PMATH 336: Introduction to Group Theory with Applications

University of Waterloo

Instructor: Andrew Zucker

Spring 2023

Andrew Wang

Table of Contents

Introduction to Groups

Functions Review

Definition: given two sets X and Y let $f : X \to Y$ be a *function*

- f is an assignment (mapping) to each possible input $x \in X$ to some output $f(x) \in Y$
- X is the *domain* of f
- Y is the *codomain* of f
- $f[X] :=$ *range/image* of $f = \{f(x) : x \in X\}$

The function $f : X \to Y$ is called:

- **Injective** (one-to-one): when $\forall x_1, x_2 \in X$

$$x_1 \neq x_2 \implies f(x_1) \neq f(x_2)$$

- **Surjective** (onto): when $\forall y \in Y$

$$\exists x \in X \text{ where } f(x) = y$$

- **Bijective**: when f is both injective and surjective

Recall: if we are negating a statement we switch $\forall$ to $\exists$ and vice versa

Definition: for sets X, Y, Z the *composition* of functions $f : X \to Y$ and $g : Y \to Z$ is the function

$$g \circ f : X \to Z \text{ given by } (g \circ f)(x) = g(f(x))$$

Theorem: function composition is *assocative*

- given sets W, X, Y, Z along with the functions $f : W \to X$, $g : X \to Y$, $h : Y \to Z$ we have

$$(h \circ g) \circ f = f \circ (g \circ f)$$

Proof: two functions are equal when they produce the same output for all inputs

- Select an arbitrary $w \in W$ then

$$((h \circ g) \circ f)(w) = (h \circ g)(f(w)) = h(g(f(w)))$$

$$(h \circ (g \circ f))(w) = h((g \circ f)(w)) = h(g(f(w)))$$

- Since $(h \circ g) \circ f = h \circ (g \circ f)$ for arbitrary inputs, hence they are equal

Definition: given a set X, let X^X denote the set of functions of the form $f : X \to X$

Notice that: $f, g \in X^X \implies g \circ f \in X^X$

Semigroup, Monid, Group

Definition: Let S be a set, a *binary operation* on S is a function $b : S \times S \to S$

- Takes two elements from S as input and produces a element from S as output
- Written *multiplicatively* if given $s, t \in S$ then the output of $b(s, t)$ is denoted $s \cdot t$ (or just st)
- Written *additively* if given $s, t \in S$ then the output of $b(s, t)$ is denoted $s + t$

Thus for an operation to be a binary operation it must be closed under the set it acts on.

The following is a informal progression of increasing structure towards a group:

- *Magma*: set equipped with a single binary operation (closed by definition of binary operation)
- *Semigroup*: magma except the binary operation is also associative
- *Monoid*: semigroup except that the set contains an identity element
- *Group*: monoid except each element of the set has an inverse

Semigroup

Definition: a *semigroup* is a set S equipped with an associative binary operation, denoted $(S, \cdot)$

- The binary operation on S is *associative* if $\forall s, t, u \in S$

$$s \cdot (t \cdot u) = (s \cdot t) \cdot u$$

- $e_L \in S$ is a *left identity* of S if for every $t \in S$, we have $e_L \cdot t = t$
- $e_R \in S$ is a *right identity* of S if for every $t \in S$, we have $t \cdot e_R = t$
- $e \in S$ is a *2-sided identity* (or just *identity*) of S if e is both a left and right identity of S

Theorem: suppose S is a semigroup and $e_L \in S$ a left identity with $e_R \in S$ a right identity

- $e_L = e_R$ as the 2-sided identity
- Semigroup may have at most one 2-sided identity.

Proof: consider the element $e_L \cdot e_R \in S$ then we have

$$e_L \cdot e_R = e_R \quad \text{and} \quad e_L \cdot e_R = e_L \quad \implies \quad e_R = e_L$$

Definition: given a semigroup $(S, \cdot)$ a *subsemigroup* is a subset $T \subseteq S$ such that

- T is closed under the binary operation inherited from $(S, \cdot)$

$$T \cdot T := \{u \cdot v : u, v \in T\} \subseteq T$$

Note that T is a semigroup in its own right.

Monoid

Definition: a *monoid* is a semigroup S which contains a (necessarily unique) 2-sided identity.

- When written multiplicatively we write the identity element as 1_S
- When written additively we write the identity element as 0_S
- If S is a monoid and $T \subseteq S$, then T is a *submonoid* of S if T is a subsemigroup of S and $1_S \in T$

Fact: $(X^X, \circ)$ is a monoid with id_x (the identity function) as it 2-sided identity

- If $T \subseteq X^X$ is any subsemigroup, then $T \cup \{\mathrm{id}_x\}$ is a monoid
- A subsemigroup $T \subseteq X^X$ can be monoid while not containing id_x, so T is not a submonoid of S

Facts: fix a function $f : X \to Y$ then

- f has a left inverse iff f is injective
- f has a right inverse iff f is surjective
- f has a 2-sided inverse iff f is bijective

If f has a 2-sided inverse it must be unique and we typically denote it as f^{-1}.

Definition: let S be a monoid with identity 1_S and fix $u \in S$

- $v \in S$ is a *left inverse* of u if $v \cdot u = 1_S$
- $v \in S$ is a *right inverse* of u if $u \cdot v = 1_S$
- $v \in S$ is a *2-sided inverse* of u if v is both a left and right inverse of u

Theorem: Let S be a monoid and $u \in S$

- If $v_L, v_R \in S$ are left and right inverses of u then $v_L = v_R$
- It directly follows that u has at most one 2-sided inverse

Proof: consider the element $v_L \cdot u \cdot v_R$ since the binary operation is assocative the following are equivalent:

$$(v_L \cdot u) \cdot v_R = 1_S \cdot v_R = v_R \quad \text{and} \quad v_L \cdot (u \cdot v_R) = v_L \cdot 1_S = v_L$$

When $u \in S$ has a 2-sided inverse we denote that by u^{-1}.

Group

Definition: a *group* is a monoid with every element having a (necessarily unique) 2-sided inverse

Summary: a *group* is a set equiped by some operation where

- The set must must be closed under the operation
- The operation must be associative
- The set must contain an 2-sided identity element
- Every element in the set must have another element in the set that is its 2-sided inverse

Basic Properties of Groups

Definition (*Group*): a set G equipped with associative binary operation with:

- *2-sided identity* $1_G \in G$ (i.e. for every $g \in G$ we have $1_G \cdot g = g = g \cdot 1_G$)
- *2-sided inverse* $g^{-1} \in G$ for every $g \in G$ (i.e. $g^{-1} \cdot g = 1_G = g \cdot g^{-1}$)

Definition: an *Abelian group* (also called a *commutative group*) is a group where $\forall g, h \in G$

$$g \cdot h = h \cdot g$$

Definition: let set X be non-empty, the *symmetric group* on X is

$$\text{Sym}(X) := \{f \in X^X : f \text{ is bijective}\} \subseteq X^X$$

- A bijection of the form $X \to X$ can be called a *permutation* of X
- $\text{Sym}(X)$ may be called a *group of permuations of X*
- When $X = \{1, \ldots, n\}$ we write S_n

For a set of n elements there are $n!$ permutations so $|S_n| = n!$.

Cancellative

Definition: for a semigroup S we say it is

- *Left cancellative* if for any $a, b, c \in S$

$$ab = ac \implies b = c$$

- *Right cancellative* if for any $a, b, c \in S$

$$ba = ca \implies b = c$$

- *Cancellative* if S is both left and right cancellative

Theorem: if G is a group then G is cancellative

Proof: to prove this we show that G is both left and right cancellative

- Suppose that $a, b, c \in S$ satisfies $ab = ac$, then since G is a group we multiply by inverse $a^{-1} \in G$

$$ab = ac \implies a^{-1}ab = a^{-1}ac \implies b = c$$

- Suppose that $a, b, c \in S$ satisfies $ba = ca$, then since G is a group we multiply by inverse $a^{-1} \in G$

$$ba = ca \implies baa^{-1} = caa^{-1} \implies b = c$$

Thus G is both left and right cancellative so it is cancellative.

Order

Definitions:

- *Order of group* G is the size of set $|G|$ (or ∞ if G is infinite)
- *Order of element* $g \in G$ is the least positive number n with $g^n = 1_G$ (or ∞ if no such n exists)

Lemma: Let G be a finite group then every $g \in G$ has finite order

Proof: consider the finite set $\{g^n : n \in \mathbb{N}\} \subseteq G$ (note: $0 \in \mathbb{N}$ for this class)

- $|G| = n$ is finite, so there must exist some $m \geq n$ where $g^m = g^n$ for $n \in \{0, \ldots, n-1\}$
- Then $g^n \cdot g^{-m} = g^{n-m} = 1_G$ and it follows that g has order $N = n - m$ which is finite

Subgroups

Definition: for G a group, a *subgroup* is a subset $H \subseteq G$ is also a group (under the same operation)

- *Subsemigroup*: associatively and $a, b \in H \implies ab \in H$
- *Identity*: there exists $1_H \in H$ such that $1_H a = a = a 1_H$ for all $a \in H$
- *Inverse*: given $g \in H$ we require $g_H^{-1} \in H$ such that $g_H^{-1} g = 1_H = g g_H^{-1}$

We write $H \leq G$ to denote that H is a subgroup of G

Lemma: let G be a group and $H \leq G$ a subgroup, then $1_H = 1_G$

Proof: since H is a subgroup we have $u = (1_H)^{-1}$ (invese of $1_H \in G$) then

$$1_G = u \cdot 1_H = u \cdot (1_H \cdot 1_H) = (u \cdot 1_H) \cdot 1_H = 1_G \cdot 1_H = 1_H$$

Lemma: if G is a group and $H \leq G$ is a subgroup, then for $g \in H$ we have $g_H^{-1} = g^{-1}$ (so $g^{-1} \in H$)

Proof: take $g \in H$ and use $1_H = 1_G = 1$ from earlier (don't assume group is Abelian)

$$g_H^{-1} g = 1_H = 1_G = 1 \quad \text{and} \quad g g_H^{-1} = 1_H = 1_G = 1 \qquad \to \qquad g_H^{-1} = g^{-1} \in H$$

Definition: let G be a group, then a *subgroup* $H \leq G$ must satisfy:

- *Subsemigroup*: $a, b \in H \implies ab \in H$ (and associative)
- *Identity*: $1_G \in H$
- *Inverse*: $g \in H \implies g^{-1} \in H$

Examples of Groups

Symmetric Group

$$\mathrm{Sym}(X) := \{f \in X^X : f \text{ is bijective}\}$$

$f \in \mathrm{Sym}(x)$ is a bijection of the form $f : X \to X$ and can also be called a permuation of X.

We write S_n to denote $\mathrm{Sym}(X)$ when $X = \{1, \ldots, n\}$ and $|S_n| = n!$ (S_n contains $n!$ elements)

- S_0 and S_1 each contain exactly one element (groups with one element are called *trivial*)
- S_2 contains the identity and an element to swap 1 and 2 which we denote by (12)
  - Notice that $(12)^2 := (12) \circ (12) = \mathrm{id}_2$ so we can create a *multiplication table*:

	id_2	(12)
id_2	id_2	(12)
(12)	(12)	id_2

    S_2 is Abelian but S_n in general is not.
  - By convention the entry in the table in row g and column h is the element $g \circ h$

We will now consider S_3 which has 6 elements and can be described in *cycle notation* as the set:

$$S_3 = \{\mathrm{id}_3, (12), (23), (13), (123), (132)\}$$

- (12) denotes ther permutation of $\{1, 2, 3\}$ which swaps 1 and 2 and leaves 3 fixed
- (123) sends $1 \to 2$, $2 \to 3$, $3 \to 1$ and (132) sends $1 \to 3, 3 \to 2, 2 \to 1$
- Composition of permuations described in this notation is requires some practice

$$\text{Example:} \quad (12) \circ (13) = (132)$$

  This can be seen by considering what $(12) \circ (13)$ does on every possible input:

$$((12) \circ (13))(1) = (12)(3) = 3$$
$$((12) \circ (13))(2) = (12)(2) = 1$$
$$((12) \circ (13))(3) = (12)(1) = 2$$

The full multiplication table for S_3 (note that on row g column h is the entry $g \circ h$)

	id_3	(12)	(23)	(13)	(123)	(132)
id_3	id_3	(12)	(23)	(13)	(123)	(132)
(12)	(12)	id_3	(123)	(132)	(23)	(13)
(23)	(23)	(132)	id_3	(123)	(13)	(12)
(13)	(13)	(123)	(132)	id_3	(12)	(23)
(123)	(123)	(13)	(12)	(23)	(132)	id_3
(132)	(132)	(23)	(13)	(12)	id_3	(123)

- Notice that $gh = hg$ is not always satisfied so S_3 is not Abelian.
  - An example of this can be seen with (13) and (12)

$$((12) \circ (13))(\{1,2,3\}) = (12)(\{3,2,1\}) = \{3,1,2\} \quad \to \quad (12) \circ (13) = (132)$$

$$((13) \circ (12))(\{1,2,3\}) = (13)(\{2,1,3\}) = \{2,3,1\} \quad \to \quad (13) \circ (12) = (123)$$

  - Notice that (123) is the same as (231) and (312)
- id_3 appears in an entry for each row and in each column

$$\text{every row as has an id} \iff \forall g \in G\ \exists h \in G \ \ gh = \text{id} \iff \text{every element has a right inverse}$$

$$\text{every column has an id} \iff \forall g \in G\ \exists h \in G \ \ hg = \text{id} \iff \text{every element has a left inverse}$$

- There are also no repeats in any row or column which corresponds to being cancellative

$$(\forall g, h_0, h_1 \in G \qquad h_0 \neq h_1 \implies h_0 g \neq h_1 g_1) \iff \text{right cancellative}$$

$$(\forall g, h_0, h_1 \in G \qquad h_0 \neq h_1 \implies g h_0 \neq g h_1) \iff \text{left cancellative}$$

  note this is the contrapositive of the definition of cancellative.

S_3 is a group so the last two observations should not be surprising but it is nice to get a concrete example.

