gcd(\frac{a}{d}, \frac{n}{d}) = 1$. □

1. Suppose by way of contradiction that

$$|x| = \infty \text{ and } |x^a| = m < \infty$$

By definition of order

$$(x^a)^m = 1 \iff x^{am} = 1$$

It follows that

$$(x^{am})^{-1} = 1^{-1} \iff x^{-am} = 1$$

Since $a \neq 0$ by assumption and $m \neq 0$ by definition of order, then $am \neq 0$ and one of $-am$ or am is positive, so some positive power of x is the identity, contradicting $|x| = \infty$. So, $|x^a| = \infty$.

2. Let $|x| = n < \infty$ and let $y = x^a$, $\gcd(a, n) = d$. We also write $n = db$ and $a = dc$ for some integers c, b (not thate $b > 0$). From our claim,

$$\gcd(c, b) = \gcd(\frac{a}{d}, \frac{n}{d}) = 1$$

We want to show that $|y| = b$. To this end, cotice that

$$\begin{aligned} y^b = (x^a)^b &= x^{ab} \\ &= x^{(dc)b} \\ &= x^{(dc)(\frac{n}{d})} \\ &= (x^n)^c \\ &= 1^c \\ &= 1 \end{aligned}$$

Thus, $|y|$ divides b. Let $k = |y|$. Then

$$y^k = 1 = x^{ak}$$

Hence, $|x| \mid ak$. That is,

$$\begin{aligned} n \mid ak &\iff db \mid dck \\ &\iff b \mid ck \\ &\iff \frac{n}{d} \mid \frac{a}{d} k \end{aligned}$$

Since $\frac{n}{d}$ and $\frac{a}{d}$ are relatively prime, this gives $\frac{n}{d} \mid k$, that is $b \mid k$. Since $b \mid k$ and $k \mid b$, $k = b$ as both $k, b \in \mathbb{N}$. □

Proposition 2.3.4. Let $H =< x >$.

1. Assume $|x| = \infty$. then $H =< x^a >$ if and only if $a = \pm 1$.
2. Assume $|x| = n\infty$. Then $H =< x^a >$ if and only if $\gcd(a, n) = 1$. In particular, the number of generators of H is $\phi(n)$, where ϕ is Euler's Phi funciton.

Proof. 2. If $|x| = n < \infty$, we know that $|x^a| = | < x^a > |$. This subgroup equals all of $H \iff |x^a| = n \iff \frac{n}{\gcd(a,n)} = n \iff \gcd(a, n) = 1$. Since $\phi(n)$ is the number of $a \in \{1, 2, 3, ..., n\}$, which are relatively prime to n, $\phi(n)$ gives the number of generators of H. □

What are the generators of $< x >= \mathbb{Z}_{10}$? $\phi(1) = \phi(2)\phi(5) = 4$

$$x^1, x^3, x^7, x^9$$

What are the generators of $\mathbb{Z}/15\mathbb{Z} =< \overline{1} >= \left\{ k\dot{1} : k \in \mathbb{Z} \right\}$?

$$\overline{1}, \overline{2}, \overline{4}, \overline{7}, \overline{8}, \overline{11}, \overline{13}, \overline{14}$$

Theorem 2.3.2. (Subgroups of Cyclic Groups)
Let $H =< x >$ be a cyclic group.

1. Every subgroup of H is cyclic. More precisely, if $K \leq H$ then either

$$K = \{1\} \text{ or } K =< x^d >$$

where d is the smallest positive integer such that $x^d \in K$.

2. If $|H| = \infty$, then for any distinct nonnegative integers a and b
$$< x^a > \neq < x^b >$$
and $\forall m \in \mathbb{Z}$
$$< x^m > = < x^{|m|} >$$
where $|m|$ denotes the absolute value of m. So, the nontrivial subgroups of H correspond bijectively with the integers $1, 2, 3, ...$

3. If $|H| = n < \infty$, then for every $a \in \mathbb{N}$ which divides n, there is a unique subgroup H with order a. This subgroup is the cyclic group $< x^d >$ where $d = \frac{n}{a}$. Furthermore, for every $m \in \mathbb{Z}$, $< x^m > = < X^{\gcd(n,m)} >$ so the subgroups of H correspond bijectively with the positive divisors of n.

