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
2.2 Centralizers and Normalizers, Stabilizers and Kernels 12
2.3 Cyclic Groups 15
2.4 Subgroups Generated by Subsets of a Group 20
2.5 Quotient Groups and Homomorphisms 22
2.6 Cosets and Lagrange's Theorem 26

3 Quotient Groups and Homomorphisms **30**
3.1 Isomorphism Theorems 30
3.2 The Alternating Group 33

4 Group Actions **35**
4.1 The Orbit-Stabilizer Theorem 35
4.2 Groups Acting on Themselves by Left Multiplication 39
4.3 Conjugates and the Class Equation 43
4.4 Conjugates of Permutations 46

Chapter 1

Preliminaries

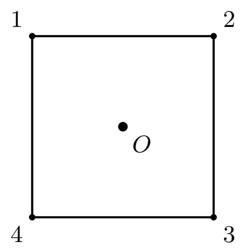
1.1 Groups, Permutations and Cycle Decompositions

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?

(1 2 3 4 5)   (5 4 3 2 1)

(1 2 3 5 4)   ~~(2 3 4 5 1)~~

$\vdots$

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 $r \le n$ 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 $e.a = a$) $\ \ \forall a \in A$ (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 $\Psi(g_1 g_2) = \Psi(g_1) \circ \Psi(g_2)$. 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.

$\square$

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

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

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, $C_G(A) \leq G$. $\square$

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 $g.a = gag^{-1} \ \ \forall g \in G, a \in A$ 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.

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

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

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

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,

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

   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 $|H| = \infty$.

$\square$

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 $x19nG$. 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 $\mathbb{Z}/15\mathbb{Z} =< \overline{1} >= \{k\dot{1} : k \in \mathbb{Z}\}$?

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

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 2.5.2 (2) says

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

and

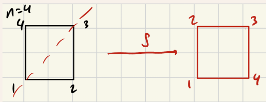
$$\left|x^{\gcd(m,n)}\right| = \frac{n}{\gcd(n, \gcd(m, n))}$$

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. $\square$

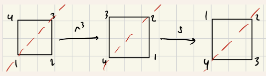
2.4 Subgroups Generated by Subsets of a Group

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

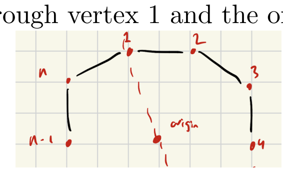
$$sr^j \neq r^i$$

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

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

This contradicts $i \neq j$.

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

$$(s \circ r)(1) = s(r(1)) = s(2) = n \qquad (r \circ s)(1) = r(s(1)) = r(1) = 2$$

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 $\bigcap_{H \in \mathcal{A}} H \leq G$.

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

2.5 Quotient Groups and Homomorphisms

Let G be a group and $N \leq G$. Define a relation on G by

$$a \sim b \iff a^{-1}b \in N$$

It is straightforward to verify that this is an equivalence relation on G. For $a \in G$, the equivalence class of a is

$$\begin{aligned}\{b \in G : a \sim b\} &= \left\{b \in G : a^{-1}b \in N\right\} \\ &= \left\{b \in G : a^{-1}b = n \text{ for } n \in N\right\} \\ &= \{b \in G : b = an \text{ for } n \in N\} \\ &= \{an : n \in \mathbb{N}\} \\ aN := \{an : n \in N\}\end{aligned}$$

Definition 2.5.1. (Coset)
For a subgroup N of G and $g \in G$, let

$$\begin{aligned}gN &= \{gn : n \in N\} \\ Ng &= \{ng : n \in N\}\end{aligned}$$

be called the left coset and right coset of N in G, respectively. Any element of a coset is called a representative of that coset. We will denote the set of all left cosets of N in G by G/N (read G modulo N or G mod N).

Proposition 2.5.1. Let $N \leq G$. G/N forms a partition of G. For all $a, b \in G$,

$$aN = bN \iff a \text{ and } b \text{ are representatives of the same coset.}$$

Proof. Since we have recognized left cosets as the equivalence classes induced by an equivalence relation, they form a partition. That is,

$$G = \bigcup_{g \in G} gN$$

$$\forall g_1, g_2 \in G \quad g_1N = g_2N \iff g_1N \cap g_2N \neq \emptyset$$

Suppose $a^{-1}b \in N$. Then $a^{-1}b = n$ for some $n \in N$. It follows that $b = an \in aN$ so $b \in aN$. Since N is a subgroup, $1 \in N$ hence $b \cdot 1 \in bN$. It follows that $aN \cap bN \neq \emptyset \implies aN = bN$.
Now assume $aN = bN$. Then $an = b$ for some $n \in N$. It follows that $n = ba^{-1} \in N$. Finally, we have

$$\begin{aligned}aN = bN &\iff a^{-1}b \in N \\ &\iff b \in aN \\ &\iff b \in aN \text{ and } a \in aN \\ &\iff a \text{ and } b \text{ are representatives of } aN (\text{or } bN)\end{aligned}$$

□

Proposition 2.5.2. Let $N \leq G$.

1. The operation on G/N described by $aN \cdot bN = (ab)N \quad \forall a, b \in G$ is well-defined if and only if $gng^{-1} \in N \quad \forall g \in G, n \in N$
2. If the operation above is well-defined, then G/N defines a group, where

$$\begin{gathered}1 \cdot N \text{ is the identity} \\ (gN)^{-1} = g^{-1}N \ \forall g \in G\end{gathered}$$

Proof. 1. ($\Longleftarrow$) Suppose $gng^{-1} \in N \ \forall g \in G, n \in N$. Let $a, a_1 \in aN$ and $b, b_1 \in bN$. We want to show that

$$abN = a_1b_1N$$

$a_1 = an$ and $b_1 = bm$ for some $n, m \in N$. Note that $a_1b_1 \in abN \iff a_1b_1N = abN$, so we will prove the former.

$$\begin{aligned} a_1b_1 = (an)(bm) &= a(bb^{-1})nbm \\ &= ab(b^{-1}nb)m \end{aligned}$$

by assumption, $b^{-1}n(b^{-1})^{-1} \in N$ so it follows that $a_1b_1 = abn_1m$ where $n_1 \in N$. Since N is a subgroup of G, $n_1m \in N$, call it n_2. Thus $a_1b_1 = abn_2$ where $n_2 \in N$. That is, $a_1b_1 \in abN$, proving our result ($a_1b_1N = abN$).
2. Suppose the operation is well-defined. We want to show G/N is a group.

Associativity: Let $aN < bN < cN \in G/N$ $(a, b, c \in G)$. Then

$$\begin{aligned} aN(bNcN) &= aN\left((bc)N\right) \\ &= a(bc)N \\ &= (ab)cN \\ &= \left((ab)N\right)cN \\ &= (aNbN)cN \end{aligned}$$

Identity, Closure, and Inverses: Let $aN \in G/N$ be given. Since B is a group, $1 \in G$ and thus

$$1N \in G/N$$

and

$$(aN)(1N) = (a1)N = aN$$

Also,

$$\left.\begin{array}{l} a \in G \\ G \text{ is a group} \end{array}\right\} \implies a^{-1} \in G \implies a^{-1}N \in G/N$$

and so

$$\begin{aligned} (aN)(a^{-1}N) &= (aa^{-1})N \\ &= 1N \\ &= (a^{-1}a)N \\ &= (a^{-1}N)(aN) \end{aligned}$$

□

G/N will be a group when N has that nice property, detailed in the following definition.

Definition 2.5.2. (Normal Subgroup)
A subgroup N of G is called normal in G if every element of g normalizes N. That is, N is normal in G if

$$gNg^{-1} = N \quad \forall g \in G$$

If N is a normal subgroup of G, then we write $N \trianglelefteq G$.

Theorem 2.5.1. (Characterizations of Normal Subgroups)
The $N \leq G$. The following are equivalent:

1. $N \trianglelefteq G$
2. $N_G(N) = G$
3. $gN = NG \quad \forall g \in G$
4. The operation "coset multiplication" is well-defined
5. $gNg^{-1} \subseteq N \quad \forall g \in G$

Example 2.5.1. Checking that a subgroup is normal is not practical using the definition. We would need to check that $gng^{-1} \in N \ \ \forall g \in G, n \in N$. If a subgroup is finitely generated, it suffices to check that the generators map back to the subgroup by conjugating.
Let $G = D_{16}$. Is $< s >$ normal in D_{16}? We need to examine gsg^{-1} for an arbitrary $g \in D_{16}$. Letting $g = s^i r^j$ where $i \in \{0, 1\}$ and $j \in \{0, ..., 7\}$. Then

$$\begin{aligned} gsg^{-1} &= (s^i r^j)s(s^i r^j)^{-1} \\ &= s^i r^j s r^{-j} s^{-i} \\ &= r^j s r^{-j} \text{ (when } i = 0) \\ &= r^j r^{-j} s \ (sr^{-j} = r^{-(-j)} s = r^j s) \\ &= r^{2j} s \end{aligned}$$

When $j = 1$, this gives that $gsg^{-1} = r^2 s \notin < s >$ since this would imply that r^2 is either the identity or s $(r^2 s = 1 \implies r^2 = s, \ r^2 s = s \implies r^2 = 1)$ which is a contradiciton.