Remark: elements of S_3 correspond to symmetrices of a triangle's rotations and flips

- In general however S_n *does not* correspond to symmetrices of an n-gon

Dihedral Group

$$D_{2n} = \{f \in S_n : \forall i, j \in \{1, \ldots, n\},\ i \sim j \iff f(i) \sim f(j)\}$$

The Dihedral group D_{2n} is a subgroup of S_n where the permutation respects the *edges*

- For a more concrete understanding imagine n points arranged in a circle
  - S_n is if you are allowed to swap any point with any other point
  - D_{2n} is if adjacent vertices must remain adjacent vertices after the mapping

- This is much more restrictive and we find that $|D_{2n}| = 2n$ while $|S_n| = n!$
- Note that most literature use D_n to mean the same thing as our D_{2n}

We will inspect D_8 which is the group of symmetries of a square (4-gon)

$$D_8 = \{f \in S_4 : \forall i, j \in \{1,2,3,4\},\ i \sim j \iff f(i) \sim f(j)\}$$

- We have vertices labelled $1, 2, 3, 4$
- We also have the edge relations $1 \sim 2,\ 2 \sim 3,\ 3 \sim 4,\ 4 \sim 1$
  - note: for $a, b \in \{1,2,3,4\}$ having $a \sim b$ also means we have $b \sim a$ and we also take $a \sim a$
- There are 8 elements of D_8 which are

$$D_8 = \{\mathrm{id}_4,\ R_{90},\ R_{180},\ R_{270},\ F,\ R_{90} \circ F,\ R_{180} \circ F,\ R_{270} \circ F\}$$

  - R_n denotes rotate n degrees
  - F denotes flip (any flip that does not move the square is fine)
  - $R_n \circ F$ denotes flip then rotate n degrees

Let us verify $D_8 \leq S_4$. begin by letting $i, j \in \{1,2,3,4\}$

- Subsemigroup: $f, g \in D_8$

$$\begin{aligned} i \sim j &\iff g(i) \sim g(j) && (\text{as } g \in D_8) \\ &\iff f(g(i)) \sim f(g(j)) && (\text{as } f \in D_8) \end{aligned}$$

  Hence $f \circ g \in D_8$
- Identity $\mathrm{id}_4 \in D_8$

$$i \sim j \iff i = \mathrm{id}_4(i) \sim \mathrm{id}_4(j) = j$$

- Inverse: if $f \in D_8$ consider $f^{-1} \in S_4$ (show that $f^{-1} \in D_8$)

$$\begin{aligned} f^{-1}(i) \sim f^{-1}(j) &\iff f(f^{-1}(i)) \sim f(f^{-1}(j)) && (f \in D_8) \\ &\iff i \sim j && (f \circ f^{-1} = \mathrm{id}_4) \end{aligned}$$

  which shows that $f^{-1} \in D_8$

Additive Group of Integers Modulo n

Let $\mathbb{Z}_n := \{i \in \mathbb{N} : 0 \leq i < n\}$ then given $a, b \in \mathbb{Z}_n$ we set

$$a + b = i \bmod n \iff a + b = i + cn \text{ for some } c \in \mathbb{Z}$$

- Proof of associative is trivial
- This group is Abelian because normal addition is commutative
- The 2-sided identity is 0 and given $i \in \mathbb{Z}_n$ the $-i$ (inverse) is

$$-i = \begin{cases} 0 & \text{if } i = 0 \\ n - 1 & \text{if } i \neq 0 \end{cases}$$

- As a result we know that $(\mathbb{Z}_n, +)$ is a group
- For $a \in \mathbb{Z}_n$ what are the possible values for $|a|$?
  - e.g. for $3, 4 \in \mathbb{Z}_6$ then $|4| = 3$ $(4, 2, 0)$ and $|3| = 2$ $(3, 0)$
  - We know that $m \leq n$ is a possible order iff $m \mid n$

Other related groups:

- $(\mathbb{Z}, +)$ is an *additive* group (Abelian and every *non-zero* element has order ∞)
- $(\mathbb{R}, +)$ is an *additive* group

Multiplicative Group of Integers Modulo n and Unit Group

Let $\mathbb{Z}_n := \{i \in \mathbb{N} : 0 \leq i < n\}$ then given $a, b \in \mathbb{Z}_n$ we set

$$a \cdot b = i \bmod n \iff a \cdot b = i + cn \text{ for some } c \in \mathbb{Z}$$

- Proof of associative is trivial
- This group is Abelian because normal multiplication is commutative
- The 2-sided identity is 1
- 0 will never have an inverse so $(\mathbb{Z}_n, \cdot)$ is not a group when $n \geq 2$
  - another failure: in $\mathbb{Z}_4$, 2 does not have an inverse

Lemma (*Bézout*): let $a, b \in \mathbb{Z}$ then $\exists x, y \in \mathbb{Z}$ such that

$$\gcd(a, b) = ax + by$$

- If $\gcd(m, n) = 1$ there would exist some $x, y \in \mathbb{Z}$ such that

  $$1 = mx + ny \quad \rightarrow \quad 1 = mx \bmod n$$

  This means that m's inverse x will exist if $\gcd(m, n) = 1$
- If x is m's inverse then $1 = mx + ny$ and letting $g = \gcd(m, n)$ then

  $$g \mid m \text{ and } g \mid n \quad \Longrightarrow \quad g \mid mx + ny \quad \Longrightarrow \quad g \mid 1$$

  Since only 1 and -1 divides 1 the only choice is that $\gcd(m, n) = 1$ (since gcd can't be negative)

As a result, $m \in \mathbb{Z}_n$ has a multiplicative inverse iff $\gcd(m, n) = 1$

Definition: the *unit group* is the subset $\mathbb{U}_n \subseteq \mathbb{Z}_n$ of elements with a multiplicative inverse:

$$\mathbb{U}_n = \{m \in \mathbb{Z}_n : \gcd(m, n) = 1\}$$

- e.g. $\mathbb{U}_7 = \{1, 2, 3, 4, 5, 6\}$
- e.g. $\mathbb{U}_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\}$

Notice that when p is prime then $\mathbb{U}_p = \{1, \ldots, p - 1\}$

Free Group

The *free group* on 2 generators F_2 is built from the formal symbols $\{a, a^{-1}, b, b^{-1}\}$

- A word over this alphabet is just a finite string of the symbols
- The *reduced word* over this alphabet is a word where no more cancellation is possible
  - $aa^{-1},\ a^{-1}a,\ bb^{-1},\ b^{-1}b$ can all be cancelled into into identity 1
  - every word is *equivalent* to some unique reduced word
  - e.g. $abaa^{-1}b^{-1}ab \to abb^{-1}ab \to aab$

The *free group* F_2 is the set of reduced words under the operation of concatenation and reduction

- e.g. $(aab) \cdot (b^{-1}ab) = aaab$
- The identity is the empty word
- Inverse is flipping the word and inverting all the symbols
  - e.g. $(ab)^{-1} = b^{-1}a^{-1}$

This group is not Abelian and every non-identity element has infinite order

Infinite Dihedral Group

The *infinite dihedral group* D_∞ is the set of reduced words built from the formal symbols $\{a, b\}$

- This time we let a and b as their own inverse symbol and use the same reduction rule
  - $aa = 1 = bb$ then $|a| = 2 = |b|$
  - e.g. $baab = 1 = abba$
  - e.g. $|ab| = \infty = |ba|$
  - e.g. $aaababb \to ababb \to aba$
- The identity is once again the empty string
- Inverse of a given string is produced by flipping the string backwards
  - e.g. $(ab)^{-1} = ba$

This group is not Abelian but notice that it is a infinite group with elements of finite order

The finite dihedral group D_{2n} denotes the symmetries of an n-gon so what do elements of D_∞ act on?

- A shape with ∞ edges (∞-gon) is a infinite line up and down wich each vertex labelled
- Applying a flips the line at the point just above 0
- Applying b flips the line at 0
- ab shifts the line 1 slot upwards (ba shifts the line one slot downwards)

Say that $|D_\infty| = \infty$ while many elements have order 2 and many others have order ∞

Subgroups and Generators

Subgroup Tests

Proposition (*one-step subgroup test*): suppose G is a group, then $H \leq G$ if H is *non-empty* and

- H is a subsemigroup of G
- H is closed under inverses

Proof: just need to show that $1_G \in H$

- Since $H \neq \emptyset$, fix any $g \in H$
- Using H's closure under inverses we also must have $g^{-1} \in H$
- As $H \subseteq G$ is a subsemigroup (closed under composition) we have

$$g^{-1} \cdot g = 1_G \in H$$

Proposition (*finite subgroup test*): suppose G is a *finite* group, then $H \leq G$ if H is *non-empty* and

- H is a subsemigroup of G

Proof: just need to show that H is closed under inverses

- Since $H \neq \emptyset$, fix any $g \in H$
- Then to show that $g^{-1} \in H$ we use G is finite and find $|g| = n \in \mathbb{N}\backslash\{0\}$
  - If $n = 1$ then $g = 1_G = g^{-1}$
  - If $n \geq 2$ then $g^{n-1} \cdot g = 1_G = g \cdot g^{n-1}$ so we get $g^{n-1} = g^{-1} \in H$

Generators

Definitions: let G be a group and $X \subseteq G$

- $\langle X \rangle_s$ denotes *subsemigroup generated by* X, which is the smallest subsemigroup of G containing X
- $\langle X \rangle$ denotes *subgroup generated by* X, which is the smallest subgroup of G containing X

Proposition: let G be a group and $X \subseteq G$ then

1. $\langle X \rangle_s = \{x_1^{n_1} \cdots x_m^{n_m} : x_1, \ldots, x_m \in X;\ m, n_1, \ldots, n_m \in \mathbb{N}\backslash\{0\}\}$
2. $\langle X \rangle = \{x_1^{n_1} \cdots x_m^{n_m} : x_1, \ldots, x_m \in X;\ m \in \mathbb{N};\ n_1, \ldots, n_m \in \mathbb{Z}\}$

Proof: we have $1_G \in \langle X \rangle_s$ and $1_G \in \langle X \rangle$ since we an take $m = 0$

1. To show $\langle X \rangle_s$ is a subsemigroup take some $x_1^{n_1} \cdots x_m^{n_m},\ y_1^{k_1} \cdots y_\ell^{k_\ell} \in \langle X \rangle_s$

- Consider the product $x_1^{n_1} \cdots x_m^{n_m} \cdot y_1^{k_1} \cdots y_\ell^{k_\ell}$ by renaming y_j to x_{m+j} and k_j to n_{m+j} then

$$x_1^{n_1} \cdots x_{m+\ell}^{n_{m+\ell}} \in \langle X \rangle_s$$

  so $\langle X \rangle_s$ is a subsemigroup

2. To show $\langle X \rangle$ is a group we use the one-step subgroup test
   - By the same argument as (1) we get that $\langle X \rangle$ is a subsemigroup
   - To show that $\langle X \rangle$ is closed under inverses, let $x_1^{n_1} \cdots x_n^{n_m} \in \langle X \rangle$ then

$$(x_1^{n_1} \cdots x_m^{n_m})^{-1} = x_m^{-n_m} \cdots x_1^{-n_1} \in \langle X \rangle$$

     so $\langle X \rangle$ is a group

These are the smallest since they are produced from taking products of elements and inverses of X

Remarks:

- If $\langle X \rangle = G$ then we say that X *generates* G
- When $X = \{g_1, \cdots, g_k\}$ for some $g, \ldots, g_k \in G$ we usually write $\langle g_1, \ldots, g_k \rangle$ for $\langle \{g_1, \ldots, g_k\} \rangle$
- When $X = \{g\}$ for some $g \in G$ then $\langle g \rangle$ is the *cyclic subgroup* generated by $g \in G$

Examples:

- Consider the group $(\mathbb{Z}, +)$

$$\langle 15, -10 \rangle = 5\mathbb{Z} = \{5n : n \in \mathbb{Z}\}$$

  since $\gcd(15, -10) = 5$
- Consider the group $D_8 = \{\mathrm{id}_4, R_{90}, R_{180}, R_{270}, F, R_{90} \cdot F, R_{180} \cdot F, R_{270} \cdot F\}$

$$\langle R_{90} \rangle = \{\mathrm{id}_4, R_{90}, R_{180}, R_{270}\}$$

  via the finite subgroup test $\langle R_{90} \rangle_s = \langle R_{90} \rangle$ the set is finite
- Consider the free group on 2 generators $F_2 = \langle a, b \rangle$

$$\langle ab, a \rangle = F_2$$

  since $a^{-1}ab = b$ so we have $\{a, b\}$ to construct any element of F_2

Center, Centralizer, Commutator Subgroups

Definitions: let G be a group then

- *Center* of G (subset of G that is Abelian)

$$Z(G) := \{g \in G : \forall h \in G,\ gh = hg\}$$

  - Note that $gh = hg \iff g = hgh^{-1} \iff g = h^{-1}gh$

- *Centralizer* of subset $S \subseteq G$ in G (subset of G that is Abelian with S)
$$C_G(S) := \{g \in G : \forall h \in S,\ gh = hg\}$$
  - Note that $C_G(G) = Z(G)$
  - If $S = \{g\}$ for some $g \in G$ we write $C_G(g)$ instead of $C_G(\{g\})$

- *Commutator* of some given $a, b \in G$ is the group element
$$[a, b] := a^{-1}b^{-1}ab$$
(this notation does not denote an interval)
  - note that $ab = ba \cdot [a, b]$
  - this tells use how far the elemenets are from being commutative
  - if a, b are commuative then $[a, b] = 1_G$

- *Commutator subgroup* of G (sometimes called the *derived subgroup*) is
$$[G, G] := \langle [a, b] : a, b \in G \rangle$$
($[G, G]$ is the subgroup generated by commutators)

Fact: for a group G the following are equivalent:

- G is Abelian
- $Z(G) = G$
- $[G, G] = \{1_G\}$

Examples:

- Consider D_8
  - $C_{D_8}(F)$ has id_4, F, R_{180} and add $R_{180}F$ because the set needs to be a subgroup
$$C_{D_8}(F) = \{\mathrm{id}_4,\ F,\ R_{180},\ R_{180} \circ F\}$$
  - $C_{D_8}(R_{90})$ contains all rotations because that is the cyclic subgroup generated by R_{90}
$$C_{D_8}(R_{90}) = \{\mathrm{id}_4,\ R_{90},\ R_{180},\ R_{270}\}$$
  - Since $D_8 = \langle R_{90}, F \rangle$ we have
$$Z(D_8) = C_{D_8}(F) \cap C_{D_8}(R_{90}) = \{\mathrm{id}_4, R_{180}\}$$
In general for non-empty subsets $A_1, \ldots, A_k \subseteq G$ if we have $G = \langle A_1, \ldots, A_k \rangle$ then
$$Z(G) = C_G(A_1) \cap \cdots \cap C_G(A_k)$$
In order for $a \in Z(G)$ it would need to commute $\forall g \in G$ so it should show up in every $C_G(A_i)$
$$C_G(S) := \{g \in G : \forall h \in S,\ gh = hg\}$$