Proof. 1. Let $K \leq H$. If $K = \{1\}$, then we are done. Suppose $K \neq \{1\}$. Thus, there exists some $a \neq 0$ such that $x^a \in K$. Since K is a group, $(x^a)^{-1} \in K$. That is, $x^{-a} \in K$, and since either a or $-a$ must be positive the set of all positive powers of x such that x to that positive power is an element of K is nonempty. That is,
$$P = \{n \in \mathbb{N} : x^n \in K\} \neq \emptyset$$
Thus, by the well-ordering principle, the set P contains a minimal element, call it d. By definition, $x^d \in K$. and since K is a group $< x^d > \leq K$. Let $k \in K$. Then, $k = x^b$ for some $b \in \mathbb{Z}$. By the division algorithm, we have integers q, r, such that
$$b = qd + r \text{ where } 0 \leq r < d$$
Hence,
$$\begin{aligned} x^b &= x^{qd+r} \\ \implies x^b &= (x^{qd})x^r = (x^d)^q x^r \\ \implies (x^d)^{-q} x^b &= x^r \end{aligned}$$
Since $x^d, x^b \in K$ and K is a group,
$$(x^d)^{-q} \in K \text{ and } (x^d)^{-q} x^b \in K$$
so $x^r \in K$. However, since d is the minimal positive power of x such that $x^d \in K$, r must not be a positive power. Therefore, $r = 0$ and it follows that
$$k = x^b = (x^d)^q \in < x^d >$$
Therefore, $K \leq < x^d >$. This gives $< x^d > = K$.

2. Suppose $|H| = n < \infty$ and $a \mid n$ where $a \in \mathbb{Z}$. Let $d = \frac{n}{a}$. Hence
$$| < x^d > | = \frac{n}{n/a} = a$$

Uniqueness: To show uniqueness, suppose K is any subgroup of H of order a. Then by part 1, $K = < x^b >$ where b is the smallest positive integer such that $x^b \in K$. We know
$$\frac{n}{d} = a = |K| = |x^b| = \frac{d}{\gcd(n, b)}$$
It follows that
$$d = \gcd(n, b)$$
Hence, $d \mid b$ by definition and $x^b \in < x^d >$. It follows that
$$K = < x^b > \leq < x^d >$$
and so $K = < x^d >$ as they have the same order. The final assertion follows from the fact that
$$< x^m > \leq < x^{\gcd(m,n)} >$$

and 2.3.3 (2) says

$$|< x^m >| = \frac{n}{\gcd(n,m)}$$

and

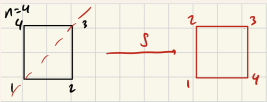
$$\left|x^{\gcd(m,n)}\right| = \frac{n}{\gcd(n,\gcd(m,n))}$$

and we know $\gcd(n,\gcd(m,n)) = \gcd(n,m)$. Since $\gcd(,m,n) \mid n$ this shows that every subgroup of H arises from a divisor of n. □

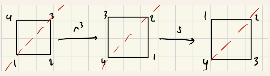
2.4 Subgroups Generated by Subsets of a Group

We have already examined the case of generating a subgroup with one element ($< x >$). What does it mean to generate a subgroup or a group with more than one element?

Example 2.4.1. D_{2n} = symmetries of a regular n-gon centered around the origin. Let r be a $360/n$ clockwise rotation of the n-gon about the origin. Let S be a reflection of the n-gon about the line from vertex 1 to the origin.



Notice: $1, r, r^2, r^3$ are all distinct. Now consider s, sr, sr^2, sr^3 (we read these right-to-left). sr^3 is the 270° rotation clockwise, then the reflection about the line where vertex 1 was to the origin.



Is $s \in \{1, r, r^2, r^3\}$? No, s fixes vertex 1 and the only element that fixes vertex 1 is the identity. But $s \neq 1$, so s is not a rotation. From here, we can deduce that

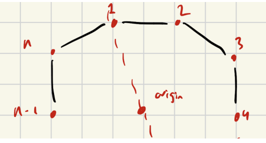
$$sr^j \not r^i$$

for any $0 \leq j \leq 3$ or $0 \leq i \leq 3$ (if it were true that $sr^j = r^i$ for some i and j, then $s = r^{i-j}$). Hence $D_{24} = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\} =< r, s > /$

In $D_{2n}, n \geq 3$, we want to show that

$$D_{2n} = \{e, r, r^2, r^3, ..., r^{n-1}, s, sr, sr^2, ..., sr^{n-1}\}$$

where s is a reflection over the line passing through vertex 1 and the origin.