Theorem 2.5.2. (Big Theorem)
A subgroup $N \leq G$ is normal in G if and only if it is the kernel of some homomorphism.

Proof. $(\impliedby)$ HW
$(\implies)$Suppose $N \trianglelefteq G$. Let's define

$$\begin{aligned} \pi : G \to G/N \\ \pi(g) = gN \ \ \forall g \in G \end{aligned}$$

Let $g_1, g_2 \in G$. Then

$$\begin{aligned} \pi(g_1 g_2) &= (g_1 g_2)N \\ &= (g_1 N)(g_2 N) \\ &= \pi(g_1)\pi(g_2) \end{aligned}$$

Hence, π is a homomorphism. It remains to show that $\ker \pi = N$. Note that

$$\begin{aligned} \ker \pi &= \{g \in G : \pi(g) = 1N\} \\ &= \{g \in G : gN = 1N\} \\ &= \{g \in G : g \in 1N\} \\ &= \{g \in G : g \in N\} \\ &= N \end{aligned}$$

completing the proof. □

Definition 2.5.3. (Natural Projection Homomorphism)
Let $N \trianglelefteq G$. The homomorphism

$$\begin{aligned} \pi : G \to G/N \\ \pi(g) = gN \end{aligned}$$

is called the natural projection (homomorphism) of G onto G/N.

If $\overline{H} \leq G/N$, the complete preimage of $\overline{H}$ is $\pi^{-1}(\overline{H})$.

Note . If $\overline{H} \leq G/N$, then

$$N \leq \pi^{-1}(\overline{H})$$

Since $1N \in \overline{H}$, we have $N = \ker \pi = \pi^{-1}(1N) \subseteq \pi^{-1}(\overline{H})$.

Q_8: we have that $< -1 >$ is a normal subgroup, so $Q_8 / < -1 >$ is a group consisting of $1 < -1 >, i < -1 >, j < -1 >, k < -1 >$

$$(i < -1 >)^2 = i^2 < -1 >= -1 < -1 >= 1 < -1 >$$

so, $Q_8/ < -1 > \cong V_4$.

$$\langle i < -1 > \rangle \cong Q_8 / < -1 >$$
$$\langle i < -1 > \rangle = \{ i < -1 >, 1 < -1 > \} = \overline{H}$$
$$\pi^{-1}(\overline{H}) = \left\{ g \in Q_8 : \pi(g) \in \overline{H} \right\}$$

$$\pi(1) = 1 < -1 > \in \overline{h}$$
$$\pi(i) = i < -1 > \in \overline{H}$$
$$\pi(-1) = -1 < -1 > = 1 < -1 > \in \overline{H}$$
$$\pi(-i) = -i < -1 > = i < -1 > \in \overline{H}$$

$$\pi^{-1}(\overline{H}) = \{1, i, -1, -i\}$$

2.6 Cosets and Lagrange's Theorem

There are a lot of ways to see if a subgroup is normal.

Some things to know about normal subgroups: Let G be a group.

1. $\{1\} \trianglelefteq G$ and $G \trianglelefteq G$ and $G/\{1\} \cong G, G/G \cong \{1\}$
2. When G is clearly an additive group we denote left and right cosets $g+N$ and $N+g$, respectively, where $N \leq G$ and
$$g + N = \{g + n : n \in N\}$$
$$N + g = \{n + g : n \in N\}$$
3. When G is abelian, every subgroup is normal

We move away from normal subgroups and just analyze subgroups.

Theorem 2.6.1. (Lagrange's Theorem)
If G is a finite group and $H \leq G$, then $|H| \mid |G|$ and the number of left cosets of H in H is $|G|/|H|$.

Proof. Here is a proof idea (problems 18, 19 from section 1.7): the left cosets form a partition of G
$$G = \bigcup_{g \in G} gH$$
There is a bijection from H to gH ($h \mapsto gh$) so $|H| = |gH|$. Then,
$$|G| = k|H|$$
where k is the number of distinct left cosets of H in G. Rearranging gives
$$k = \frac{|G|}{|H|}$$
□

Definition 2.6.1. (Index of a Subgroup)
If G is a group (possibly finite) and $H \leq G$, then the number of distinct left cosets of H in G is called the index of H in G, denoted $|G : H|$.

Corollary 2.6.1. If G is a finite group and $x \in G$, then $|x| \mid |G|$.

Proof. We proved that $|x| = |<x>|$ and $<x> \leq G$. The claim follows immediately from Lagrange's theorem. □

Example 2.6.1. For a finite group with $H \leq G$
$$|G : H| = |G|/|H|$$

Example 2.6.2. Consider $G = \mathbb{Z}$ and $H = 3\mathbb{Z}$.
$$|\mathbb{Z} : 3\mathbb{Z}| = 3 = |\mathbb{Z}/3\mathbb{Z}|$$
$$3\mathbb{Z} = \{3x : x \in \mathbb{Z}\}$$
$$1 + 3\mathbb{Z} = \{1 + 3x : x \in \mathbb{Z}\}$$
$$2 + 3\mathbb{Z} = \{2 + 3x : x \in \mathbb{Z}\}$$
$$3 + 3\mathbb{Z} = \{3 + 3x : x \in \mathbb{Z}\} = 0 + 3\mathbb{Z}$$

Corollary 2.6.2. If G is a group of prime order p, then G is cyclic.

Proof. Let $x \in G$ where $x \neq 1_G$. Then $|x| \mid |G|$. Since $|G| = p$, a prime, then $|x| \in \{1, p\}$. Since $x \neq 1_G$, $|x| \neq 1$. Thus $|x| = p$ and hence $< x >= G$. □

Example 2.6.3. A subgroup H of a group G with index 2 is normal ($|G : H| = 2$). Let $g \in G - H$. Then $gH \neq 1H$. Since $|G : H| = 2$, there are two distinct cosets of H in G and since one of them is $1H$, the other must be gH. Similary, there are only two distinct right cosets of H in G, namely $H1$ and Hg. Since $1H = H1$ and cosets form a partition of G, we have

$$gH = G - H = Hg$$

Hence th left and right cosets of H are the same and H is normal in G.

Example 2.6.4. A subgroup H is a normal subgroup of G is not a transitive statement. Let $G = D_8$. Then $|D_8| = 8$, $| < s > | = 2$, $| < s, r^2 > | = 4$. Clearly,

$$< s > \leq < s, r^2 > \leq D_8$$

We have

$$|D_8 :< s, r^2 > | = 2$$

and

$$| < s, r^2 >:< s > | = 2$$

so

$$< s > \trianglelefteq < s, r^2 > \trianglelefteq D_8$$

but $< s >$ is not normal in D_8 since $rsr^{-1} = r^2 s \notin < s >$.

Definition 2.6.2. (Product of Subgroups)
Let $H, K \leq G$. define

$$HK = \{hk : h \in H, k \in K\}$$

Theorem 2.6.2. (Order of Products of Subgroups)
If H and K are finite subgroups of a group, then

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$$

Note that HK need not be a group for this to hold.

Proof. Notice that HK is the union of left cosets of K. That is,

$$HK = \bigcup_{h \in H} hK$$

Since each coset of K has $|K|$ elements, we will count the number of distinct cosests in the above union. We know $h_1 K = h_2 K$ for $h_1, h_2 \in H$ if and only if $h_2^{-1} h_1 \in K$. It follows that

$$\begin{aligned} h_1 K = h_2 K &\iff h_2^{-1} h_1 \in K \cap H \\ &\iff h_1 (K \cap H) = h_2 (K \cap H) \end{aligned}$$

Thus the number of distinct cosets of the form $hK, h \in H$ is the same as the number of distinct cosets of $K \cap H$ in H. Since $H \cap K \leq H$, this is $|H|/|K \cap H|$. Therefore, HK consists of $|H|/|H \cap K|$ distinct cosets of K, each of which contains $|K|$ elements. It follows that

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$$

□

HK is not always a subgroup of G.

Example 2.6.5. Let $G = S_3$, $H =< (1\ 2) >$, and $K =< (2\ 3) >$. Then $H \cap K = \{1\}$ and

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|} = \frac{2 \cdot 2}{1} = 4$$

Lagrange says that if $HK \leq G$, then $4 \mid 3! = 6$, a contradiction.
We can further deduce

$$< (1\ 2), (2\ 3) >= S_3$$

since

$$4 \leq |< (1\ 2), (2\ 3) >| \leq 6$$

and $|< (1\ 2), (2\ 3) >|$ must also divide 6, so $< (1\ 2), (2\ 3) >$ generates all of S_3.