- Consider $F_2 = \langle a, b \rangle$ we claim that $Z(F_2) = \{1_{F_2}\}$
  - Let $w \in F_2$ be a non-trivial reduced word, say $w = y_1 \cdots y_n$ with $y_i \in \{a, b, a^{-1}, b^{-1}\}$
  - Let $x \in \{a, b, a^{-1}, b^{-1}\}$ be chosen so $x \neq y_1$ and $x \neq y_1^{-1}$ then

$$xw = xy_1 \cdots y_n$$

    * If $n = 1$ then $wx = y_1 x$ is reduced and $xw \neq wx$ since $xy_1 \neq y_1 x$
    * If $n \geq 2$ then wx even after reducing still starts with the same letter as w
      · xw specifically does not start with the same letter as w so we must have $xw \neq wx$

  as a result we can say that $w \notin Z(G)$

Isomorphisms, Cyclic Groups, Permutation Groups

Isomorphisms

Definitions: Let G and H be groups

- An *isomorphism* is a bijection $\psi : G \to H$ which respects the group operations:

$$\forall a, b \in G \qquad \psi(a \cdot b) = \phi(a) \cdot \phi(b)$$

  - $a \cdot b$ uses the group operation from G while $\phi(a) \cdot \phi(b)$ uses the group operation from H
- G and H are *isomorphic* (written $G \cong H$) if there is an isomorphism from G to H (or vice versa)

Remark: we can have isomorphisms between groups written additively and multiplicatively:

$$\psi(a + b) = \psi(a) \cdot \psi(b)$$

Proposition: let G and H be groups and $\psi : G \to H$ be an isomorphism, then

1. $\psi^{-1} : H \to G$ is also an isomorphism
2. $\psi(1_G) = 1_H$
3. $\forall g \in G$ we get $\psi(g^{-1}) = \psi(g)^{-1}$

Proofs:

1. ψ^{-1} is clearly a bijection so we just need to check that it respects the group operations
   - Let $h_0, h_1 \in H$, then since ψ is an isomorphism

$$\begin{aligned} \psi(\psi^{-1}(h_0) \cdot \psi^{-1}(h_1)) = \psi(\psi^{-1}(h_0)) \cdot \psi(\psi^{-1}(h_1)) &= h_0 \cdot h_1 \\ \psi(\psi^{-1}(h_0 \cdot h_1)) &= h_0 \cdot h_1 \end{aligned}$$

   - Since ϕ is a bijection these outputs can only be the same iff the inputs are the same so

$$\psi^{-1}(h_0) \cdot \psi^{-1}(h_1) = \psi^{-1}(h_0 \cdot h_1)$$

2. Let $a \in G$ and $b \in H$ where $\psi(a) = b$ then

$$b = \psi(a \cdot 1_G) = a \cdot \psi(1_G)$$

$$b = \psi(1_G \cdot a) = \psi(1_G) \cdot a$$

   since $\psi(1_G)$ is a (necessarily unique) 2-sided inverse then $1_H = \psi(1_G)$
3. Let $a \in G$ then

$$\psi(a^{-1}) \cdot \psi(a) = \psi(a^{-1}a) = 1_H = \psi(a)^{-1} \cdot \psi(a) \quad \implies \quad \psi(a^{-1}) = \psi(a)^{-1}$$

Proposition: if G, H, K are groups with $G \cong H$ and $H \cong K$ then $G \cong K$

Proof: let $\psi : G \to H$ and $\varphi : H \to K$ be isomorphisms. to show that

$$\varphi \circ \psi : G \to K$$

is an isomorphism we observe that it is a bijection. Then consider $a, b \in G$

$$\begin{aligned} \varphi \cdot \psi(a \cdot b) &= \varphi(\psi(a \cdot b)) \\ &= \varphi(\psi(a) \cdot \psi(b)) \\ &= \varphi(\psi(a)) \cdot \varphi(\psi(b)) \\ &= (\varphi \circ \psi(a)) \cdot (\varphi \circ \psi(b)) \end{aligned}$$

Keep in mind that there are three different group operations present in the above.

Cyclic Groups

Definition: a group G is *cyclic* if there exists $a \in G$ with $G = \langle a \rangle$

We have two examples for cyclic groups (and all other cyclic groups are isomorphic to these)

1. $(\mathbb{Z}, +) = \langle 1 \rangle$
2. $(\mathbb{Z}_n, +) = \langle 1 \rangle$ for $n \in \mathbb{N} \backslash \{0\}$

Remark: all cyclic groups are Abelian but not all Abelian groups are cyclic

Theorem: let $G = \langle a \rangle$ be a cyclic group then $|G| = |a|$

- Order of $a \in G$ denoted $|a| = n \geq 1$ is the lowest value with $a^n = 1_G$ (or ∞ if no such n exists)

Proof: by definition we have $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$

- If $|a| = \infty$
  - If $|G|$ is finite then for some $m, n \in \mathbb{Z}$ with $m < n$ there exists $a^m = a^n$ however
  $$a^m = a^n \iff 1_G = a^{n-m}$$
  but $n - m \in \mathbb{N} \backslash \{0\}$ contradicting that $|a|$ has infinite order so $|G| = \infty$
- If $|a| = n \in \mathbb{N} \backslash \{0\}$
  - If $|G| < n$ then for some $i, j \in \{0, \ldots, n-1\}$ with $j < i$ there exists $a^j = a^i$ however
  $$a^j = a^i \iff 1_G = a^{i-j}$$
  but $i - j < n$ contradicts that $|a| = n$ so we must have $|G| \geq n$
  - Noting that every $m \in \mathbb{Z}$ satisfies $m = nq + r$ for some $q \in \mathbb{Z}$ and $r \in \{0, \ldots, n-1\}$ then
  $$a^m = a^{nq} \cdot a^r = (a^n)^q \cdot a^r = 1_G \cdot a^r = a^r$$
  this says that $|G| \leq n$ which combined with the previous point shows that $|G| = n$

Theorem: let $G = \langle a \rangle$ be a cyclic group then

- If $|a| = \infty$ then $G \cong (\mathbb{Z}, +)$
- If $|a| = n \in \mathbb{N}\backslash\{0\}$ then $G \cong (\mathbb{Z}_n, +)$

Proof:

1. Define $\psi : \mathbb{Z} \to G$ via $\psi(m) = a^m$
   - from proof of $|G| = |a|$ we argued if $|a| = \infty$ then for all $m, n \in \mathbb{Z}$ with $m < n$ we get $a^m \neq a^n$
   - from that we get that ψ is an injection and also surjective by definition of $\langle a \rangle$
   - ψ is bijective so just need to show it respects the group operations to be an isomorphism

$$\forall m, n \in \mathbb{Z} \qquad \psi(m+n) = a^{m+n} = a^m \cdot a^n = \psi(m) \cdot \psi(n)$$

2. Assume $|a| = n$ with $n \in \mathbb{N}\backslash\{0\}$ and define $\psi : \mathbb{Z}_n \to G$ via $\psi(m) = a^m$
   - from proof of $|G| = |a|$ we argued that for all $m, n \in \{0, \ldots, n-1\}$ with $m < n$ that $a^m \neq a^n$
   - from that we get that ψ is an injection
   - since ψ is an injection from one finite set another set of the same size, ψ is a bijection
   - with ψ bijective we just need to check that ψ respects group operations, so fix $k, \ell \in \mathbb{Z}_n$
     - if $k + \ell < n$ then

$$\begin{aligned} \psi(k + \ell \bmod n) &= \psi(k + \ell) \\ &= a^{k+\ell} \\ &= a^k \cdot a^\ell \\ &= \psi(k) \cdot \psi(\ell) \end{aligned}$$

     - if $k + \ell \geq n$ then

$$\begin{aligned} \psi(k + \ell \bmod n) &= \phi(k + \ell - n) \\ &= a^{k+\ell-n} \\ &= a^k \cdot a^\ell \cdot a^{-n} && \text{(note: } a^{-n} = (a^n)^{-1} = 1_G) \\ &= \psi(k) \cdot \psi(\ell) \end{aligned}$$

Theorem: every subgroup of a cyclic group is cyclic

Proof:

- Consider subset $X \subseteq \mathbb{Z}$
  - $\gcd(X) = d \in \mathbb{N}$ is the greatest number that divides every $x \in X$
  - by Bézout's identity for $x_1, \ldots, x_n \in X$ there exists $a_1, \ldots, z_n \in \mathbb{Z}$ with

    $$d = a_1 x_1 + \cdots + a_n x_n$$

    this means that $d \in \langle X \rangle$ and hence $\langle d \rangle \subseteq \langle X \rangle$
  - also if $m \in \langle X \rangle$ then, since $d \mid x$ for $x \in X$, we must have $d \mid m$ so $m \in \langle d \rangle$ thus $\langle d \rangle = \langle X \rangle$
- Consider subset $X \subseteq \mathbb{Z}_n$
  - just like above we have $\gcd(X) = d \in \mathbb{N}$ and $a_1 x_1 + \cdots + a_n x_n = d \in \langle X \rangle$ so $\langle d \rangle \subseteq \langle X \rangle$
  - if $m \in \langle X \rangle$ then, since $d \mid x$ for $x \in X$, we must have $d \mid m + qn$ for some $q \in \mathbb{Z}$
  - since $m + qn = m \bmod n$ we conclude that $m \in \langle d \rangle$ thus $\langle d \rangle = \langle X \rangle$

Euler's Totient Function

Definition: *Euler's phi function* $\phi : \mathbb{N}\backslash\{0\} \to \mathbb{N}\backslash\{0\}$ defined by

$$\phi(d) := |\{k \in \mathbb{N}\backslash\{0\} \ : \ k < d \ \text{ and } \ \gcd(k, d) = 1\}|$$

Remark: usually refered to as *Euler's totient function* in the literature

Example: $\phi(8) = |\{1, 3, 5, 7\}| = 4$

Theorem: fix $n \in \mathbb{N}\backslash\{0\}$ and consider $\mathbb{Z}_n$

1. If $d \in \mathbb{Z}_n$ and $d \mid n$ then

   $$\langle d \rangle = \{0, \ d, \ 2d, \ \ldots, \ n - d\} \quad \text{and} \quad |d| = \frac{n}{d}$$

2. For any $a \in \mathbb{Z}_n$ we have

   $$\langle a \rangle = \langle \gcd(a, n) \rangle$$

3. Given $a, b \in \mathbb{Z}_n$ we have

   $$\langle a \rangle = \langle b \rangle \iff \gcd(a, n) = \gcd(b, n)$$

Proof:

1. Since $\frac{n}{d} \cdot d = 0 \bmod n$ we definitely have $|d| \leq \frac{n}{d}$
   - for $|d| \geq \frac{n}{d}$ we know that for all $k \in \mathbb{N}\backslash\{0\}$ with $k < \frac{n}{d}$ we have $0 < kd < n$ so we get $|d| = \frac{n}{d}$
2. Write $d = \gcd(a, n)$ as $a = qd$ for some $q \in \mathbb{Z}$ and directly get $\langle a \rangle \subseteq \langle d \rangle$
   - to show that $d \in \langle a \rangle$ we use Bézout's identity to say there exists $k, \ell \in \mathbb{Z}$ with $d = ka + \ell n$
   - then $d = ka + \ell n = ka \bmod n$ and $d \in \langle a \rangle$ so hence $\langle a \rangle = \langle d \rangle$

3. the right to left implication follows directly from (2)
    - for the converse suppose $\gcd(a, n) \neq \gcd(b, n)$ then by (1)

    $$|\langle \gcd(a, n) \rangle| = \frac{n}{\gcd(a, n)} \neq \frac{n}{\gcd(b, n)} = |\langle \gcd(b, n) \rangle|$$

    since the cyclic subgroups have different sizes by (2) we have $\langle a \rangle \neq \langle b \rangle$

Corollary: if G finite cyclic group and $d \mid n$ then G has exactly one subgroup H of order d

Proof: we may assume that $G = \mathbb{Z}_n$ (because conclusion of corollary is preserved by isomorphism)

- For existance of $H \leq G$ with order d we let $H = \langle \frac{n}{d} \rangle$
    - then since $\frac{n}{d} \mid n$ by part 1 of the previous theorem $|\frac{n}{d}| = n/\frac{n}{d} = d$ and we get $|H| = |\frac{n}{d}| = d$
- For uniqueness consider some subgroup $K \leq G$ with $|H| = d$
    - for some $a \in \mathbb{Z}_n$ we have $H = \langle a \rangle$ and by part 2 of previous theorem $\langle a \rangle = \langle \gcd(a, n) \rangle$
    - for $|\langle \gcd(a, n) \rangle| = d$ by part 1 of previous theorem then $\gcd(a, n) = n/d$ thus $K = H$

Corollary:

1. If G is a cyclic group of order $n \in \mathbb{N}\backslash\{0\}$ then

$$|\{g \in G : \langle g \rangle = G\}| = \phi(n)$$

2. If G is a cyclic group of order $n \in \mathbb{N}\backslash\{0\}$ and $d \geq 1$ divides n then

$$|\{a \in G : |a| = d\}| = \phi(d)$$

3. If G is *any* finite group and $d \in \mathbb{N}\backslash\{0\}$

$$|\{a \in G : |a| = d\}| \text{ is a multiple of } \phi(d)$$

Proof: for parts (1) and (2) we work with $G = \mathbb{Z}_n$

1. Given $a \in \mathbb{Z}_n$ we know $\langle a \rangle = \langle \gcd(a, n) \rangle$ so

$$\langle a \rangle = G = \langle 1 \rangle \iff \gcd(a, n) = 1$$

and the number of such $a \in \mathbb{Z}_n$ is exactly $\phi(n)$

2. Any $a \in \mathbb{Z}_n$ with $|a| = d$ belongs to *unique* subgroup of order d generated by $\langle \frac{n}{d} \rangle$

We then just apply part (1) to this subgroup

3. Consider the collection

$$X = \{H \leq G : H \cong \mathbb{Z}_d\}$$

every $a \in G$ of order d belongs to at least one memory of X, namely $\langle a \rangle$

- Inside each $H \in X$ there are exactly $\phi(d)$-many elements of order d by part (2)
- If $H_0, H_1 \in X$ and $a \in H_0 \cap H_1$ has order d then $\langle a \rangle = H_0 = H_1$ hence

$$|\{a \in G : |a| = d\}| = |X| \cdot \phi(d)$$

Permutation Groups

Recall: permutation groups are subgroups of the symmetric group.