1. Why are all $e, r, r^2, ..., r^{n-1}$ distinct?

$$\begin{aligned} r^i(1) &= i+1 \text{ for } 0 \leq i \leq n-1 \\ r^i(1) &= r^j(1) \\ \implies i+1 &= j+1 \\ \implies i &= j \end{aligned}$$

so the r^i's are distinct.

2. $s \neq r^i$ for any $i \in \{0, ..., n-1\}$. $s(1) = 1$ if $r^i(1) = 1$, we know from part 1 that $i = 0$. That is, $r^i = e$. But $s(2) = n \neq 2 = e(2) \implies s \neq e, s \neq r^i \ \forall 0 \leq i \leq n$

3. Let's show that $r^i \neq sr^j$ for any $i, j \in \{0, ..., n-1\} = A$. Suppose there exists $i, j \in A$ such that $r^i = sr^j$. We define r^{-1} as a counter-clockwise rotation; $r^-1 = r^{n-1}$. This gives

$$\begin{aligned} r^i &= sr^j \\ \implies r^{i-j} &= s \\ \implies r^{i+n-j} &= s \end{aligned}$$

where we adjust $(i + n - j) \mod n$ as needed. This contradicts $s \notin \{e, r, r^2, ..., r^{n-1}\}$. Hence $r^i \neq sr^j$ for any $i, j \in A$.

4. Show that $sr^i \neq sr^j$ for any $i \neq j$ in A. For the sake of contradiction, suppose there exists $i, j \in A$ such that $sr^i = sr^j$. Then

$$\begin{aligned} s^2r^i &= s^2r^j \\ \implies er^i &= er^j \\ \implies r^i &= r^j \end{aligned}$$

This contradicts $i \neq j$.

$$
\begin{aligned}
&D_{2n} = \left\{e, r, r^2, ..., r^{n-1}, s, sr, sr^2, ..., sr^{n-1}\right\} \\
&sr \neq rs
\end{aligned}
$$

$$
\begin{aligned}
(s \circ r)(1) &= s(r(1)) & \qquad (r \circ s)(1) &= r(s(1)) \\
&= s(2) & &= r(1) \\
&= n & &= 2
\end{aligned}
$$

But $sr = r^{-1}s$. If $sr(1) = r^{-1}s(1)$ and $sr(2) = r^{-1}s(2)$, then $sr = r^{-1}s$. It can be shown inductively that $sr^i = r^{-i}s \ \forall i \in \mathbb{Z}$.

Let $x \in G$ and $H \leq G$. If $x \in H$, then $< x > \leq H$. In some sense, $< x >$ is the smallest subgroup of G which contains x. "Smallest" refers to containment.

Proposition 2.4.1. If $\mathcal{A}$ is any collection of subgrops of a group G, then $\bigcap\limits_{H \in \mathcal{A}} H \leq G$.

Proof. HW

Definition 2.4.1. (Generating Sets)
If A is any subset of the group G, define

$$< A > = \bigcap_{H \leq G, A \subseteq H} H$$

This is called the subgroup of G generated by A. A is called the generating set.

Notice that in the notation of prop 2.4.1

$$\mathcal{A} = \{H \leq G : A \subseteq H\} \, (\text{nonempty as } G \in A \text{ since } G \leq G \text{ and } A \subseteq G)$$

We will show that $< A >$ is the unique minimal element of $\mathcal{A}$.

We know that $A \subseteq H \quad \forall H \in \mathcal{A}$. Thus $A \subseteq < A >$, so $< A > \in \mathcal{A}$. Let $K \in \mathcal{A}$. We know that

$$\bigcap_{H \in \mathcal{A}} H \leq K$$

That is, $< A > \leq K$. Hence, $< A >$ is minimal with respect to inclusion. When A is finite, that is

$$A = \{a_1, ..., a_n\} \text{ for } n \in \mathbb{N}$$

then we write

$$< A > = < a_1, a_2, ..., a_n >$$

This is a more concrete verion of the previous set $< A > = \bigcap\limits_{H \leq G, A \subseteq H} H$. Denote

$$\overline{A} = \{a_1^{\epsilon_1} a_2^{\epsilon_2} ... a_n^{\epsilon_n} : n \in \mathbb{N}, \epsilon_i = \pm 1, a_i \in A\}$$

In D_{2n}, $x \in < r, s >$ could look like

$$rssssssr^{-1}s^{-1}srrs^{-1}rr^{-1}s = r^2$$

Proposition 2.4.2. $< A > = \overline{A}$.