Proposition 2.6.1. If $H, K \leq G$, then $HK \leq G$ if and only if $HK = KH$. (Note: $HK = KH$ does NOT indicate the elements of H and K commute with each other, only that for $hk \in HK$ we have $hk = k_1h_1$ for some $k_1 \in K, h_1 \in H$.)

Proof. ($\Longrightarrow$) Assume $HK = KH$. Since H and J are nonemtpy, HK is nonempty. It remains to show that if $a, b \in HK$, then $ab^{-1} \in HK$. Let $a, b \in HK$. Then $a = h_1k_1$ and $b = h_2k_2$. Then

$$\begin{aligned} ab^{-1} &= (h_1k_1)(h_2k_2)^{-1} \\ &= h_1k_1k_2^{-1}h_2^{-1} \end{aligned}$$

Since $K \leq G$, we have

$$k_1k_2^{-1} = k_3 \in K$$

and since $H \leq G$ we have

$$h_2^{-1} = h_3 \in H$$

This gives

$$ab^{-1} = h_1k_3h_3$$

Since $HK = KH$, we know that $k_3h_3 \in HK$. That is,

$$k_3h_3 = h_4k_4 \text{ for some } h_4 \in H, k_4 \in K$$

so,

$$ab^{-1} = h_1h_4k_4$$

and letting $h_1h_4 = h_5 \in H$ we have

$$ab^{-1} = h_5k_4 \in HK$$

Thus $HK \leq G$.
($\Longleftarrow$) Conversely, suppose $HK \leq G$. Our goal is to show $HK = KH$. That is, we want to show $HK \subseteq KH$ and $KH \subseteq HK$. Since $K \leq HK$ and $H \leq HK$,

$$KH \subseteq HK \text{ by closure of } HK$$

To show $HK \subseteq KH$, let $hk \in HK$. Since HK is a subgroup, hk is the inverse to some $a \in HK$. That is

$$hk = a^{-1} = (hk)^{-1} = (h_ak_a)^{-1} = k_a^{-1}h_a^{-1} \in KH$$

It follows that $HK \subseteq KH$. Thus, $HK = KH$. □

Example 2.6.6. Let $G = D_8, H =< r >, K =< s >$. Notice $rs \in HK$ and $rs = sr^{-1} \in KH$. Also,

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|} = \frac{4 \cdot 2}{1} = 8$$

So, $HK = D_8 = KH$.

Corollary 2.6.3. If $H, K \leq G$ and $H \leq N_G(K)$, then $HK \leq G$. In particular, if $K \trianglelefteq G$, then $HK \leq G \ \ \forall H \leq G$.

Proof. We will prove $HK = KH$. Let $h \in H$ and $k \in K$. By assumption,

$$H \leq N_G(K) \implies hkh^{-1} \in K$$

Then

$$hk = hkh^{-1}h \in KH$$

Thus $HK \subseteq KH$. Similarly,

$$kh = hh^{-1}kh \in HK$$

It follows that $KH \subseteq KH$. Hence, $HK = KH$. □

Theorem 2.6.3. (Subgroup Index Theorem)
Let H, K be subgroups of a group G with $H \leq K \leq G$. Then

$$|G : H| = |G : K| \cdot |K : H|$$

Proof. Let g_i be a distinct representation for a left coset of H in G, $\forall i \in I$ where I is an indexing set. So

$$\{g_iH : i \in I\} = G/H = \{gH : g \in G\}$$

and $g_iH = Hg_j$ if and only if $g_i = g_j$. Let $\psi : I \times K/H \to G/H$ be defined by

$$\psi(i, kH) = g_ikH$$

We will show ψ is a well-defined bijection.

Well-defined: Suppose that $k_1H = k_2H$ for some $k_1, k_2 \in K$. That is, $k_1^{-1}k_2 \in H$. Then

$$\psi(i, k_1H) = g_ik_1H\psi(i, k_2H) \qquad = g_ik_2H$$

So,

$$\begin{aligned}(g_ik_1)^{-1}(g_ik_2) &= k_1^{-1}g_i^{-1}g_ik_2 \\ &= k_1^{-1}1_Gk_2 \\ &= k_1^{-1}k_2 \in H \text{ by assumption.}\end{aligned}$$

Hence, ψ is well-defined.

Bijection: Suppose $\psi(i, k_1H) = \psi(j, k_2H)$. Then

$$\begin{aligned}&g_ik_1H = g_jk_2H \\ \implies &(g_ik_1)^{-1}(g_jk_2) \in H \\ \implies &k_1^{-1}g_i^{-1}g_jk_2 = h \text{ for some } h \in H \qquad (*) \\ \implies &g_i^{-1}g_j = k_1hk_2^{-1} \text{ for some } h \in H \\ \implies &g_i^{-1}g_j \in K \text{ since } H \subseteq K \\ \implies &g_iK = g_jK \\ \implies &g_i = g_j \\ \implies &i = j\end{aligned}$$

Using this in $(*)$ gives

$$\begin{aligned}&k_1^{-1}g_i^{-1}g_ik_2 = h \text{ for some } h \in H \\ \implies &k_1^{-1}k_2 = h \in H \\ \implies &k_1H = k_2H\end{aligned}$$

Hence ψ is one-to-one.

Let $gH \in G/H$. Since the left cosets of K partition the group G we have that $g \in g_iK$. That is, $g = g_ik$ for some $k \in K$. Hence

$$\psi(i, kH) = g_ikH = gH$$

Thus, ψ is onto.

We have that ψ is a well-defined bijection. Hence,

$$I \times K/H \to G/H$$
$$|G : K| \cdot |K : H| = |G : H|$$

Chapter 3

Quotient Groups and Homomorphisms

3.1 Isomorphism Theorems

Theorem 3.1.1. (The First Isomorphism Theorem)
If $\phi : G \to H$ is a group homomorphism, then $\ker \phi \trianglelefteq G$ and

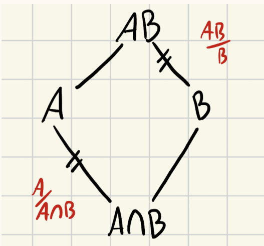
$$G/ker\phi \cong \phi(G) \leq H$$

Corollary 3.1.1. Let $\phi : G \to H$ be a group homomorphism.

1. ϕ is injective if and only if $\ker \phi = \{1\}$
2. $|G : \ker \phi| = |\phi(G)|$

Theorem 3.1.2. (The Second Isomorphism Theorem; The Diamond Theorem)
Let G be a group and let $A, B \leq G$. Assume $A \leq N_G(B)$. Then

$$\begin{aligned} AB &\leq G \\ B &\trianglelefteq AB \\ A \cap B &\trianglelefteq A \\ AB/B &\cong A/A \cap B \end{aligned}$$



Proof. Since $A \leq N_G(B), B \leq N_G(B)$, it follows that

$$AB \leq N_G(B)$$

and since $B \leq AB$, we have $B \trianglelefteq AB$.
Since $B \trianglelefteq AB$, then AB/B is a group. Define

$$\begin{aligned} \phi &: A \to AB/B \\ \phi(a) &= aB \quad \forall a \in A \end{aligned}$$

By the First Isomorphism Theorem, if ϕ is a homomorphism then

$$A/\ker \phi \cong \phi(A)$$

We need to show

1. ϕ is a homomorphism

2. $\phi(A) = AB/B$
3. $\ker\phi = A \cap B$

1. Let $a_1, a_2 \in A$. Then

$$\begin{aligned}\phi(a_1a_2) &= a_1a_2B \\ &= (a_1B)(a_2)B \\ &= \phi(a_1)\phi(a_2)\end{aligned}$$

2. Notice that $abB = aB$ since $b \in B$. That is, $\forall abB \in AB/B \;\; abB = aB$. Thus our mapping is surjective. Hence $\phi(A) = AB/B$.

3. Notice

$$\begin{aligned}\ker\phi &= \{a \in A : \phi(a) = 1B\} \\ &= \{a \in A : aB = 1B\} \\ &= \{a \in A : a \in B\} \\ &= A \cap B\end{aligned}$$

By the First Isomorphism Theorem on 1, 2, and 3, we have $A/\ker\phi \cong \phi(A)$. That is,

$$A/A \cap B \cong AB/B$$

where $A \cap B \trianglelefteq A$. □

Theorem 3.1.3. (The Third Isomorphism Theorem)
Let G be a group and let H and K be normal subgroups of G with $H \leq K$. Then

$$\frac{G/H}{K/H} \cong G/K$$

Proof. We proceed to define a homomorphism from $G/H \to G/K$ that is surjective such that $\ker\phi = K/H$. Then the claim follows fro the First Isomorphism Theorem.