- Given a set X, we write $\mathrm{Sym}(X)$ for the group of permuations of X (bijections from X to itself)
- If $X = \{1, \ldots, n\}$ for some $n \in \mathbb{N}\backslash\{0\}$ we write S_n for the symmetric group

Definitions: let X be a set, and fix $\sigma \in \mathrm{Sym}(X)$

- Subset $Y \subseteq X$ is σ-*invariant* if $\sigma[Y] = Y$
- Given $y \in X$, the σ-*orbit* of y is the smallest σ-invariant set containing y

$$O_\sigma(y) := \{\sigma^m(y) : m \in \mathbb{Z}\}$$

  - the cycle created by repeatedly applying σ to y
- The *support* of σ is the σ-invariant set

$$\mathrm{supp}(\sigma) := \{y \in X : \sigma(y) \neq y\}$$

  - the set of all $y \in X$ that was moved by σ

Proposition:

1. Supposing $\sigma, \theta \in \mathrm{Sym}(x)$ have disjoint supports then

$$\sigma \circ \theta = \theta \circ \sigma$$

2. Suppose $\sigma \in \mathrm{Sym}(X)$ and that $\mathrm{supp}(\sigma) = Y \cup Z$ with Y and Z disjoint, non-empty, and σ-invariant
   - then there are $\sigma_Y, \sigma_Z \in \mathrm{Sym}(X)$ with

$$\mathrm{supp}(\sigma_Y) = Y,\ \mathrm{supp}(\sigma_Z) = Z \quad \text{and} \quad \sigma = \sigma_Y \circ \sigma_Z = \sigma_Z \circ \sigma_Y$$

Proof:

1. Given $x \in X$ we have

$$\sigma \circ \theta(x) = \theta \circ \sigma(x) = \begin{cases} x & \text{if } x \notin \mathrm{supp}(\sigma) \cup \mathrm{supp}(\theta) \\ \sigma(x) & \text{if } x \in \mathrm{supp}(\sigma) \\ \theta(x) & \text{if } x \in \mathrm{supp}(\theta) \end{cases}$$

   Remark: this fails if the supports are *not disjoint*

2. Define $\sigma_Y, \sigma_Z \in \mathrm{Sym}(X)$ where given $x \in X$, we have

$$\sigma_Y(x) = \begin{cases} x & \text{if } x \notin Y \\ \sigma(x) & \text{if } x \in Y \end{cases} \qquad \sigma_Z(x) = \begin{cases} x & \text{if } x \notin Z \\ \sigma(x) & \text{if } x \in Z \end{cases}$$

   Now we check that σ_Y and σ_Z are bijections.

- Consider $\sigma^{-1} \in \mathrm{Sym}(X)$ and define $(\sigma^{-1})_Y : X \to X$ via

$$(\sigma^{-1})_Y(x) = \begin{cases} x & \text{if } x \notin Y \\ \sigma^{-1}(x) & \text{if } x \in Y \end{cases}$$

  As Y is σ-invariant it is also σ^{-1}-invariant (verify that $(\sigma^{-1})_Y = (\sigma_Y)^{-1}$)
- We can say that σ_Y is invertible and thus a bijection (similar argument for σ_Z)
- Notice that $\mathrm{supp}(\sigma_Y) = Y$ and $\mathrm{supp}(\sigma_Z) = Z$ and so

$$\sigma_y \circ \sigma_z(x) = \sigma_z \circ \sigma_y(x) = \begin{cases} x & \text{if } x \notin Y \cup Z = \mathrm{supp}(\sigma) \\ \sigma(x) & \text{if } x \in Y \\ \sigma(x) & \text{if } x \in Z \end{cases}$$

  since they are disjoint we get $\sigma_Y \circ \sigma_Z = \sigma$

Proposition: let $\sigma \in \mathrm{Sym}(X)$ then given $x, y \in X$ either

$$O_\sigma(x) = O_\sigma(y) \quad \text{or} \quad O_\sigma(x) \cap O_\sigma(y) = \emptyset$$

Proof: suppose $z \in O_\sigma(x) \cap O_\sigma(y)$, we will show that $O_\sigma(x) = O_\sigma(y) = O_\sigma(z)$

- Write $z = \sigma^m(x)$ for some $m \in \mathbb{Z}$, so we also have $x = \sigma^{-m}(z)$
- Given $u \in O_\sigma(x)$ we have $u = \sigma^n(x)$ for some $n \in \mathbb{Z}$, so we also have

$$u = \sigma^n(\sigma^{-m}(z)) = \sigma^{n-m}(z) \in O_\sigma(z)$$

- Given $v \in O_\sigma(z)$ we have $v = \sigma^k(z)$ for some $k \in \mathbb{Z}$, so we also have

$$v = \sigma^k(\sigma^m(x)) = \sigma^{k+m}(x) \in O_\sigma(x)$$

- Hence $O_\sigma(x) = O_\sigma(z)$ and we can make a simular proof for $O_\sigma(y) = O_\sigma(z)$

Permutation Cycles

Definitions: let $\sigma_1, \sigma_2 \in \mathrm{Sym}(X)$

- *Cycle* is any $\sigma \in \mathrm{Sym}(X)$ with exactly one *non-trivial* orbit (i.e. of size > 1)
- *Size* of a cycle is the size of its unique non-trivial orbit
- *Disjoint* when if cycles $O_1, O_2 \subseteq X$ denotes unique non-trival orbits of σ_1, σ_2 then $O_1 \cup O_2 = \emptyset$

Theorem: any $\sigma \in S_n$ can be written as the product of *finitely many pairwise-disjoint cycles*

- We call such a product the *disjoint cycle form of* σ
- The full disjoint cycle form is unique

Proof: let $X = \{O_i : i \leq k\}$ list all non-trivial orbits of σ_i

- Since each O_i is a subsets of $\{1, \ldots, n\}$ then X is also finite
- Now perform induction on k where the inductive step is handled by earlier proposition

Theorem: let $\sigma = \sigma_k \cdots \sigma_1 \in S_n$ be written in disjoint cycle form, then letting $n_i = |\text{supp}(\sigma_i)|$

$$|\sigma| = \text{lcm}(n_i : i \leq k)$$

(i.e. lowest common multiple of the non-trivial orbit sizes)

Proof: given $m \in \mathbb{Z}$ then since disjoint cycles commute we have

$$\sigma^m = \sigma_k^m \circ \cdots \circ \sigma_1^m$$

- The order of each σ_i is n_i, so if m is a common multiple of each n_i, then $\sigma^m = \text{id}_n$
- Conversely, if m was not a multiple of some n_i then $\sigma_i^m \neq \text{id}_n$ which results in

$$\sigma^m(x) = (\sigma_k^m \cdots \sigma_1^m)(x) \neq x$$

- Thus it follows that for any $x \in \text{supp}(\sigma_i)$ that $\sigma^m(x) \neq x$

Example:

- What are the possible orders of elements of S_8?
  - we know that $|\sigma| = \text{lcm}(n_i : i \leq k)$ and need $\sum_{i \leq k} n_i \leq 8$ so the possible orders are

$$8, 7, 6, 5, 15, 10, 4, 12, 3, 6, 2, 1$$

- How many elements in S_4 have order 4?
  - We have 4 ways to partition 8 such that $\text{lcm}(n_i : i \leq k) = 4$

$$4+4 \qquad 4+2+2 \qquad 4+2+1+1 \qquad 4+1+1+1$$

  - Now we count the number of cycles of length k we have

$$\text{cycle}(n, k) := \frac{n!}{(n-k)!k}$$

    * there are $n(n-1)\cdots(n-k+1) = \frac{n!}{(n-k)!}$ partial lists of length k in list of length n
    * partial list is ordered tuple and don't want choosing unordered subsets: $\binom{n}{k} = \frac{n!}{(n-k)!k!}$
    * we want to preserve order but allow rotations to represent the same element

$$(1234) = (2341) = (3412) = (4123)$$

    so there are k ordered tuples that represent the same cycle and $\frac{n!}{(n-k)!k}$

- Using this we can count:
  - $4+4$: 4-cycles picking order does not matter

$$\frac{\frac{8\cdot7\cdot6\cdot4}{4}\cdot\frac{4\cdot3\cdot2\cdot1}{4}}{2} = 1260$$

  - $4+2+2$: 2-cycles picking order does not matter

$$\frac{\frac{8\cdot7\cdot6\cdot4}{4}\cdot\frac{4\cdot3}{2}\cdot\frac{4\cdot3}{2}}{2} = 1260$$

  - $4+2+1+1$: 2520
  - $4+1+1+1+1$: 420
- As a result we conclude that S_8 contains exactly $1260+1260+420+5460$ elements of order 4

Fact: every $\sigma \in S_n$ can be written as a product of 2 cycles (cycles of length 2)

- However unlike our disjoint cycle form which is unique, this product is not unique

Proposition: fix $n \in \mathbb{N}\backslash\{0\}$. If $\mathrm{id}_n = \alpha_r \cdots \alpha_1$ with each α_i a 2-cycle, then r is even

Proof: we will prove by induction on r (TODO)

Corollary: for any $\alpha \in S_n$ if $\sigma = \alpha_r \cdots \alpha_1 = \beta_s \cdots \beta_1$ where the α_i and β_j are 2-cycles then

$$r \equiv s \bmod 2$$

Proof: $\beta_1 \cdots \beta_s \alpha_r \cdots \alpha_1 = \mathrm{id}_n$ so $r+s$ is even (the inverse of a 2-cycle is itself)

Alternating Groups

Definition: *alternating group* A_n is a subgroup of S_n which is defined as

$$A_n := \{\sigma \in S_n : \sigma \text{ can be written with an } \textit{even} \text{ number of 2-cycles}\}$$

Proposition: if $\sigma \in S_n$ and $\sigma = \sigma_k \circ \cdots \circ \sigma_1$ is the disjoint cycle form. Let $n_i = |\mathrm{supp}(\sigma_i)|$ then

$$\sigma \text{ even} \iff (n_1 + \cdots + n_k) - k \text{ even}$$

Proof: each n_i-cycle can be written as a product of $(n_i - 1)$-many 2-cycles, i.e.

$$(a_1 \cdots a_{n_i}) = (a_1 a_2)(a_2 a_3) \cdots (a_{n_i-1} a_{n_i})$$

Thus σ can be written as a product of $(n_1 + \cdots + n_k) - k$ 2-cycles

Proposition: for every $n \geq 2$

$$|A_n| = \frac{n!}{2} = \frac{|S_n|}{2}$$

Proof: fix some 2-cycle $g \in S_n$ then consider $\lambda_g : S_n \to S_n$ given by $\lambda_g(h) = gh$ which is a bijection.

- If $h \in A_n$ then $gh \notin A_n$
- If $h \notin A_n$ then $gh \in A_n$
- Hence $\lambda_g[A_n] = S_n \backslash A_n$ (set subtraction) and since λ_g is a bijection we must have $|A_n| = |S_n \backslash A_n|$

$$|S_n| = |A_n| + |S_n \backslash A_n| = 2|A_n| \quad \Longrightarrow \quad |A_n| = |S_n|/2$$

Cayley's Theorem

Theorem (*Cayley's Theorem*): for any group G, there is a set X and subgroup $H \leq \mathrm{Sym}(X)$ with $G \cong H$

- In fact, we can take $X = G$

Proof: for each $g \in G$, let $\lambda_g : G \to G$ be defined via $\lambda_g(h) = gh$.

- We know that $\lambda_y \in \mathrm{Sym}(G)$ so define

$$\lambda : G \to \mathrm{Sym}(G) \quad \text{via } \lambda(g) = \lambda_g$$

- To see that λ is injective, fix $g \neq h \in G$ and consider λ_g and λ_h on input 1_G

$$\lambda_g(1_G) = g \quad \text{and} \quad \lambda_h(1_G) = h \quad \Longrightarrow \quad \lambda_g \neq \lambda_h$$

- To see that λ repects group ops, fix $g, h \in G$ and consider $\lambda_g \circ \lambda_h$ and λ_{gh}, fix some $k \in G$ then

$$\lambda_g \circ \lambda_h(k) = \lambda_g(hk) = ghk \qquad \lambda_{gh}(k) = ghk$$

  as a result

$$\lambda_g \circ \lambda_h = \lambda_{gh}$$

For "isomorphic to subgroup of" it suffices to find injection $G \to \mathrm{Sym}(X)$ which respects group operations

Automorphisms, Conjugation, Normality, Cosets

Automorphisms

Definition: let G be group, an *automorphism* of G is an isomorphism from G to itself.