Since $K \trianglelefteq G, \pi_H(G) = \{kH : k \in K\}$. We know that the

$$\pi_H(K) \trianglelefteq \pi_H(G) = G/H$$

Notice $\{kH : k \in K\} = K/H$. Define

$$\begin{aligned}\phi : G/H &\to G/K \\ gH &\mapsto gK \quad \forall g \in G\end{aligned}$$

We proceed to show ϕ is a well-defined, epimorphism (surjective homomorphism).

ϕ is well-defined: Suppose $g_1H = g_2H$. Then $g_1 = g_2h$ for some $h \in H$. Since $H \leq K$, $h \in K$. That is

$$\begin{aligned} & g_1 = g_2h \text{ where } h \in K \\ \Longrightarrow\ & g_1K = g_2K\end{aligned}$$

Hence $\phi(g_1H) = \phi(g_2H)$ and our function is well-defined.

ϕ is a homomorphism: Let $g_1H, g_2H \in G/H$. Then

$$\begin{aligned}\phi(g_1Hg_1H) &= \phi(g_1g_2H) \\ &= g_1g_2K \\ &= (g_1K)(g_2K) \\ &= \phi(g_1H)\phi(g_2H)\end{aligned}$$

Hence, ϕ is a homomorphism.

ϕ is surjective: ϕ is clearly surjective by construction.

$\ker \phi = K/H$**:**

$$\begin{aligned}\ker \phi &= \{gH \in G/H : \phi(gH) = 1K\} \\ &= \{gH \in G/H : gK = 1K\} \\ &= \{gH \in G/H : g \in K\} \\ &= K/H\end{aligned}$$

By the First Isomorphism Theorem,

$$\frac{G/H}{K/H} \cong G/K$$

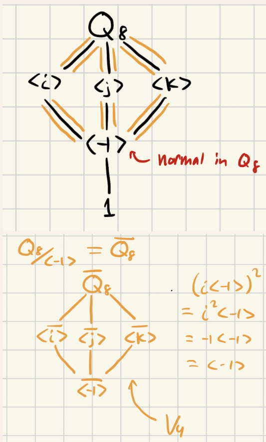
□

Theorem 3.1.4. (The Fourth Isomorphism Theorem; The Lattice Isomorphism Theorem)
Let G be a group with $N \trianglelefteq G$. Then there is a bijection from $\{A \leq G : N \leq A\}$ to the set of subgroups of G/N. In particular, every subgroup of $\overline{G} = G/N$ is of the form $\overline{A} = A/N$ for some subgroup A of G, containing N (Namely, the complete preimage of the subgroup of G/N, under the natural projection from G to G/N).

This bijection has the following properties:

1. $A \leq B \iff \overline{A} \leq \overline{B}$ $(A/N \leq B/N)$
2. If $A \leq B$ then $|A : B| = |B/N : A/N| = |\overline{B} : \overline{A}|$
3. $\overline{< A, B >} =< \overline{A}, \overline{B} >$
4. $\overline{A \cap B} = \overline{A} \cap \overline{B}$
5. $A \trianglelefteq G \iff \overline{A} \trianglelefteq \overline{G}$

Example 3.1.1. The group Q_8 :



3.2 The Alternating Group

The following are important theorems that we will come later. We do not prove these yet, but we will soon.

Theorem 3.2.1. (Cauchy's Theorem)
If G is a finite group and p is a prime dividing $|G|$, then G has an element of order p.

Theorem 3.2.2. (Sylow Theorem)
If G is a finite group of order $p^\alpha \cdot m$, where p is prime and $p \nmid m$, then G has a subgroup of order p^α.

Proposition 3.2.1.
If G is a finite abelian group and p is a prime dividing $|G|$, then G contains an element of order p.

Proof. We will use strong induction to prove this result. We will assume the result holds for all groups with order $< |G|$ and show this implies the result for G.

Since $|G| > 1$ there is an element $x \in G$ such that $x \neq 1_G$. If $|G| = p$, then we are done (by Lagrange's theorem, we know $< x >= G$ hence $|x| = p$). Suppose $|G| > p$, and suppose $p \mid |x|$ for some $x \in G$. Then

$$|x| = pn \text{ for some } n \in \mathbb{Z}$$

We know

$$|x^n| = \frac{|x|}{\gcd(|x|, n)} = \frac{|x|}{n} = \frac{pn}{n} = p$$

We now assume $p \nmid |x|$. Let $< x >= N$. Since G is abelian, $N \trianglelefteq G$ and by Lagrange's theorem,

$$|G : N| = |G/N| = |G|/|N|$$

and since $N \neq 1_G$, $|G|/|N| < |G|$. Since $p \nmid |N|$ we have that $p \mid |G/N|$. By our inductive assumption, we can conclude there exists $yN \in G/N$ such that $|yN| = p$. Since $yN \neq 1N$ we have that $y \notin N$. But $y^p \in N$ since

$$(yN)^p = y^p N$$

Since $< y^p >\leq N$ we have $< y >\neq< y^p >$. That is, $\langle y^p \rangle < \langle y \rangle$ and further $|y^p| < |y|$. We know

$$|y^p| = \frac{|y|}{\gcd(|y|, p)} = \frac{|y|}{p}$$

Thus $p \mid |y|$. By our first case, we are done.
This completes the induction and every abelian group with $p \mid |G|$ has one element of order p. □

Central to this proof was finding $N \trianglelefteq G$. What if we can't?

Definition 3.2.1. (Simple Group)
A (finite or infinite) group G is called simple if $|G| > 1$ and the only normal subgroups of G are 1 and G.

Example 3.2.1. $\mathbb{Z}_p$ where p is prime is the most important simple group (for us) ((to be proved later)).

We shift our attention back to permutations. Consider $\sigma \in S_3$.

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

Notice that in general for any m-cycle in S_n we have

$$(a_1\ a_2\ a_3\ \dots\ a_m) = (a_1\ a_m)(a_1\ a_{m-1})\dots(a_1\ a_3)(a_1\ a_2)$$

That is, every m-cycle in S_n cna be written as a product of 2-cycles (transpositions) since efery permutation in S_n can be written as a product of disjoint cycles. Hence, every permutation in S_n can be written as a product of transpositions. That is,

$$\langle T \rangle = S_n \text{ where } T = \{(i\ j) : 1 \leq i < j \leq n\}$$

Example 3.2.2. S_4, T has the elements

$$(1\ 2), (1\ 3), (1\ 4), (2\ 3), (2\ 4), (3\ 4)$$

Definition 3.2.2. (Even Permutation)
A permutation $\alpha \in S_n$ is called even if it can be written as a product of an even number of transpositions. Otherwise, α is called odd.

Remark 3.2.1. $(1\ 2\ 3) = (1\ 3)(1\ 2)$, so $(1\ 2\ 3)$ is even. However, $(1\ 2\ 3) = (1\ 3)(1\ 2)(1\ 3)(1\ 2)$. Is this a well-defined definition? Can a permutation be both even and odd? **NO:** Permutations in S_n are either even or odd but not both.

Definition 3.2.3. (The ε Homomorphism)
For each $\sigma \in S_n$, define

$$\varepsilon(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is even} \\ -1 & \text{if } \sigma \text{ is odd} \end{cases}$$

ε defines a mapping from S_n to the multiplicative group $G = \{-1, 1\}$.

Let $\sigma, \tau \in S_n$. Assume σ, τ are both even or both odd. Then $\sigma\tau$ is an even permutation, so

$$\varepsilon(\sigma\tau) = -1 \text{ and } \varepsilon(\sigma) \cdot \varepsilon(\tau) = 1$$

If one of σ, τ is odd and the other is even, then $\sigma\tau$ is odd and

$$\varepsilon(\sigma\tau) = -1 \text{ and } \varepsilon(\sigma) \cdot \epsilon(\tau) = -1$$

so ε is a homomorphism. By the First Isomorphism theorem, we have

$$\frac{S_n}{\ker \varepsilon} \cong \varepsilon(S_n) = \{-1, 1\}$$

By Lagrange's Theorem,

$$\begin{aligned} \frac{|S_n|}{|\ker \varepsilon|} &= |\{-1, 1\}| = 2 \\ \implies \frac{n!}{|\ker \varepsilon|} &= 2 \\ \implies |\ker \varepsilon| &= \frac{n!}{2} \end{aligned}$$

Notice that

$$\ker \varepsilon = \{\sigma \in S_n : \varepsilon(\sigma) = 1\} = \{\sigma \in S_n : \sigma \text{ is even}\}$$

Definition 3.2.4. (The Alternating Group)
The alternating group of degree n, denoted by A_n, is the kernel of the Homomorphism ε. It is more commonly referred to as the set of all even permutations in S_n.