- Let $\mathrm{Aut}(G) \subseteq \mathrm{Sym}(G)$ denote the collection of automorphisms of G
- For every group, the identity map $\mathrm{id}_G : G \to G$ is an automorphism, hence $\mathrm{Aut}(G) \neq \emptyset$

Proposition: for any group G, $\mathrm{Aut}(G) \leq \mathrm{Sym}(G)$ is a subgroup

Proof: we know that $\mathrm{id}_G \in \mathrm{Aut}(G)$

- Also recall that the composition of two isomorphisms is also an isomorphism
  - so the composition of two automorphisms is also an automorphism (monoid)
- In addition, the inverse of an isomorphism is also isomorphic
  - so the inverse of an automorphism is an automorphism (group)

Example: the map $\sigma : \mathbb{Z} \to \mathbb{Z}$ is given by $\sigma(n) = -n$ is an automorphsim of $\mathbb{Z}$

- An isomorphism must send generators to generators so 1 must go to either 1 or -1

Propostion: $\mathrm{Aut}(\mathbb{Z}_n) \cong \mathbb{U}_n$

Proof: let $\sigma \in \mathrm{Aut}(\mathbb{Z}_n)$

- Notice that if we can find $\sigma(1) = a$ then this information completely determines σ by

$$\sigma(k) = \sigma(k \cdot 1) = k \cdot \sigma(1) = a \cdot k$$

  - σ just becomes a multiplication by a
- Define $\sigma_a : \mathbb{Z}_n \to \mathbb{Z}_n$ via the mapping $\sigma_a(k) = a \cdot k$
- Every element of $\mathrm{Aut}(\mathbb{Z}_n)$ has the form σ_a for some $a \in \mathbb{Z}_n$
- Find find that the mapping σ_a is bijective iff $\gcd(a, n) = 1$ (i.e. if $a \in \mathbb{U}_n$) so

$$\mathrm{Aut}(\mathbb{Z}_n) = \{\sigma_a :\in \mathbb{U}_n\}$$

- Now we check that this is isomorphic to $\mathbb{U}_n$ by considering the map $\psi : \mathbb{U}_n \to \mathrm{Aut}(\mathbb{Z}_n)$ given by

$$\psi(a) = \sigma_a$$

- We find that for $a, b \in \mathbb{U}_n$ we have

$$\psi(ab) = \sigma_{ab} = \sigma_a \circ \sigma_b = \psi(a) \circ \psi(b)$$

Conjugation

Definition: fix a group G, given $g \in G$ we define $\phi_g : G \to G$ via $\phi_g(x) := {}^g x = gxg^{-1}$

- We call $\phi_g(x) = gxg^{-1}$ the left *conjugate* of x by g
- We saw similar notation of conjugate $x^g = g^{-1}xg$ which is more-or-less equivalent to ${}^g x = gxg^{-1}$
- The intuition for this is the action of x viewed in the perspective of g

Proposition: let G be a group then $\phi_g \in \mathrm{Aut}(G)$

Proof: first note that $\phi_{g^{-1}}$ is a 2-sided inverse of ϕ_g, showing that ϕ_g is bijective. Now fix $x, y \in G$ then

$$\phi_g(xy) = gxyg^{-1} = gx(g^{-1}g)yg^{-1} = \phi_g(x) \cdot \phi_g(y)$$

Definition: given a group G we call $\psi \in \mathrm{Aut}(G)$ an *inner automorphism* if there is $g \in G$ with $\psi = \phi_g$

$$\mathrm{Inn}(G) := \{\phi_g : g \in G\} \subseteq \mathrm{Aut}(G)$$

denotes the collection of inner automorphisms of G.

Proposition: $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$

Proof: we already know that $\mathrm{Inn}(G) \subseteq \mathrm{Aut}(G)$ so

- Just need to verify that $\mathrm{id}_G = \phi_{1_G}$, that $\phi_g \circ \phi_h = \phi_{gh}$, and that $(\phi_g)^{-1} = \phi_{g^{-1}}$

Homomorphism

Definition: given groups G and H, a map $\psi : G \to H$ is a *homomorphism* if for every $x, y \in G$ we have

$$\psi(x \cdot y) = \psi(x) \cdot \psi(y)$$

- Note that the mapping does not have to be a bijection (or even injection/surjection)
- Every isomorphism is a homomorphism
  - since the definition of a homomorphism is a direct weakening of that of isomorphism

Lemma: let G, H groups and $\psi : G \to H$ be a homomorphism

- Then $\psi(1_G) = 1_H$ and for every $g \in G$ we have $(\psi(g))^{-1} = \psi(g^{-1})$

Proof: for all $g \in G$

$$\psi(g) = \psi(1_G \cdot g) = \psi(1_G) \cdot \psi(g) \quad \Longrightarrow \quad 1_H = \psi(1_G)$$

$$1_H = \psi(1_G) = \psi(g^{-1}g)\psi(g^{-1}) \cdot \psi(g) \quad \Longrightarrow \quad (\psi(g))^{-1} = \psi(g^{-1})$$

Proposition: the map $\phi : G \to \mathrm{Inn}(G)$ is an isomorphism iff $Z(G) = \{1_G\}$

- Recall that the center of a group is the set of group elements that commute with everything
- Furthermore, we have $\phi_g = \phi_h$ iff $g^{-1}h \in Z(G)$

Proof:

- Recall that $\mathrm{Inn}(G) := \{\phi_g : g \in G\}$ where $\phi_g(x) = gxg^{-1}$
- The map $\phi : G \to \mathrm{Inn}(G)$ defined via $\phi(g) = \phi_g$ is a homomorphism since for $g, h \in G$
$$\phi(gh) = \phi_{gh} = \phi_g \circ \phi_h = \phi(g) \circ \phi(h)$$
- We have two cases:
  - suppose $g \in Z(G)$ (g commutes with all elements in G) then given $x \in G$
  $$\phi_g(x) = gxg^{-1} = xgg^{-1} = x$$
  - suppose $g \in G$ with $\phi_g = \mathrm{id}_G$, then for any $x \in G$
  $$x = \phi_g(x) = gxg^{-1} \quad \Longrightarrow \quad gx = xg$$
  since x was arbitrary we have $g \in Z(G)$
- For the furthermore allow $a := g^{-1}h$ for ease of reading
  - if $g^{-1}h \in Z(G)$ then given $x \in G$
  $$\phi_a(x) = aha^{-1} = xaa^{-1} = x \quad \Longrightarrow \quad \phi_a = \mathrm{id}_G$$
  $$\mathrm{id}_G = \phi_a = \phi_{g^{-1}h} = \phi_{g^{-1}} \circ \phi_h \quad \Longrightarrow \quad \phi^g = \phi_h$$
  - if $g^{-1}h \notin Z(G)$ then there is some $x \in G$ with
  $$ax \neq xa \quad \Longrightarrow \quad \phi_a(x) = axa^{-1} \neq xaa^{-1} = x \quad \Longrightarrow \quad \phi_a \neq \mathrm{id}_G$$
  $$\mathrm{id}_G \neq \phi_a = \phi_{g^{-1}h} = \phi_{g^{-1}} \circ \phi_h \quad \Longrightarrow \quad \phi^g \neq \phi_h$$
- If $Z(G)$ is non-trival then ϕ is not an isomorphism as it would not be injective
  - since every $g \in Z(G)$ would correspond to a ϕ_g that equals id_G

Example: for $G = D_8$, understand the map $\phi_8 \to \mathrm{Inn}(D_8)$, we know that
$$\mathrm{Inn}(D_8) = \{\phi_{\mathrm{id}_4},\ \phi_{R_{90}},\ \phi_{R_{180}},\ \phi_{R_{270}},\ \phi_F,\ \phi_{R_{90}\circ F},\ \phi_{R_{180}\circ F},\ \phi_{R_{270}\circ F}\}$$
However this list could have repeated elements

- We have seen that $Z(D_8) = \{\mathrm{id}_4, R_{180} \circ F\}$
- Thus for any $g, h \in D_8$ we have
$$\phi_g = \phi_h \quad \Longleftrightarrow \quad g^{-1}h \in \{\mathrm{id}_4, R_{180} \circ F\} \quad \Longleftrightarrow \quad h \in g \cdot \{\mathrm{id}_4, R_{180} \circ F\}$$
- These possible sets of the form $g \cdot \{\mathrm{id}_4, R_{180} \circ F\}$ are exactly
$$\{\mathrm{id}_4, R_{180} \circ F\},\ \{R_{90}, R_{270} \circ F\},\ \{R_{180}, F\},\ \{R_{270}, R_{90}F\}$$
- Hence $\phi_g = \phi_h$ iff both of g and h belong to the same set among these 4 sets and $|\mathrm{Inn}(D_8)| = 4$

Kernel

Definition: let G, H be groups and $\psi : G \to H$ be a homomorphism

- The *kernel* of ψ is the set
$$\ker(\phi) := \{g \in G : \psi(g) = 1_H\}$$
- e.g. for $\phi : G \to \operatorname{Inn}(G)$ we know that $\ker(\phi) = Z(G)$

Proposition: let G, H be groups and $\psi : G \to H$ be a homomorphism. Then $\ker(\psi) \leq G$ is a subgroup

Proof:

- To see that $\ker(\psi)$ is a semigroup, if $g, h \in \operatorname{Ker}(\psi)$ then
$$\psi(g \cdot h) = \psi(g) \cdot \psi(h) = 1_H \cdot 1_H = 1_G$$
hence $g \cdot h \in \ker(\psi)$
- Note that
$$\psi(1_G) = \psi(1_G \cdot 1_G) = \psi(1_G) \cdot \psi(1_G) \quad \implies \quad 1 = \phi(1_G)$$
hence $1_G \in \operatorname{Ker}(\phi)$
- Now suppose $g \in \ker(\psi)$ then
$$\psi(g^{-1} \cdot g) = 1_H = \psi(g^{-1}) \cdot \psi(g) = \psi(g^{-1}) \quad \to \quad 1_H = \phi(g^{-1})$$
hence $g^{-1} \in \operatorname{Ker}(\phi)$

Normality

Definition: let G be a group. A subgroup $K \leq G$ is called *normal* (in G) if $\forall g \in G$
$$gKg^{-1} = K$$

- If $K \leq G$ is normal we write $K \trianglelefteq G$.
- Note that $gKg^{-1} := \{gxg^{-1} : x \in K\}$
- Warning: $K \trianglelefteq H$ and $H \trianglelefteq G$ do *not* in general imply $K \trianglelefteq G$

Proposition: let $\psi : G \to H$ be a homomorphism, then $\ker(\psi) \trianglelefteq G$

Proof: Let $x \in \ker(\psi)$ and let $g \in G$ then
$$\psi(gxg^{-1}) = \psi(g)\psi(x)\psi(g^{-1}) = \psi(g)\psi(g^{-1}) = 1_H$$
Hence $gxg^{-1} \in \ker(\psi)$ so $\ker(\psi) \trianglelefteq G$

Cosets

Definition: let G be a group and $H \leq G$.

- *Left coset* of H in G is a subset of G of the form $gH = \{gh : h \in H\}$ for some $g \in G$
- *Right coset* of H in G is a subset of G of the form $Hg = \{hg : h \in H\}$ for some $g \in G$

Definition: for $H \leq G$ we also have the *set* of left/right cosets

- $G/H := \{gH : g \in G\}$ denotes the set of left cosets of H in G
- $G/H := \{Hg : g \in G\}$ denotes the set of right cosets of H in G

Let $H \leq G$ and $g \in G$, the following are some basic facts about cosets:

- $g \in gH$ and $g \in Hg$
- $|gH| = |H| = |Hg|$ (due to there existing a bijection between them)
- $(gH)^{-1} := \{k^{-1} : k \in gH\} = Hg^{-1}$ (left coset becomes right coset, and vice versa)
- $H \trianglelefteq G$ iff $gH = Hg$ for every $g \in G$

Example: $G = \mathbb{Z}$ and $H = 5\mathbb{Z}$

- We use additive notation for this group (which by convention means the group is Abelian)
- There are 5 cosets of H in G which are $k + 5\mathbb{Z}$ as k ranges over members of $\mathbb{Z}_5$
  - $g = 0$ then $5\mathbb{Z} = \{n \in \mathbb{Z} : n \equiv 0 \bmod 5\}$
  - $g = 1$ then $1 + 5\mathbb{Z} = \{n \in \mathbb{Z} : n \equiv 1 \bmod 5\}$
  - $g = 2$ then $2 + 5\mathbb{Z} = \{n \in \mathbb{Z} : n \equiv 2 \bmod 5\}$
  - $g = 3$ then $3 + 5\mathbb{Z} = \{n \in \mathbb{Z} : n \equiv 3 \bmod 5\}$
  - $g = 4$ then $4 + 5\mathbb{Z} = \{n \in \mathbb{Z} : n \equiv 4 \bmod 5\}$

Lemma: if $g, k \in G$ a group with $H \leq G$ and $k \in gH$ then $kH = gH$ (similarly for right cosets)

Proof: since as $k \in gH$ we find $h \in H$ with $k = gh$ then

$$k = gh \quad \implies \quad kH = ghH = g(hH) \subseteq gH$$

$$g = kh^{-1} \quad \implies \quad gH = kh^{-1}H = k(h^{-1}H) \subseteq kH$$

Then using that $kH \subseteq gH$ and $gH \subseteq kH$ we have $kH = gH$ as expected.

Example: choosing $G = \mathbb{Z}_8$ and subgroup $H = \{0, 4\}$

- The cosets G/H are $\{0, 4\}$, $\{1, 5\}$, $\{2, 6\}$, $\{3, 7\}$

Example: choosing $G = D_8$ and subgroup $H = Z(D_8) = \{\mathrm{id}_4, R_{180} \circ F\}$

- Since $H \trianglelefteq G$ the left and right cosets are = right cosets
$$\{\mathrm{id}_4, R_{180} \circ F\}, \quad \{R_{90}, R_{270} \circ F\}, \quad \{R_{180}, F\}, \quad \{R_{270}, R_{90} \circ F\}$$
once we see all the elements of G we are basically done

Proposition: suppose G a group, $H \leq G$, and $g, k \in G$.