Chapter 4

Group Actions

4.1 The Orbit-Stabilizer Theorem

Definition 4.1.1. (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)

Recall that for each $g \in G$, there is a mapping $\sigma_g : A \to A$ such that $g \mapsto g.a$ which is an element in S_A (a permutation of A).
We define

$$\varphi : G \to S_A \text{ by } \varphi(g) = \sigma_g$$

We proved this is a Homomorphism. We called it the permutation representation of G in A.

Important Things:

1. The kernel of the action is
$$\ker \varphi = \{g \in G : g.a = a \ \ \forall a \in A\}$$
2. The stabilizer of $a \in A$ in G is
$$G_a = \{g \in G : g.a = a\}$$
3. An action is called faithful if its kernel is 1_G

Example 4.1.1. We know that S_n acts on $A = \{1, 2, ..., n\}$ by

$$\sigma.i = \sigma(i) \ \ \forall \sigma \in S_n, i \in A$$

$$\begin{aligned}\{\sigma \in S_n : \sigma.i = i \ \forall i \in A\} &= \{\sigma \in S_n : \sigma(i) = i \ \forall i \in A\} \\ &= \{1_{S_n}\}\end{aligned}$$

This action is faithful.
Consider the stabilizer

$$G_i = \{\sigma \in S_n : \sigma(i) = i\}$$

Recall that $|G_i| = (n-1)!$
In general, we can say

$$\ker \varphi = \bigcap_{a \in A} G_a$$

Given a homomorphism $\Psi : G \to S_A$ where A is a nonempty set and G is a group, the mapping defined by

$$g.a = (\Psi(g))(a)$$

is a group action.

Let $g_1, g_2 \in G$ and $a \in A$. Then

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

and

$$\begin{aligned}1_G.a &= (\Psi(1_G))(a) \\ &= 1_{S_A}(a) \\ &= a\end{aligned}$$

Proposition 4.1.1.
Let G be a group acting on $A \neq \emptyset$. The relation on A defined by

$$a \sim b \iff a = g.b \text{ for some } g \in G$$

is an equivalence relation.

Definition 4.1.2. (Orbit of a Group Action)
Let G act on A.

1. The equivalence class $\{g.a : g \in G\}$ (where $a \in A$) is called the orbit of G containing a, denoted $\mathcal{O}_a$.
2. The action of G on A is called transitive if there is only one orbit. That is, given $a, b \in A$,

$$\exists g \in G \text{ such that } a = g.b$$

Example 4.1.2. Let $G = S_n$ act on $A = \{1, 2, ..., n\}$ in the usual way.

$$\begin{aligned}\mathcal{O}_2 &= \{g.2 : g \in S_n\} \\ &= \{\sigma.2 : \sigma \in S_n\} \\ &= \{\sigma(2) : \sigma \in S_n\} \\ &= \{1, 2, 3, ..., n\} = A\end{aligned}$$

Hence, this action is transitive.

Theorem 4.1.1. (Orbit-Stabilizer Theorem)
For each $a \in A$ the number of elements in the equivalence class $\mathcal{O}_a = \{g.a : g \in G\}$ is $|G : G_a|$ (the number of left cosets of G_a in G).

Proof. To prove the last statement, let $\mathcal{O}_a$ be the orbits of G containing a. Let $b \in \mathcal{O}_a$. Then $b = g.a$ for some $g \in G$. Notice that gG_a is a left coset of G_a in G. Define

$$\begin{aligned}f : \mathcal{O}_a &\to G/G_a \\ b = g.a &\mapsto gG_a\end{aligned}$$

Then f is a bijection:

Onto: Let $gG_a \in G/G_a$. Then $g.a \in \mathcal{O}_a$ and $f(g.a) = gG_a$ so f is onto.

1-1 and well-defined: Notice

$$\begin{aligned} f(g.a) = f(h.a) &\iff gG_a = hG_a \\ &\iff h^{-1}g \in G_a \\ &\iff (h^{-1}g).a = a \\ &\iff h.\left((h^{-1}g).a\right) = h.a \\ &\iff \left(hh^{-1}g\right).a = h.a \\ &\iff g.a = h.a \end{aligned}$$

Hence f is $1-1$ and well-defined.

So, f is a bijection from $\mathcal{O}_a$ to G/G_a. Thus $\mid \mathcal{O}_a \mid = \mid G/G_a \mid$. Hence, $\mid \mathcal{O}_a \mid = \mid G : G_a \mid$. □

Example 4.1.3. We know S_n acts on $A = \{1, ..., n\}$ in the usual way. Given $i \in A$, we have $\mathcal{O}_i = \{\sigma(i) : \sigma \in S_n\}$. By the orbit-stabilizer theorem,

$$\begin{aligned} \mid \mathcal{O}_i \mid &= \mid S_n : G_i \mid \\ \implies n &= \frac{\mid S_n \mid}{\mid G_i \mid} = \frac{n!}{\mid G_i \mid} \\ \implies \mid G_i \mid &= \frac{n!}{n} = (n-1)! \end{aligned}$$

Let $\sigma \in S_7$.

$$\begin{aligned} \sigma(1) &= 2 \\ \sigma(2) &= 3 \\ \sigma(3) &= 4 \\ \sigma(4) &= 5 \\ \sigma(5) &= 6 \\ \sigma(6) &= 1 \end{aligned}$$

Let $G = \langle \sigma \rangle \leq S_7$. By the definition of group action if a group acts on a set A then any subgroup of the group acts on A ($g.a$ is a mapping from $G \times A$ to A) so

$$g.a \in A \quad \forall g \in G, a \in A$$

so certainly we have an action when we restrict g to a subgroup. Let $\langle \sigma \rangle$ act on $A = \{1, 2, ..., 7\}$ in the usual way.

Determine the Orbits:

$$\begin{aligned} \mathcal{O}_1 &= \{\tau(1) : \tau \in \langle \sigma \rangle\} \\ &= \left\{\sigma^k(1) : k \in \{0, 1, 2, 3\}\right\} \\ &= \left\{1, \sigma(1), \sigma^2(1), \sigma^3(1)\right\} \\ &= \{1, 2, 3, 4\} \\ \mathcal{O}_5 &= \left\{5, \sigma(5), \sigma^2(5), \sigma^3(5)\right\} \\ &= \{5, 6\} \\ &= \mathcal{O}_6 \\ \mathcal{O}_7 &= \{7\} \\ \sigma &= (1\ 2\ 3\ 4)(5\ 6) \end{aligned}$$

Proposition 4.1.2. Every $\sigma \in S_n$ can be written as a product of disjoint cycles.

Proof. Let $\sigma \in S_n$ and $A = \{1, 2, ..., n\}$. Also, let $G = \langle \sigma \rangle$. Then G acts on A in the usual way. Then, by the orbit-stabilizer theorem, this action partitions A into a unique set of disjoint orbits. Let

$$\mathcal{O}_x = \left\{\sigma^k(x) : k \in \mathbb{Z}\right\}$$

be one such orbit where $x \in A$.
Again, by the orbit-stabilizer theorem applied to $\mathcal{O}_x$ there is a bijection between $\mathcal{O}_x$ and $G/G_x = \langle\sigma\rangle / G_x$ defined by $\sigma^k(x) \mapsto \sigma^k G_x$. Since G is cyclic, G is abelian and so $G_x \trianglelefteq G$. Hence, G/G_x is cyclic of order d where d is the smallest integer such that $\sigma^d \in G_x$. Also,

$$d =\mid G : G_x \mid=\mid \mathcal{O}_x \mid$$

Thus, the different cosets of G_x in $G = \langle\sigma\rangle$ are

$$1G_x, \sigma G_x, \sigma^2 G_x, ..., \sigma^{d-1} G_x$$

and the corresponding elements of $\mathcal{O}_x$ are

$$x, \sigma(x), \sigma^2(x), ..., \sigma^{d-1}(x)$$

Thus σ cycles the elements of $\mathcal{O}_x$. That is, the elements are a cycle of size d (σ creates a d-cycle). Since the orbits form a partition of A each orbit gives a disjoint cycle in our decomposition of σ. $\square$

4.2 Groups Acting on Themselves by Left Multiplication

Let G be a group and let $A = G$. Define

$$\begin{aligned}(\ . \ ) &: G \times A \to G \\ g.a &= ga \quad \forall g \in G, a \in G\end{aligned}$$

Let Ψ be the permutation representation of this action:

$$\begin{aligned}\Psi &: G \to S_A \\ \Psi(g) &= \sigma_g \in S_A\end{aligned}$$

Let $G = V_4 = \{1, a, b, c\}$ where $a^2 = b^2 = c^2 = 1$. Let's see the permutation representation in action when G acts on itself by left multiplication. Look at the mapping $\sigma_1(x)$:

$$\left.\begin{aligned}\sigma_1(1) &= 1 \cdot 1 = 1 \\ \sigma_1(a) &= 1 \cdot a = a \\ \sigma_1(b) &= 1 \cdot b = b \\ \sigma_1(c) &= 1 \cdot c = c\end{aligned}\right\} \implies \sigma_1 = 1_{S_4}$$

Look at the mapping $\sigma_a(x)$:

$$\left.\begin{aligned}\sigma_a(1) &= a \cdot 1 = a \\ \sigma_a(a) &= a \cdot a = 1 \\ \sigma_a(b) &= a \cdot b = c \\ \sigma_a(c) &= a \cdot c = b\end{aligned}\right\} \implies \sigma_a = (1 \ a)(b \ c)$$

Look at the mapping $\sigma_b(x)$:

$$\left.\begin{aligned}\sigma_b(1) &= b \cdot 1 = b \\ \sigma_b(a) &= b \cdot a = c \\ \sigma_b(b) &= b \cdot b = 1 \\ \sigma_b(c) &= b \cdot c = a\end{aligned}\right\} \implies \sigma_b = (1 \ b)(a \ c)$$

Look at the mapping $\sigma_c(x)$:

$$\left.\begin{aligned}\sigma_c(1) &= c \cdot 1 = c \\ \sigma_c(a) &= c \cdot a = b \\ \sigma_c(b) &= c \cdot b = a \\ \sigma_c(c) &= c \cdot c = 1\end{aligned}\right\} \implies \sigma_c = (1 \ c)(a \ b)$$

We know $\Psi : V_4 \to S_4$ by the first isomorphism theorem

$$\frac{V_4}{\ker \Psi} \cong \Psi(V_4) = \{1_{s_4}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

and

$$\begin{aligned}\ker \Psi &= \{g \in G : g.a = a \quad \forall a \in A\} \\ &= \{1_{V_4}\} \\ V_4 &\cong \Psi(V_4) \ (V_4 \text{ is isomorphic to a subgroup of } S_4)\end{aligned}$$

Let G be a group. Let $H \leq G$. Let $A = G/H$ and define the action of G on A by

$$g.aH = gaH \quad \forall g \in G, aH \in A$$

(note: if $H = \{1\}$, then $g.aH = gaH = ga\{1\} = \{ga\}$)

Example 4.2.1. $G = D_8$ and $H = \langle s \rangle = \{1, s\}$.

$$\mid D : H \mid = 4$$

so the cosets of H are

$$\overset{1}{1H}, \overset{2}{rH}, \overset{3}{r^2H}, \overset{4}{r^3H}$$

Let's find the permutation representation of this action, specifically σ_s and σ_r.

σ_s:

$$\begin{aligned} s.1H &= sH = 1H & \sigma_s(1) &= 1 \\ s.rH &= srH = r^{-1}sH = r^{-1}H = r^3H & \sigma_s(2) &= 4 \\ s.r^2H &= sr^2H = r^{-1}srH = r^{-1}r^{-1}sH = r^2H & \sigma_s(3) &= 3 \\ s.r^3H &= sr^3H = r^{-3}H = rH & \sigma_s(4) &= 2 \end{aligned}$$

σ_r:

$$\begin{aligned} r.1H &= rH = rH & \sigma_r(1) &= 2 \\ r.rH &= rrH = r^2H & \sigma_r(2) &= 3 \\ r.r^2H &= r^3H & \sigma_r(3) &= 4 \\ r.r^3H &= r^4H = 1H & \sigma_r(4) &= 1 \end{aligned}$$

So

$$\sigma_s = (2\ 4) \qquad \sigma_r = (2\ 3\ 4\ 1)$$

G acting on itself by left multiplication is a special case of G acting on the cosets of $H \leq G$ by left multiplication. That is,

$$g.aH = (ga)H \quad \forall g \in G, \forall aH \in G/H$$

We will prove some things about the permutation representations of G acting on the cosets of a subgroup H.

$$\begin{aligned} &\Psi : G \to S_{G/H} \\ &\Psi(G) = \sigma_g \end{aligned}$$

where

$$\sigma_g(xH) = g.xH = (gx)H$$

Theorem 4.2.1. (Associated Permutation Representation Afforded by Left Cosets)
Let G be a group and $H \leq G$. Let G act on $A = G/H$ by left multiplication. Let $\pi_H : G \to S_{G/H}$ be the permutation representation afforded by this action. Then

1. G acts transitively on A (for any $aH, bH \in A$ $\exists g \in G$ such that $bH = g.aH$)
2. $G_{1H} = H$
3. The kernel of the action is
$$\ker \pi_H = \bigcap_{x \in G} xHx^{-1}$$
and $\ker \pi_H$ is the largest normal subgroup of G contained in H.

Proof.

1. Let $aH, bH \in A$. Let $g = ba^{-1}$. Then
$$g.aH = (ba^{-1}a)H = bH$$
2. $G_{1H} = \{g \in G : g.1H = 1H\} = \{g \in G : (g1)H = H\} = \{g \in G : gH = H\} = \{g \in G : g \in H\} = H$

3. By definition,

$$\begin{aligned}\ker \pi_H &= \{g \in G : \pi_H(g) = 1_{S_A}\} \\ &= \{g \in G : g.xH = xH \ \forall xH \in A\} \\ &= \{g \in G : (gx)H = xH \ \forall x \in G\} \\ &= \left\{g \in G : x^{-1}gx \in H \ \forall x \in G\right\} \\ &= \left\{g \in G : g \in xHx^{-1} \ \forall x \in G\right\} \\ &= \bigcap_{x \in G} xHx^{-1}\end{aligned}$$

Observe $\ker \pi_H \trianglelefteq G$ and $\ker \pi_H \leq H$. Let $N \trianglelefteq G$ such that $N \leq H$. Then

$$N = xNx^{-1} \leq xHx^{-1} \quad \forall x \in G$$

Thus

$$N \leq \bigcap_{x \in G} xHx^{-1} = \leq \pi_H$$

□

Theorem 4.2.2. (Cayley's Theorem)
Every group is isomorphic to a subgroup of some symmetric group. If $|G| = n < \infty$, then G is isomorphic to a subgroup of S_n.

Proof. Let $H = \{1\}$. By the first isomorphism theorem, we have that

$$\frac{G}{\ker \pi_H} \cong \pi_H(G) \leq S_G$$

Since $\ker \pi_H \leq H$, we have

$$\ker \pi_H \leq \{1\} \implies \ker \pi_H = 1$$

Hence

$$\frac{G}{\ker \pi_h} \cong G$$

so

$$G \cong \frac{G}{\ker \pi_H} \cong \pi_H(G) \leq S_G$$

□

Termionology: The permutation representation of this action when $H = \{1\}$ is called the left regular representation of G.

Corollary 4.2.1. If G is a finite group of order $n \in \mathbb{N}$ and p is the smallest prime dividing n, then any subgroup of index p is normal in G.

Proof. Let π_H be the permutation representation afforded by G acting on the left cosets of H by left multiplication. Let $K = \ker \pi_H$ and $\mid H : K \mid= k$. Notice that $k \mid |H|$ and so $k \mid |G|$. Then

$$\mid G : K \mid = \mid G : H \mid \cdot \mid H : K \mid = pk$$

Since H has p cosets in G

$$\pi_H : G \to S_p$$

and by the first isomorphism theorem

$$\begin{aligned}&\frac{G}{K} \cong \pi_H(G) \leq S_p \\ \implies\ & pK = \mid G : K \mid = \frac{|G|}{|K|} = |\pi_H(G)|\end{aligned}$$

and so

$$\begin{aligned}pk \mid |S_p| &\implies pk|p! \\ &\implies k \mid (p-1)!\end{aligned}$$

However, since $k \mid |G|$ any prime factors of k would be larger than p, so $k = 1$ by the minimality of p. Thus

$$\begin{aligned} \mid H : K \mid = 1 &\implies H = K \\ &\implies H = \ker \pi_H \trianglelefteq G \end{aligned}$$

$\square$

Example 4.2.2. Give a group G of order 15, by Cauchy's theorem G contains a subgroup of order 5, and by the previous corollary we know that subgroup is normal since its index must be 3 which is the smallest prime dividing 15.

4.3 Conjugates and the Class Equation

Let G be a group acting on itself by conjugation:

$$g.a = gag^{-1} \quad \forall g \in G, \forall a \in G$$

We proved this is a group action.

Definition 4.3.1. (Conjugates and Conjugacy Classes)
We say $a, b \in G$ are conjugate in G if

$$\exists g \in G \text{ such that } b = gag^{-1}$$

That is, a and b are conjugate in G if and only if $a, b \in \mathcal{O}_x$ for some $x \in G$.

$$\begin{aligned} \mathcal{O}_x &= \{g.x : g \in G\} \\ &= \left\{gxg^{-1} : g \in G\right\} \end{aligned}$$

The orbits of G acting on itself by conjugation are called the conjugacy classes of G

Example 4.3.1. If G is abelian, then G acting on itself by conjugation is the trivial action. That is,

$$g.a = gag^{-1} = a \quad \forall a \in G, g \in G$$

So, the conjugacy class of a in G is

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

More generally, for G acting on itself, where G is not assumed to be abelian, the conjugacy class of $g \in G$ is $\{g\}$ if and only if $g \in Z(G)$.