- Then either $gH = kH$ or $gH \cap kH = \emptyset$ (similar for right cosets)

Proof:

- Fix $x \in gH \cap kH$, then there are $h_1, h_1 \in H$ with
$$x = gh_0 = kh_1$$
  - since $k = gh_0h_1^{-1}$ we have $kH \subseteq gH$
  - since $g = gh_1h_0^{-1}$ we have $gH \subseteq kH$
- As a result we get $gH = kH$ whenever $gH \cap kH \neq \emptyset$

Lagrange's Theorem

Definition: let G be a group and $H \leq G$. The *index* of H in G is the number of left cosets of H in G
$$|G : H| := |G/H|$$

Theorem (*Lagrange's Theorem*): Let G be a *finite* group and $H \leq G$. Then $|H|$ divides $|G|$

Proof: we will show that the set of left cosets of H in G *partition* G, and each coset has size $|H|$

- Let G be a finite group with order n and $H \leq G$ be a subgroup
  - notice that $\mathrm{id}_G \in H$
  - if we pick $g \in G$ with $g \notin H$ we can construct gH with
$$H \cap gH = \emptyset$$
since that would require $gh_i = h_j$ for some i, j however
$$gh_1 = h_j \quad \implies \quad g = h_jh_i^{-1} \in H$$
which contradicts that $g \notin H$
  - if we pick another $g' \in G$ with $g' \notin H$ and $g' \notin gH$ we can show that
$$gH \cap g'H = \emptyset$$
since if there is an overlapping element then $gh_i = g'h_j$ for some $i.j$ however
$$gh_i = g'h_j \quad \implies \quad gh_ih_j^{-1} = g' \quad \implies \quad g' \in gH$$
which contradicts that $g' \notin gH$ (similar argument for $H \cap g'H = \emptyset$)

- Repeating this we get a non-overlapping set of left cosets

$$\{H,\ g_1H,\ g_2H,\ \dots,\ g_nH\}$$

  notice that this set is just G/H

  - the definition of $G/H = \{gH : g \in G\}$ has repeating elements
- Each of these cosets have the size $|H|$ so by construction we know G/H partitions G into cosets
- Using the index of H in G as $|G : H| = |G/H|$ we see that

$$|G| = |H| \cdot |G/H|$$

  as a result $|H|$ divides $|G|$

Corollary: $|G : H| = |G/H| = |G|/|H|$

Corollary: for G finite group with $g \in G$ we know $|g| = |\langle g \rangle|$ divides $|G|$ (since $\langle g \rangle \leq G$)

Corollary: groups of prime order are cyclic

Proof: let G have prime order then the only subgroups of G are itself or $\{1_G\}$

- If $G = \{1_G\}$ then cyclic
- Otherwise picking any $g \neq 1_G$ leads to $\langle g \rangle = G$
  - since $|\langle g \rangle|$ must divide $|G|$ which is prime
  - while $g \neq 1_G$ so $|\langle g \rangle| \neq 1$ so $|\langle g \rangle| = p$ and G is cyclic

Corollary: for any finite group G and $g \in G$, $g^{|G|} = 1_G$

Proof: order of g divides order of G so $|G| = q|g|$ for some $q \in \mathbb{N}$ then

$$g^{|G|} = g^{|g| \cdot q} = (g^{|g|})^q = 1_G^q = 1_G$$

Corollary (*Fermat's Little Theorem*): for every integer $a \in \mathbb{Z}$ and prime p

$$a^p \equiv a \bmod p$$

Proof: we may write $a = qp + r$ for some $q \in \mathbb{Z}$ and $r \in \mathbb{Z}_p$

- If $r = 0$ then $a^p \equiv a \equiv 0 \bmod p$
- If $r \neq 0$ then $r \in \mathbb{U}_p = \mathbb{Z}_p \backslash \{0\}$ (since when p prime, $\mathbb{U}_p$ has a order of $p - 1$) then

$$a^p \equiv r^p \equiv (r^{p-1})r \equiv 1 \cdot r \equiv r \equiv a \bmod p$$

  since $r^{p-1} = r^{|\mathbb{U}_p|} = 1$

Example: converse of Lagrange's theorem is not true in general

- Consider A_4 and since $|S_4| = 4!$ we have $|A_4| = |S_4|/2 = 12$
- We will show that A_4 has no subgroup of order 6
- The elements of A_4
  - id_4
  - 2 2-cycles:
  $$\frac{\frac{4\cdot3}{2}\cdot\frac{2\cdot1}{2}}{2} = 3$$
  - 3-cycle:
  $$\frac{4\cdot3\cdot2}{3} = 8$$
- If there is a subgroup $H \leq A_4$ with $|H| = 6$ it would need to contain at least 2 3-cycle elements
- Fix $a \in A_4$ with $|a| = 3$ then ...

Orbit-Stabilizer Theorem

Definition: let G be a group and $g \in G$ then

$$\mathrm{Stab}_G(g) := \{g \in G : g(x) = x\}$$

Example: for $G = S_6$ and $H = \mathrm{Stab}_G(1)$ what is G/H

- Consider some left coset gH, if $h \in H$ then $gh(1) = g(1)$
- Conversely, suppose $g, k \in G$ satisfy $g(1) = k(1) = \ell$ for some $\ell \leq 6$ then
  $$g^{-1}k(1) = g^{-1}(\ell) = 1 \quad\implies\quad g^{-1}k \in H \quad\implies\quad k \in gH$$
  as a result $hK = gH$
- So left cosets of H in G are exactly sets of the form
  $$\{g \in S_6 : g(1) = \ell\} \quad \text{for } \ell \in \{1, \dots, 6\}$$

Theorem (*Orbit-Stabilizer Theorem*): let X be a set, $G \leq \mathrm{Sym}(X)$ then for $x \in X$

$$|G| = |O_G(x)| \cdot |\mathrm{Stab}_G(x)|$$

Proof: we know that $|G|/|H| = |G/H|$ so it suffices to find a bijection from G/H to $O_G(x)$

- $g, h \in G$ belongs the same left H-coset iff $g(x) = h(x)$
- Thus the map $F : G/H \to O_G(x)$ given by $f(gH) = g(x)$ is well-defined and injective

- f is a bijction since if $O_G(x)$ then $\exists g \in G$ with $g(x) = y$ so $f(gH) = g(x) = y$

Theorem: let G be a group. let $H, K \leq G$ be finite subgroups, then $|HK| = \{hk : h \in H, k \in K\}$

- Then $|HK| = |H| \cdot |K| / |H \cap K|$
- While HK may not be a group the $H \cap K$ is always a subgroup

Proof: form the cartesian product $H \times K$ (as sets) and the map $\pi : H \times K \to HK$ given by $\pi(h, k) = hk$

- π is surjective and we claim that π is $|H \cap K|$-to-1
- Fix some $x = hk \in HK$ for every $t \in H \cap K$ then also $x = (ht)(t^{-1}k)$
- So if we have one way of representing x then we have $|H \cap K|$ other ways
- So $|\pi^{-1}(\{x\})| \geq |H \cap T|$
- Conversely, if $x = h'k'$ for some $h' \in H$ and $k' \in K$ then

$$x = hk = h'k' \implies (k')^{-1}(k')^{-1}hk = 1_G \implies (h')^{-1}h = h'k^{-1} \in H \cap K$$

- set $t = h^{-1}(h') = k(k')^{-1}$ then $h' = ht$ and $k' = t^{-1}k$

Theorem: if G a group and H, K are subgroups of G with at least one normal in G then

$$HK \leq G$$

Proof: suppose wlog that H is normal to G then $HK = KH$ (which can be used to prove subgroup)

- show that $\text{id}_G \in HK$ and that HK is closed under composition and inverses
- the fact that $HK = KH$ is used to show closed under inverses

Example: given a group of order $2p$, $p > 2$ prime we have two groups of order $2p$

$$\mathbb{Z}_{2p} \qquad D_{2p}$$

Theorem: up to isomorphism, these are the only groups of order $2p$

Proof: let G be a group of order $2p$

- If $\exists g \in G$ with $|g| = 2p$ then $G \cong \mathbb{Z}_{2p}$
- Otherwise $\forall g \in G$ we have $|g| \neq 2p$
  - first a bit about D_{2p} generated by a rotation r of order p and a flip of order 2
  - Then $F \circ r = r^{p-1} \circ F$
- claim: G has an element of order p
  - In particular $\forall g \in G$ $g = g^{-1}$ hence

$$gh = (gh)^{-1} = h^{-1}g^{-1} = hg$$

so G is abelian and any $g + h \in G \backslash \{1_G\}$ generate the subgroup

$$\{1_G, g, h, gh\}$$

and nothing else (since closed under inverses $g = g^{-1}$, closed under product since everything has order 2)

  - However this contradicts Lagrange's theorem since $4 \nmid 2p$
  - Thus there is an element of p

- Fix $r \in G$ with $|r| = p$ let $F \notin \langle r \rangle$
  - If p then $|\langle r \rangle \cdot \langle F \rangle| = |\langle r \rangle| \cdot |\langle F \rangle| / |\langle r \rangle \cap \langle F \rangle| = p \cdot p/1 = p^2 > 2p$
  - as the only proper subgroup of $< F >$ is of order p or 1 because Lagrange
  - so $|F| = 2$ and now consider $r \cdot F$ as

$$r \cdot F \notin \langle r \rangle, \ |rF| = 2$$

so $(rF)^{-1} = rF$ but also $F^{-1} \circ r^{-1} = F \circ r^{p-1}$

  - so $r \cdot F = F \cdot r^{p-1}$ then if a group has this then it is isomoriphic to the dihedral group

Products

Definition: let G and H be groups their *direct product* is defined as

$$G \times H = \{(g, h) : g \in G, h \in H\}$$

- With two elements from $G \times H$ we have

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2)$$

- Textbook uses notation $G \oplus H$ but they are the same if working with finitely many groups.

Example: direct products are useful for creating new groups

- Cyclic groups: for positive integers m, n then

$$\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn} \qquad \Longleftrightarrow \qquad \gcd(m, n) = 1$$

- Unit groups: given positive integers m, n with $\gcd(m, n)$ then

$$\mathbb{U}_{mn} \cong \mathbb{U}_m \times \mathbb{U}_n$$

- Permutation groups: if X, Y disjoint sets, $G \leq \mathrm{Sym}(X)$ and $H \leq \mathrm{Sym}(Y)$ then

$$G \times H \text{ is isomorphic to a subgroup of } \mathrm{Sym}(X \cup Y)$$

Direct Products of Cyclic Groups

Warmup: groups of order 6: there are only two $S_3 = D_6$ and $\mathbb{Z}_6$

$$\mathbb{Z}_3 \times \mathbb{Z}_2 \cong \mathbb{Z}_6$$

$(1, 1)$ has order 6:

$$(1,1),\ (2,0),\ (0,1),\ (1,0),\ (2,1),\ (0,0)$$

Given positive integers m, n can try the same thing for $\mathbb{Z}_n \times \mathbb{Z}_n$: is $(1, 1)$ a generator?

Theorem: $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic iff $\gcd(m, n) = 1$

Proof: first note that for any k, m, n and any $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$

$$k \cdot (a, b) = (ka, kb)$$

so if both $n \mid k$ and $m \mid k$ then (a, b) has order of most k. In particular

$$|(a, b)| \leq \mathrm{lcm}(n, m) = \frac{nm}{\gcd(n, m)}$$

- so if $\gcd(m, n) \neq 1$ then no element of $\mathbb{Z}_m \times \mathbb{Z}_n$ has order mn
- if $\gcd(m, n) = 1$ then $(1, 1)$ has order exactly m, n (exercise)

by calegy's theorem every group can be represented as a subgroup of a permutation group

Let X, Y be disjoint sets $G \leq \text{Sym}(X)$ and $H \leq \text{Sym}(Y)$

Claim: $G \times H$ is isomorphic to a subgroup of $\text{Sym}(X \cup Y)$

Proof (*sketch*):

- we just need a injective homomorphim from $G \times H$ to $\text{Sym}(X \cup Y)$
- we can just take for $(a, b) \in G \times H$ that since they are disjoint they just do their own thing (since they are disjoint) as an element of $\text{Sym}(X \cup Y)$

Unit groups: given positive integers m, n with $\gcd(m, n) = 1$ we have

$$\mathbb{U}_{mn} \cong \mathbb{U}_m \times \mathbb{U}_n$$

idea:

$$\psi : \mathbb{U}_{mn} \to \mathbb{U}_m \times \mathbb{U}_n$$

via $\phi(x) = (x \mod m, x \mod n)$ (exercise, or just check the book)

Gauss's Theorem

Theorem (*Gauss*):

- $\mathbb{U}_2 \cong \mathbb{Z}_1$
- $\mathbb{U}_{2^n} \cong \mathbb{Z}_{2^{n-2}} \times \mathbb{Z}_2$ for $n \geq 2$
- $\mathbb{U}_{p^n} \cong \mathbb{Z}_{p^n - p^{n-1}}$ for odd p prime and $n \geq 1$

Isomorphism of Products

Given group G and subgroups $H, K \leq G$ when do we have $G \cong H \times K$?

Necessary conditions:

- $G = HK$
- $H \cap K = \{1_G\}$ (we cannot have repeats in $H \times K$???)
- elements of H commute with elements of K

$$(h, 1_K) \cdot (1_H, k) = (h, k) = (1_H, k) \cdot (h, 1_K)$$

- In particular, both H, K are normal subgroups of G

  $$(h, k)(H \times \{1_K\})(h^{-1}, k^{-1}) = hHh^{-1} \times \{kk^{-1}\} = H \times \{1_K\}$$

  same for the reverse

these are actually also the sufficient conditions

Theorem: let G be a group and $H, K \trianglelefteq G$ are normal subgroups of G s.t. $G = HK$ and $H \cup K = \{1_G\}$ then $G \cong H \times K$

Factor Maps

Recall that $\psi : G \to H$ is a homomorhpism (map that repects group ops), then

$$\ker(\psi) := \{g \in G : \psi(g) = 1_H\} \trianglelefteq G$$

it turns out that every normal subgroup is the kernel of some homomorphism.

Lemma: G a group and $K \trianglelefteq G$ then for any $g, h \in G$,

$$gKhK = ghK$$

Proof: $g(Kh)K = g(hK)K = ghK$ since K is normal so left and right cosets are the same

Definition: G a group and $K \trianglelefteq G$ define a binary op on G/K via for $g, h \in G$

$$(gK) \cdot (hK) = ghK$$

Example: $G = \mathbb{Z}, K = 5\mathbb{Z}$, then

$$G/K = \{n + 5\mathbb{Z} : n \in \mathbb{Z}_5\}$$

given $a, b \in \mathbb{Z}$ then

$$\begin{aligned}(a + 5\mathbb{Z}) + (b + 5\mathbb{Z}) &= (a + b) + 5\mathbb{Z} \\ &= (a + b \bmod 5) + 5\mathbb{Z}\end{aligned}$$

Theorem: the binary operation from the previous definition is a group operation

Proof: we first mention that since multiplication on G is associative, also the binary operation on G/K is associative (exercise) so we at least have a semigroup

- if $gK \in G/K$ then
$$K \cdot gK = gK \cdot K = gK$$
so $K = 1_{G/K}$ is a 2-sided id
- also $(gK)(g^{-1}K) = (g^{-1}K)(gK) = K$ so gK has 2-sided inverse

Theorem: G a group and $K \trianglelefteq G$ then the map $\pi_K : G \to G/K$ given by

$$\pi_K(g) = gK$$

is a surjective hom with kernel K

Proof: given $g, h \in G$

$$\begin{aligned}\pi_K(gh) &= ghK = gK \cdot hK \\ &= \pi_K(g)\pi_K(h)\end{aligned}$$

- if $k \in K$ then $\pi_K(k) = kK = K$
- if $g \notin K$ then $\pi_K(g) = gK \neq K$ so
$$\ker(\pi_K) = K$$

Let G, H be groups and $\psi : G \to h$ be a homomorphism

Fact: $\mathrm{Im}(\psi) \leq H$ a subgroup (exercise)

$$\mathrm{Im}(\psi) = \{\psi(g) : g \in G\}$$

Let $K = \ker(\psi)$, last time we produced a specific group G/K and homomorphism $\pi_K : G \to G/K$ with kernel K

First Isomorphism Theorem

Theorem (*First Isomorphism Theorem*): let $\psi : G \to H$ be a homomorphism then

$$G/\mathrm{Ker}(\psi) \cong H$$

Proof: assume ψ is surjective, i.e. $H = \mathrm{Im}(\psi)$ and let $K = \mathrm{Ker}(\psi)$

- Let $\sigma : G/\mathrm{Ker}(\psi) \to H$ be defined by
  $$\sigma(gK) = \psi(g)$$
  - to check that σ is well defined suppose $k \in K$ then for $g \in G$
  $$\sigma(gkK) = \psi(gk) = \psi(g) \cdot \psi(k) = \psi(g) \cdot 1_H = \psi(g)$$
- Check σ is a bijection, as ψ is a surjection, so is σ

  suppose $g_0, g_1 \in G$ are such that
  $$\sigma(g_0K) = \sigma(g_1K) \iff \psi(g_0) = \psi(g_1) \iff \psi(g_0^{-1}g_1) = 1_H$$
  i.e. $g_0^{-1}g_1 \in K$, this happens iff $g_0K = g_1K$ so σ injective
- σ respects group ops: let $g_0K, g_1K \in G/K$ then
  $$\sigma(g_0K \cdot g_1K) = \sigma(g_0g_1K) = \psi(g_0g_1) = \psi(g_0 \cdot \psi(g_1) = \sigma(g_0K) \cdot \sigma(g_1K)$$

Example: let $\psi : \mathbb{Z} \to \mathbb{Z}_n$ be the homomorphism given by $\psi(m) = m \bmod n$. ψ is surjective

$$\ker(\psi) = n\mathbb{Z}$$

so $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ (so they are the same up to isomorphism)

Example: let $\psi : S_n \to \mathbb{Z}_2$ be given by

$$\psi(g) = \begin{cases} 0 & \text{if } g \in A_n \\ 1 & \text{if } g \notin A_n \end{cases}$$

ψ is a homomorphism (exercise) and $\mathrm{Ker}(\psi) = A_n$ so $S_n/A_n \cong \mathbb{Z}_2$

Example: consider D_8, let $K \trianglelefteq D_8$ be the subgroup of rotations.

$$|D_8/K| = 2 \quad \text{so} \quad D_8/K = \mathbb{Z}_2$$

we are basically just forgetting all the rotations so the only thing we remember is if we flip the square or not

Recall given groups $K \leq G$ that the index of K in G is

$$|G : K| := |G/K|$$

Prop: let G be a group and $K \leq G$ on index 2 subgroup, then $K \trianglelefteq G$

Proof: fix $g \in G$

- if $g \in K$ then $gK = Kg$
- if $g \notin K$ then $gK = \{g \in G : g \notin K\}$ and also $Kg = \{g \in G : g \notin K\}$ so $gK = Kg$

Definition: let $H \leq G$, the *normalizer* of H in G is the set $\{g \in G : gHg^{-1} = H\} = N_G(H)$

exercise: $N_G(H) \leq G$ and $H \trianglelefteq N_G(H)$

Prop:

$$C_G(H) = \{g \in G : \forall h \in H \ ghg^{-1} = h\} \trianglelefteq N_G(H)$$

furthermore

$$N_G(H)/C_G(H) \cong \text{a subgroup of } \text{Aut}(H)$$

Remark: this is just a *subgroup veroisn* of the result

$$G/Z(G) \cong \text{Im}(G) \trianglelefteq \text{Aut}(G)$$

Proof: define $\psi : N_G(H) \to \text{Aut}(H)$ to be given by $\psi(g) = \phi_g$ where we recall that $\psi_g(h) = ghg^{-1}$

- this a homomorphism (easy to show)
- the kernel of ψ is $C_G(H)$ (exercise)
- then by First Iso Theorem (FIT) we are done

Last week: (first isomorphim theorem) if $\psi : G \to H$ is a surjective homomorphism and $K = \ker(\psi)$ then $H \cong G/K$

Normalizer

Definition: the *normalizer* of $H \leq G$ is the set

$$N_G(H) := \{g \in G : gHg^{-1} = H\}$$

Lemma: $N_G(H) \leq G$ and that $C_G(H) \trianglelefteq N_G(H)$

Proof: TODO

Theorem (*Normalizer-Centralizer Theorem*): if $H \leq G$ then

- There exists a homomorphism $\psi : N_G(H) \to \mathrm{Aut}(H)$ with $\ker(\psi) = C_G(H)$
- So we get $C_G(H) \trianglelefteq N_G(H)$ and

$$N_G(H)/C_G(H) \cong \text{some subgroup of } \mathrm{Aut}(H)$$

Proof: recall that $C_G(H) := \{g \in G : \forall h \in H,\ ghg^{-1} = h\}$ TODO

Example: every group of order $35 = 5 \times 7$ is cyclic

Proof: assume G is not cyclic (no element of order 35) towards a contradiction

- Begin by noting that every non-id group element has order 5 or 7 (by Lagrange)
- The number of elements $g \in G$ with order 5 is a multiple of $\phi(5) = 4$
  - Since $4 \nmid 34$ we cannot have element of order 5
- Similarly $\phi(7) = 6$ is not a multiple of 34 so we cannot have every element of order 7
- Thus G has non-identity elements of both possible orders
- Let $H \leq G$ have order 7 (subgroup generated by taking an element of order 7)
  - If $K \leq G$ is a different subgroup of order 7 then we have

    $$|HK| = |H| \cdot |K|/|H \cap K| = 49$$

    as a result H is the *unique* subgroup of order 7
  - We have $H \trianglelefteq G$, i.e. $N_G(H) = G$, since H is cyclic and also

    $$H \leq C_G(H) \leq G$$

    since $|C_G(H)|$ divides 35 we have $C_G(H) = H$ or G
    * we know that H is the only subgroup of order 7 and gHg^{-1} is of order 7 so $gHg^{-1} = H$
- if $C_G(H) = G$ (every group element communates with elements of H) then take any non-id $h \in H$ and any $k \in G$ of order 5 (which must exist) and since h and k commute $|hk| = 35$ (wtf is this theorem, why do we need commute), which contradictions assumption that G is not cyclic
- otherwise if $C_G(H) = H$ then $N_G(H)/C_G(H)$ (normalizer mod centeralizer) has order 5 but by the normalizer-cenetralizer theorem (NC theorem) this is isomorphic to a subgroup of $\mathrm{Aut}(H)$ and $\mathrm{Aut}(H) \cong \mathbb{U}_7$ which is a group of size 6
  - so somehow we have found that a group of order 5 is isomorphic to a subgroup of a group(???) with an order of 6, so contradiciton!

Finite Abelian Groups

Theorem (*Fundamental Theorem of Finite Abelian Groups*): let G be an Abelian group with

$$|G| = p_1^{n_1} \cdots p_k^{n_k}$$

where p_i's are prime and n_i are positive integers then

- $G \cong G_1 \oplus \cdots \oplus G_k$ where each G_i is cyclic and $|G_i| = p_i^{n_i}$
- The direct sum is unique up to rearranging and each G_i is unique up to isomorphism

Theorem (IDK): a finite Abelian group is isomorphic to a direct product of cyclic groups of prime-power order, where this decomposition is unique up to the order in which the factors are written

Proof: split up this to be proved into two parts *later*

Example: all Abelian groups of order 16 up to isomorphism

$$\mathbb{Z}_{16} \qquad \mathbb{Z}_4 \oplus \mathbb{Z}_4 \qquad \mathbb{Z}_2 \oplus \mathbb{Z}_8 \qquad \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4 \qquad \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

The Fundamental theorem of Finite Abelian Groups is actually saying every finite Abelian group G is isomorphic to a direct product of cyclic groups of the form

$$\mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_n^{\alpha_n}}$$

where p_i's are primes but are not necessarily distinct (is each $G_i \cong \mathbb{Z}_p$???)

Corollary: if G is a finite Abelian group of order n and $d \mid n$ then $\exists H \leq G$ with $|H| = d$

- The converse of Lagrange's theorem holds
- Easy to show from the Fundamental Theorem (Corollary 8 in notes)
- Also recall that any subgroup of a cyclic group is also cyclic

distinctness of the stuff in example: let p be a prime and let $n_1, \ldots, n_k, m$ be positive integers, then how many elements of order p^m are there in $\mathbb{Z}_{p^{n_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{n_k}}$? (where $n_1 \leq n_2 \leq \cdots n_k$)

- If $m > n_k$ then none (as we are looking at the lcm of the orders of the stuff)
- let $p \in \mathbb{Z}_{p^{n_k}}$ has order p^{n_k}, then so does $(0, 0, \ldots, g) = \bar{g}$ let $H\langle \bar{g} \rangle$
  - then $G/H \cong \mathbb{Z}_{p^{n_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{n_{k-1}}}$
  - inductively suppose we know the number of elements of every possible order in G/H

Example $G = \mathbb{Z}_8 \oplus \mathbb{Z}_9$, $H = \{0\} \oplus \mathbb{Z}_8$ then G/H has 4 elements of order 8, 1 of order 2, or 2 elements of order 4, 1 of order 1(???)

so taking these and adding another coordinate with an element of $\mathbb{Z}_8$

- order 8: 48
- order 4: 12
- order 2: 3
- order 1: 1

Monday: Finite Abelian groups

Theorem: let G be a finite Abelian group then G is isomorphic to a direct-product of cyclic groups each with prime power order. Furthermore, this decomposition is unique.

to start, focus on the case where $|G| = p^N$ for some prime p and $N \geq 1$

If $G_1, \ldots, G_n$ have orders $p^{m_1}, \ldots, p^{m_n}$ resp. how mnay elements of each possible order are there?

Example:

- consider $\mathbb{Z}_{25}$ the possible orders are $1, 5, 25$
  - 1 elements of order 1
  - 4 elements of order 5 (???)
  - 20 elements of order 25 (???)
- equvalently we can say that we have
  - 1 elements of order at most 1
  - 5 elements of order at most 5
  - 25 elements of order at most 25
- more generally, in $\mathbb{Z}_{p^N}$ given $1 \leq k \leq N$ there are exactly p^k-many elements of order *at most* p^k, namely the mutliples of $p^{N-k} \in \mathbb{Z}_{p^N}$

Proposition: fix a prime p and integers $m_1 \geq \cdots m_n \geq 1$ for the group

$$G = \mathbb{Z}_{p^{m_1}} \times \cdots \times \mathbb{Z}_{p^{m_n}}$$

given $k \geq 1$

- let $j \leq n$ be the largest with $m_j \geq k$ (if j exists or $j = 0$ when j does not exist).
- Then G has exactly $(p^{jk} \cdot p^{m_{j+1}} \cdots p^{m_n})$-many elements of order at most p^k

Proof: recall that given groups $G_1, \ldots, G_n$ and $g_i \in G$ for $i \leq n$ the order of $(g_1, \ldots, g_n) \in G_1 \times \cdots \times G_n$ is just the lcm of order of $g_i \in G$.

- if $G_i = \mathbb{Z}_{p^{m_i}}$ then $(g_1, \ldots, g_n)$ has order $\leq p^k$ iff each g_i the formula now follows

Proposotion: fix p a prime and integers $m_1 \geq \cdots \geq m_n \geq 1$ and $a_1 \geq \cdots \geq a_\ell \geq 1$ write

$$G = \mathbb{Z}_{p^{m_1}} \times \cdots \times \mathbb{Z}_{p^{m_n}} \qquad H = \mathbb{Z}_{p^{a_1}} \times \cdots \times \mathbb{Z}_{p^{a_\ell}}$$

then $G \cong H$ iff $(m_1, \ldots, m_n) = (a_1, \ldots, a_\ell)$

Proof: obvious when equal, assume $(m_1, \ldots, m_n) \neq (a_1, \ldots, a_\ell)$

- if $|G| \neq |H|$ they cannot be isomorphic
- so let us assume $m_1 + \cdots + m_n = a_1 + \cdots + a_\ell$. let $j \geq 1$ be least with $m_j \neq a_n$ (note that $j \leq \min\{n, \ell\}$) and assume $m_j < a_j$ WLOG
- now consider in G and in H the number of elements of order at most p^{m_j}
  - In G, this number is exactly $p^{j \cdot m_j} \cdot p^{m_{j+1}} \cdots p^{m_n}$
  - In H, this number is at most $p^{j \cdot m_j} \cdot p^{a_{j+1}} \cdots p^{a_\ell}$
- since $m_{j+1} + \cdots + m_n > a_{j+1} + \cdots a_\ell$ (since $m_j < a_j$) we conclude that $G \ncong H$

now work towards existance part of main thm, i.e. G can be written as a production of cyclic groups.