Example 4.3.2. If $|G| > 1$, then G does not act transitively on itself by conjugation. The conjugacy class of 1_G is $\{1_g\}$. I.e., if G acts transitively on itself by conjugation, then there is only one orbit.

$$\left\{g1g^{-1} : g \in G\right\} = \{1 : g \in G\} = \{1\}$$

We also know that the action of conjugation can be generalized to G acting on $\mathcal{P}(G)$ by

$$g.S = gSg^{-1} \forall g \in G, S \in \mathcal{P}(G)$$

Definition 4.3.2. (Conjugate Sets)
Two subsets S and T of G are called conjugates if there exists $g \in G$ such that

$$S = gTg^{-1}$$

Proposition 4.3.1. The number of conjugates of a subset S in a group G is $|G : N_G(S)|$. In particular, the number of conugates of an element $s \in G$ is $|G : C_G(s)|$.

Proof. Using the orbit-stabilizer theorem, we know the conjugacy class of S equals $|G : G_s|$. For this particular action,

$$\begin{aligned} G_s &= \{g \in G : g.S = S\} \\ &= \left\{g \in G : gSg^{-1} = S\right\} \\ &= N_G(S) \end{aligned}$$

The second statemnt follos from

$$\begin{aligned} N_G(\{s\}) &= \left\{g \in G : g\{s\}g^{-1} = \{s\}\right\} \\ &= \left\{g \in G : gsg^{-1} = s\right\} \\ &= C_G(s) \end{aligned}$$

□

Proposition 4.3.2. $z \in G$ has conjugacy class $\{z\}$ if and only if $z \in Z(G)$.

Proof. ($\implies$) Suppose $z \in G$ has conjugacy class $\{z\}$. Then

$$z = \{gzg^{-1} : g \in G\}$$

Thus for every $g \in G$, we have $gzg^{-1} = z$. Equivalently, $gz = zg$ for all $g \in G$. Hence, $z \in Z(G)$.
($\impliedby$) Suppose $z \in Z(G)$. Then

$$\forall g \in G \quad zgz^{-1} = g \implies z = gzg^{-1}$$

Thus, the conjugacy class of z is

$$\{gzg^{-1} : g \in G\} = \{z : g \in G\} = \{z\}$$

□

Theorem 4.3.1. (The Class Equation)
Let G be a finite group and let $g_1, g_2, ..., g_r$ be representatives of distinct conjugacy classes of G not contained in $Z(G)$. Then

$$|G| = |Z(G)| + \sum_{i=1}^{r} |G : C_G(g_i)|$$

Proof. By proposition 4.3.2, $z \in Z(G)$ if and only if the conjugacy class of z is $\{z\}$. Let $Z(G) = \{z_1 = 1, z_2, z_3, ..., z_m\}$. Let $K_1, K_2, ..., K_r$ be the conjugacy classes of G not contained in the center and let g_i be a representative of K_i for each i. Then the full set of conjugacy classes is

$$\{\{1\}, \{z_2\}, \{z_3\}, ..., \{z_m\}, K_1, K_2, ..., K_r\}$$

Since this partitions G, we have

$$\begin{aligned} |G| &= = \sum_{i=1}^{m} |\{z_i\}| + \sum_{i=1}^{r} |K_i| \\ &= |Z(G)| + \sum_{i=1}^{r} |K_i| \end{aligned}$$

By proposition 4.3.1, we have $|K_i| = |G : C_G(g_i)|$ for each i. Thus,

$$|G| = |Z(G)| + \sum_{i=1}^{r} |G : C_G(g_i)|$$

□

Example 4.3.3.

1. If G is abelian of order n, then the class equation telss us nothing.

$$|G| = |Z(G)|$$

2. The class equation of Q_8:
   In any group, $\langle x \rangle \leq C_G(x)$. We know that $|\langle i \rangle| = 4$. Thus $|Q_8 : \langle i \rangle| = 2$. Also, we know that $i \notin Z(Q_8)$, so $C_{Q_8}(i) < Q_8$. Thus

$$2 = |Q_8 : \langle i \rangle| = |Q_8 : C_{Q_8}(i)| \cdot |C_{Q_8}(i) : \langle i \rangle|$$

   If $|Q_8 : C_{Q_8}(i)| = 1$, then $Q_8 = C_{Q_8}(i)$, a contradiction. So $|Q_8 : C_{Q_8}(i)| = 1$ and $|Q_8 : C_{Q_8}(i)| = 2$. Thus

$$C_{Q_8}(i) = \langle i \rangle$$

   This implies the conjugacy class of i contains 2 elements: i and $-i$. We could similarly finad all the conjugacy classes of Q_8:

$$\{1\}, \{-1\}, \{\pm i\}, \{\pm j\}, \{\pm k\}$$

   The class equation of Q_8 is therefore

$$8 = 2 + 2 + 2 + 2$$

Theorem 4.3.2. (Centers of p-Groups)
If p is a prime and P is a group of order p^α with $\alpha \geq 1$, then P has a nontrivial center $|Z(P)| > 1$.

Proof. By the class equation,

$$|P| = |Z(P)| + \sum_{i=1}^{r} |P : C_P(g_i)|$$

where $g_1, g_2, ..., g_r$ are representatives of the distinct noncentral conjugacy classes. By defintion, $C_P(g_i) \neq P$ (since $C_P(g_i) = P \iff g_i \in Z(P)$) for $i = 1, ..., r$ so p divides

$$|P : C_P(g_i)| = \frac{|P|}{|C_P(g_i)|} = \frac{p^\alpha}{|C_P(g_i)|} = p^\beta$$

Since p also divides $|P|$, if follows that p divides $|P| - \sum_{i=1}^{r} |P : C_P(g_i)|$. Equivalently, $p \mid |Z(P)|$. It follows that the center is nontrivial. □

Corollary 4.3.1. If $|P| = p^2$ for some prime p, then P is abelian. More precisely, P is isomorphic to either $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \times \mathbb{Z}_p$.

Proof. By theorem 4.3.2, $Z(P) \neq 1$. More specifically, by Lagrange's theorem,

$$|Z(P)| \in \left\{p, p^2\right\} \implies |P/Z(P)| \in \{1, p\}$$

In either case, P is cyclic and so P is abelian. If P has an element of order p^2, P is cyclic and isomorphic to $\mathbb{Z}_{p^2}$. If P is cyclic and contains no elements of order p^2, then every nonidentity element of P has order p. Let $x \in P$ such that $|x| \neq 1$ and let $y \in P \backslash \langle x \rangle$ (then $y \neq 1$ since $1 \in \langle x \rangle$). Notice x and y both have order p. Since $|\langle x, y \rangle| > |\langle x \rangle| = p$, we have $|\langle x, y \rangle| = p^2$. That is, P is abelian. Also, since $|x| = |y| = p$,

$$\langle x \rangle \times \langle y \rangle = \mathbb{Z}_p \times \mathbb{Z}_p$$

Defining a map

$$\begin{aligned} \mathbb{Z}_p \times \mathbb{Z}_p &\to P \\ \left(x^a, y^b\right) &\mapsto x^a y^b \end{aligned}$$

gives an isomorphism. Hence,

$$\mathbb{Z}_p \times \mathbb{Z}_p \cong P$$

□

4.4 Conjugates of Permutations

Let $\sigma = (1\ 2\ 3) \in S_5$ and $\tau = (3\ 5) \in S_5$. Then

$$\begin{aligned}\tau\sigma\tau^{-1} &= (3\ 5)(1\ 2\ 3)(3\ 5)^{-1}\\ &= (3\ 5)(1\ 2\ 3)(5\ 3)\\ &= (1\ 2\ 5)\\ &= (\tau(1)\ \tau(2)\ \tau(3))\end{aligned}$$

Now let $\tau = (2\ 3) \in S_5$. Then

$$\begin{aligned}\tau\sigma\tau^{-1} &= (2\ 3)(1\ 2\ 3)(2\ 3)^{-1}\\ &= (2\ 3)(1\ 2\ 3)(3\ 2)\\ &= (1\ 3\ 2)\\ &= (\tau(1)\ \tau(2)\ \tau(3))\end{aligned}$$

Now let $\tau = (1\ 4\ 3\ 2) \in S_5$. Then

$$\begin{aligned}\tau\sigma\tau^{-1} &= (1\ 4\ 3\ 2)(1\ 2\ 3)(1\ 4\ 3\ 2)^{-1}\\ &= (1\ 4\ 3\ 2)(1\ 2\ 3)(2\ 3\ 4\ 1)\\ &= (4\ 1\ 2)\\ &= (\tau(1)\ \tau(2)\ \tau(3))\end{aligned}$$

Now let $\tau = (5\ 4\ 1\ 2) \in S_5$. Then

$$\begin{aligned}\tau\sigma\tau^{-1} &= (5\ 4\ 1\ 2)(1\ 2\ 3)(5\ 4\ 1\ 2)^{-1}\\ &= (5\ 4\ 1\ 2)(1\ 2\ 3)(2\ 1\ 4\ 5)\\ &= (2\ 5\ 3)\\ &= (\tau(1)\ \tau(2)\ \tau(3))\end{aligned}$$

Now let $\sigma = (1\ 2\ 3\ 4) \in S_5$ and $\tau = (1\ 3\ 5)$. Then

$$\begin{aligned}\tau\sigma\tau^{-1} &= (1\ 3\ 5)(1\ 2\ 3\ 4)(1\ 3\ 5)^{-1}\\ &= (1\ 3\ 5)(1\ 2\ 3\ 4)(5\ 3\ 1)\\ &= (3\ 2\ 5\ 4)\\ &= (\tau(1)\ \tau(2)\ \tau(3)\ \tau(4))\end{aligned}$$

Lemma 4.4.1. Let $\sigma = (a_1\ a_2\ ...\ a_k) \in S_n$ be a k-cycle. Then for any $\tau \in S_n$, we have

$$\tau\sigma\tau^{-1} = (\tau(a_1)\ \tau(a_2)\ ...\ \tau(a_k))$$

Proof. Notice that since $\sigma(a_1) = a_2$, then

$$\begin{aligned}\tau\sigma\tau^{-1}(\tau(a_1)) &= \tau\sigma(a_1)\\ &= \tau(a_2)\end{aligned}$$

Similarly, $\sigma(a_2) = a_3$ and so

$$\tau\sigma\tau^{-1}(\tau(a_2)) = \tau\sigma(a_2)$$

In general, $\sigma(a_i) = a_{i+1}$ so

$$\tau\sigma\tau^{-1}(\tau(a_i)) = \tau(a_{i+1}) \text{ for } 1 \leq i \leq k$$

Finally, $\sigma(a_k) = a_1$ so

$$\tau\sigma\tau^{-1}(\tau(a_k)) = \tau(a_1)$$

Noting that all the $\tau(a_i)$ are distinct since τ is injective and each a_i is distinct, we have $\tau\sigma\tau^{-1}$ containts the k-cycle

$$(\tau(a_1)\ \tau(a_2)\ ...\ \tau(a_k))$$

Let $b \in A = \{1, 2, ..., n\}$ with $b \notin \{a_1, a_2, ..., a_k\}$. Then

$$\sigma(b) = b$$

and it follows that

$$\tau\sigma\tau^{-1}(\tau(b)) = \tau(b)$$

Hence, $\tau\sigma\tau^{-1} = (\tau(a_1)\ \tau(a_2)\ ...\ \tau(a_k))$. □

Proposition 4.4.1. Let $\sigma, \tau \in S_n$ and suppose that σ has the cycle decomposition

$$\sigma_1\sigma_2...\sigma_j$$

where $\sigma_i = (a_1\ a_2\ ...\ a_{k_i})$. Then $\tau\sigma\tau^{-1}$ has the cycle decomposition

$$\tau_1\tau_2...\tau_j$$

where $\tau_i = (\tau(a_1)\ \tau(a_2)\ ...\ \tau(a_{k_i}))$.

Proof. Proceed by induction on j.

Base Case: $j = 1$
We have

$$\begin{aligned}\tau\sigma\tau^{-1} &= \tau\sigma_1\tau^{-1}\\ &= (\tau(a_1)\ \tau(a_2)\ ...\ \tau(a_{k_1}))\\ &= \tau_1\end{aligned}$$

Inductive Step:
Suppose the result holds for $j = m$. That is, suppose if $\sigma = \sigma_1\sigma_2...\sigma_m$ then $\tau\sigma\tau^{-1} = \tau_1\tau_2...\tau_m$. Now, for $j = m + 1$, we have

$$\begin{aligned}\tau\sigma\tau^{-1} &= \tau(\sigma_1\sigma_2...\sigma_m\sigma_{m+1})\tau^{-1}\\ &= (\tau\sigma_1\tau^{-1})(\tau\sigma_2\tau^{-1})...(\tau\sigma_m\tau^{-1})(\tau\sigma_{m+1}\tau^{-1})\\ &= \tau_1\tau_2...\tau_m(\tau\sigma_{m+1}\tau^{-1})\\ &= \tau_1\tau_2...\tau_m(\tau(a_1)\ \tau(a_2)\ ...\ \tau(a_{k_{m+1}}))\\ &= \tau_1\tau_2...\tau_m\tau_{m+1}\end{aligned}$$

□

Example 4.4.1. Let $\sigma = (1\ 2)(3\ 4\ 5)(6\ 7\ 8\ 9)$ and $\tau = (1\ 3\ 5\ 7)(2\ 4\ 6\ 8)$ in S_9. Then

$$\tau\sigma\tau^{-1} = (3\ 4)(5\ 6\ 7)(8\ 1\ 2\ 9)$$

If $\sigma = (1\ 2\ 3)(4\ 5\ 6\ 7)(8\ 9)$, then

$$\tau\sigma\tau^{-1} = (3\ 4\ 5)(6\ 7\ 8\ 1)(2\ 9)$$

Definition 4.4.1. (Cycle Type, Partition)

1. If $\sigma \in S_n$ is the product of disjoint cycles of lengths $n_1, n_2, ..., n_r$ where $n_1 \le n_2 \le ... \le n_r$ (including 1-cycles), the integers $n_1, n_2, ..., n_r$ are called the cycle type of σ.
2. If $n \in \mathbb{Z}^+$, a partition of n is any non-decreasing sequence of positive integers whose sum is n.
3. Cycle types in S_n are in one-to-one correspondence with partitions of n.

Example 4.4.2.

1. $\sigma = (1\ 2\ 3)(4\ 5\ 6\ 7)(8\ 9)$ has cycle type $1, 2, 3, 4$ in S_10.
2. $\sigma = (2\ 4)(10\ 7)$ has cycle type $1, 1, 1, 1, 1, 1, 2, 2$ in S_10.

We have seen that conjugation preserves cycle type: two elements of S_n are conjugate implies they have the same cycle type. Does the converse of this statement hold? That is, if two elements of S_n have the same cycle type, are they conjugate? Consider two elements in S_8:

$$\sigma_1 = (3\ 4\ 7\ 2)(1\ 5\ 8) \text{ and } \sigma_2 = (1\ 2\ 3\ 4)(5\ 6\ 7)$$

Both σ_1 and σ_2 have cycle type $1, 4, 3$. To be conjugates, we want to find $\tau \in S_8$ such that $\tau\sigma_1\tau^{-1} = \sigma_2$. That is, we want to find $\tau \in S_8$ such that

$$(\tau(3)\ \tau(4)\ \tau(7)\ \tau(2))\,(\tau(1)\ \tau(5)\ \tau(8)) = (1\ 2\ 3\ 4)(5\ 6\ 7)$$

$$\begin{array}{cccccccccccc}
\sigma_1 = & (& 3 & 4 & 7 & 2 &) & (& 1 & 5 & 8 &) \\
 & & \downarrow & \downarrow & \downarrow & \downarrow & & & \downarrow & \downarrow & \downarrow & \\
\sigma_2 = & (& 1 & 2 & 3 & 4 &) & (& 5 & 6 & 7 &)
\end{array}$$

We can choose

$$\begin{array}{ll}
\tau(3) = 1 & \tau(1) = 5 \\
\tau(4) = 2 & \tau(5) = 6 \\
\tau(7) = 3 & \tau(8) = 7 \\
\tau(2) = 4 & \tau(6) = 8
\end{array}$$

Thus $\tau = (1\ 5\ 6\ 8\ 7\ 3)(2\ 4) \in S_8$ provides the desired conjugation.
Now consider the same σ_1 and σ_2, but this time in S_9. Can we find a $\tau \in \S_9$ such that $\tau\sigma_1\tau^{-1} = \sigma_2$? Proceeding as before, we can choose

$$\begin{array}{ll}
\tau(3) = 1 & \tau(1) = 5 \\
\tau(4) = 2 & \tau(5) = 6 \\
\tau(7) = 3 & \tau(8) = 7 \\
\tau(2) = 4 & \tau(6) = 9 \\
\tau(9) = 8 &
\end{array}$$

Thus $\tau = (1\ 5\ 6\ 7\ 3)(2\ 4\ 9\ 8) \in S_9$ provides the desired conjugation.

Proposition 4.4.2. Two elements of S_n are conjugate if and only if they have the same cycle type. The number of cycle types of S_n equals the bumber of partitions of n.