Lemma: say G Abelian of order p^n with p prime and $n \geq 1$. If $a \in G$ has max possible order, then $G \cong \langle a \rangle \times K$ for some $K \leq G$ (where K could be written as a cyclic group)

Proof:

- if $n = 1$, then G is cyclic and we are done $G \cong G \times \{1\}$ (iso to itself direct product the trival subgroup) (since every group of prime order is cyclic)
- Now assume the propositio nis true for groups of order p^k for $k < n$. fix $a \in G$ of max possible order, say $|a| = p^m$ for some $m \leq n$. Might as well take $m < n$.
- Now choose a $b \notin \langle a \rangle$ (note that b cannot be identity) of least possible order
- claim: $\langle a \rangle \cap \langle b \rangle = \{1_G\}$
  - as $|b^p| = |b|/p$ we have $b^p \in \langle a \rangle$
  - say $b^p = a^i$ now $1_G = b^{p^m} = (a^i)^{p^{m-1}}$ so $|a^i| \leq p^{m-1}$
  - so $i = pj$ for some integer j
  - let $c = a^{-j}b$, we have $c \notin \langle a \rangle$ since $b \notin \langle a \rangle$
- so $c^p = a^{-jp}b^p = a^{-i}b^p = 1_G$ so $|c| = p$ hence $|b| = p$ and $\langle a \rangle \cap \langle b \rangle = \{1_G\}$
  - if there is a non-trival intersection then b must entirely intersect a due to the choice of b (???)
- Now form $\bar{G} = G/\langle b \rangle$. given $x \in G$ write $\bar{x}$ for $x\langle b \rangle$
- note that $|\bar{a}| = p^m$ since if $\bar{a}^{p^{m-1}} = 1_G$, i.e. $a^{p^{m-1}} \in \langle b \rangle$, i.e. $a^{p^{m-1}} = 1_G$, contradiction (we assume that $|a| = p^m$)
- so $\bar{a}$ as max possible order in $\bar{G}$
- by induction $\bar{G} \cong \langle \bar{a} \rangle \times \bar{k}$. we set
$$K = \{a \in G : \bar{x} \in \bar{K}\}$$
  where $\bar{x} = x\langle b \rangle$ (we claim this works but still need to check)

exercise: we claim $G = \langle a \rangle \cdot K$ and $\langle a \rangle \cap K = \{1_G\}$

Theorem (*Abelian case of Cauchy's theorem*): if G is a finite Abelian group and $p \mid |G|$ then G contains an element of order p

Proof: induction on $|G|$

- base case: for groups of size 1 there is nothing to show

- inductive hypo: let $|G| = n > 1$ and asssume this result holds for all finite Abelian group of order $< n$
- inductive step: fix $g \in G, g \neq 1_G$ we may assume that $p \nmid |g|$ (otherwise we are done?)
  - write $H = \langle g \rangle$ (noting that $p \nmid |H|$) then G/H is a smaller finite Abelian group with $p \mid |G/H|$
  - by induction, we may find $aH \in G/H$ with order p in G/H then $p > 1$ is least with $a^p \in H$
  - in particular $|a|$ in G is a multiple of p
    - suppose $a^{mp+r} = 1_G$ then $1_G \in a^r H \implies a^r \in H$ but r is too small (need to be at least p) so contradiction and must be multiple

Theorem (*Fundamental Theorem of Finite Abelian Groups*): if G is a finite Abelian group and

$$|G| = p_1^{n_1} \cdots p_k^{n_k}$$

with every p_i prime and $n_i \geq 1$ then

1. $G \cong G_1 \times \cdots \times G_k$ where all $|G_i| = p_i^{n_1}$ with all G_i are cyclic
2. This decomposition of G into cyclic groups of prime-power order is unique

Proof:

- **Lemma**: G a finite Abelian group of order $p^n \cdot m$ where p is prime, $n \geq 1$, and $p \nmid m$
  - then letting $H = \{g \in G : g^{p^n} = 1_G\}$ (g's order is a divides p^n???) and $K = \{g \in G : g^m = 1_G\}$ then

$$G \cong H \times K \quad \text{and} \quad |H| = p^n$$

- **Proof**: as G is Abelian, $H, K \leq G$. we need to check $H \cap K = \{1_G\}$ and $G = HK$
  - if $a \in H \cap K$ then $|a|$ divides p^n and $|a|$ divides m, since p^n and m are relatively prime hence $|a| = 1$ so $a = 1_G$
  - fix $a \in G$ as $\gcd(m, p^n) = 1$ by Bezoit's theorem we can find integers s, t with

$$sm + tp^n = 1$$

    then $a = a^{sm} \cdot a^{tp^n}$ and we note that $(a^{sm})^{p^n} = 1_G$ and simularly $(a^{tp^n})^m = 1_G$ hence $a^{sm} \in H$ and $a^{tp^n} \in K$ so $a \in HK$ and $G \cong H \times K$
- to see that $|H| = p^n$ we have $|G| = |H| \cdot |K| / |H \cap K| = |H| \cdot |K|$
  - towards a contradiction, suppose $p \mid |K|$ and by Abelian Cauchy theorem there exists $g \in K$ of order p, by definition of K this is not possible

Cor (converse to Lagrange's theorem for finite Abelian groups): if G is a finite Abelain group and m is a positive integer with $m \mid |G|$ then $\exists$ a subgroup $H \leq G$ with $|H| = m$

Proof (sketch): by the theroem if enough to show that this corollary holds for finite cyclic groups

- e.g. $G = \mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}_9$ how to create $H \leq G$ of order 6?

$$H = \mathbb{Z}_2 \times \{0\} \times 3\mathbb{Z}_3$$

$$H = \{0\} \times 4\mathbb{Z}_2 \times 3\mathbb{Z}_3$$

  there will be some counting problems of this type

Group Actions

Groups were invented to capture how they *act* on other mathematical objects such as sets, vector spaces, topological spaces, combinatorial objects, etc.

Definition: let G a group and X a set, an *group action* of G on X is a map $\alpha : G \times X \to X$ satisfying:

1. $\forall x \in X, \;\; \alpha(1_G, x) = x$
2. $\forall x \in X$ and $\forall g, h \in G, \;\; \alpha(gh, x) = \alpha(g, \alpha(h, x))$

Notation: often if the action $\alpha : G \times X \to X$ is understood by context we just omit it:

1. $\forall x \in X, \;\; 1_G \cdot x = x$
2. $\forall x \in X$ and $\forall g, h \in G, \;\; (gh)x = g(hx)$

Examples:

1. G acts on $X = G$ by left multiplication:
$$\alpha(g, h) = gh$$
2. G acts on $X = G$ by right multiplication:
$$\alpha(g, h) = hg^{-1}$$
this is $\alpha : G \times G/H \to G/H$
3. if X is a set and $G \leq \mathrm{Sym}(X)$ then G acts on X by *application*
$$\alpha(g, x) = g(x)$$
this leads to manyy natural examples of actions (we claim that all actions are just this in disjuise)
   - if V a vector space and
   $$G = \mathrm{Aut}(V) = GL(V)$$
   GL is the general linear group (the set of all groups that perserve V???)
   - if (X, d) is a metric space and $G = \mathrm{Iso}(X)$

exercise: verify the above

- G acts on $X = G$ by conjugation
$$\alpha(g, h) = ghg^{-1}$$
- if $H \leq G$, G acts on $X = G/H$ by left mult
$$\alpha(g_0, g_1H) = g_0g_1H$$

Proposition: let G be a group and X a set. There is a 1-1 correspondence between

- Actions of G on X
- Homomorphisms from G to $\mathrm{Sym}(X)$

Proof: produce a bijective mapping between actions and hom to prove 1-1 correspondence

- let $\alpha : G \times X \to X$ be an action. We define $\bar{\alpha} : G \to \mathrm{Sym}(X)$ via $\bar{\alpha}(g)(x) = \alpha(g, x)$
- now to check that $\bar{\alpha}$ *looks like* a hom

$$\begin{aligned}
(\bar{\alpha}(g) \circ \bar{\alpha}(h))(x) &= \bar{\alpha}(g)(\bar{\alpha}(h)(x)) \\
&= \bar{\alpha}(g)(\alpha(h, x)) \\
&= \alpha(g, \alpha(h, x)) \\
&= \alpha(gh, x) && \text{(Prop 2 of actions)} \\
&= \bar{\alpha}(gh, x)
\end{aligned}$$

- now check that $\bar{\alpha}(g) \in \mathrm{Sym}(X)$. we note that

$$\begin{aligned}
\bar{\alpha}(g) \circ \bar{\alpha}(g^{-1}) &= \bar{\alpha}(g^{-1}) \circ \bar{\alpha}(g) \\
&= \bar{\alpha}(1_G) && \text{(Prop 1 of actions)} \\
&= \mathrm{id}_X
\end{aligned}$$

- Now suppose $\beta : G \to \mathrm{Sym}(X)$ is a hom. We define $\hat{\beta} : G \times X \to X$ via

$$\hat{\beta}(g, x) = \beta(g)(x)$$

- check that $\hat{\beta}$ is an action
  - if $x \in X$ then
  $$\hat{\beta}(1_G, x) = \beta(1_G)(x) = \mathrm{id}_X(x) = x$$
  - Given $g, h \in G, x \in X$
  $$\begin{aligned}
  \hat{\beta}(gh, x) &= \beta(gh)(x) \\
  &= (\beta(g) \cdot \beta(h))(x) \\
  &= \beta(g)(\beta(h)(x)) \\
  &= \hat{\beta}(g, \hat{\beta}(h, x))
  \end{aligned}$$

  exercise: check $\hat{\bar{\alpha}} = \alpha$ and $\bar{\hat{\beta}} = \beta$

now we can re-use the terminology about subgroups of $\mathrm{Sym}(X)$ when discussing actions, i.e.

- if $\alpha : G \times X \to X$ is an action and $x \in X$ then the α-orbit of x is

$$\{\alpha(g, x) : g \in G\}$$

- and the α-stabilizer of $x \in x$ is

$$\{g \in G : \alpha(g, x) = x\} = \mathrm{Stab}_{\alpha}(x)$$

  if α is understood we can omit the subscripts

Example:

- let $G = D_8 \leq S_4$ (symmetrices of a square) (note that S_4 is permutations of 4 points)
  - let $C = \{r, b\}$ and $X =$ functions from $\{1, 2, 3, 4\}$ to C
  - i.e. coloring a square's vertices with red and blue
  - given $x \in X$ and $g \in D_8$ set
    $$(g \cdot x)(i) = x(g^{-1}(i))$$
    if $g = R_{90}$ then
    $$(g \cdot x)(1) = x(g^{-1}(x)) = x(4) = b$$
    $$(g \cdot x)(2) = x(g^{-1}(2)) = x(1) = r$$
    see jul 19 10:11 am for better view of example
  - how many orbits? jul 19 10:15 am
    * drop down to 6 equivalence classes

forming new actions from old ones

- set of colorings:
  - If $\alpha : G \times X \to X$ is an action and C is a set of colors
  - We obtain a new action of G on C^X (set of C colorings of X) via $(g \cdot f)(x) = f(g^{-1} \cdot x)$
  - picture jul 21 9:38pm
- let $G = S_n$, fix some $1 \leq k \leq n$
  - then $X = [n]^k = k$-element subsets of $\{1, \ldots, n\}$
  - G acts on X in the obvious way, i.e. $g \cdot x = g[x]$
    * notice that rather than sending a single element we send a set of points???
  - for every k there is only one orbit
  - we can use the orbit-stabilizer theorem: if $\alpha : G \times X \to X$ is an actoin then $\forall x \in X$
    $$|G| = |O_\alpha(x)| \cdot |\text{Stab}_\alpha(x)|$$
    * when $G = S_n$ then $X = [n]^k$ and $|G| = n!$
    * given $x \in [n]^k$ then $|\text{Stab}_\alpha(x)| = k!(n-k)!$ (ways to permute our subset x without mixing points in x with those outside x)
    * so we get $|O_\alpha(x)| = n!/(k!(n-k)!) = \binom{n}{k} = |X|$

Polya-Burnside

Definition: if G a group, X a set, and $\alpha G \times X \to X$ an action then given $g \in G$

$$\text{fix}_\alpha(g) = \{x \in X : gx = x\}$$

Theorem (*Polya-Burnside*): let G a finite group, X a set, and $\alpha : G \times X \to X$ a action then

$$|\mathcal{O}_\alpha| = \frac{1}{|G|} \sum_{g \in G} |\mathrm{fix}_\alpha(g)|$$

where $\mathcal{O}_\alpha$ is set of orbits

Proof: consider the set

$$Y = \{(g, x) : g \in G, x \in \mathrm{fix}_\alpha(g)\}$$

We will count Y in two different ways

- Method 1: consider $g \in G$, we obtain

$$|Y| = \sum_{g \in G} |\mathrm{fix}_\alpha(g)|$$

- Method 2: consider $x \in X$ (this means that $g \in \mathrm{Stab}_\alpha(x)$)

$$\begin{aligned} |Y| &= \sum_{x \in X} |\mathrm{Stab}_\alpha(x)| \\ &= \sum_{A \in \mathcal{O}_\alpha} \left(\sum_{x \in A} |\mathrm{Stab}_\alpha(x)| \right) \end{aligned}$$

- For any $A \in \mathcal{O}_\alpha$ we recall that if $x, y \in A$ then

$$|\mathrm{Stab}_\alpha(x)| = |\mathrm{Stab}_\alpha(y)|$$

- So by the Orbit-Stablizer theorem for any $x \in A$

$$\sum_{x \in A} |\mathrm{Stab}_\alpha(x)| = |A| \cdot |\mathrm{Stab}_\alpha(x)| = |G|$$

- So now

  $$|Y| = |\mathcal{O}_\alpha| \cdot |G|$$

  hence

  $$|\mathcal{O}_\alpha| = \frac{1}{|G|} \sum_{g \in G} |\mathrm{fix}_\alpha(g)|$$

Example: $\{R, B, G\}$-colorings of $\{1, 2, 3, 4\}$ under D_8

- $X =$ colorings then $|X| = 81$
- $|\mathrm{fix}_\alpha(\mathrm{id}_4)| = 81$
- $|\mathrm{fix}_\alpha(R_{90})| = |\mathrm{fix}_\alpha(R_{270})| = 3$
  - as soon as we color two vertices differently we they get swapped by the rotation
- $|\mathrm{fix}_\alpha(R_{180})| = 9$
- $|\mathrm{fix}_\alpha(F)| = 9$
- $|\mathrm{fix}_\alpha(R_{90} \circ F)| = 27$

- $|\text{fix}_\alpha(R_{180} \circ F)| = 9$
- $|\text{fix}_\alpha(R_{270} \circ F)| = 27$
- then summing all the fix and dividing by size of group we get

$$168/8 = 21 \text{ orbits}$$

Last time: Polya Burnshide theorem: if G is a finite group and $\alpha : G \times X \to X$ is an action, then

$$|\mathcal{O}_\alpha| = \frac{1}{|G|} \sum_{g \in G} |\text{fix}_\alpha(g)|$$

Example:

- Given a circular tray with 6 holds and 2 colors of beads to place in the holes, how many different configs up to rotation of the tray
  - up to rotation: if we make a config then all the rotations of that config are considered the same config
  - our graph here provides the rotations: $\mathbb{Z}_6$
  - $\mathbb{Z}_6$ acts on itslf by left addition $\rightsquigarrow$ $\mathbb{Z}_6$ acts on $\{R, B\}^{\mathbb{Z}_6}$ (assign each point of $\mathbb{Z}_6$ a R or B) where given $m, n \in \mathbb{Z}_6$ and $\chi \in \{R, B\}^{\mathbb{Z}_6}$ then

    $$(m \cdot \chi)(n) = \chi(-m + n)$$

    (the action is written multiplicalitively and remember when converting to group element we get the inverse)
  - Apply PB: count $\text{fix}_\alpha(m)$ for each $m \in \mathbb{Z}_6$
    * how big is $\{R, B\}^{\mathbb{Z}_6}$? it is $2^6 = 64$ so

      $$|\text{fix}_\alpha(0)| = 64$$

    * then if we apply the action 1 how many configurations don't change? only all R or all B

      $$|\text{fix}_\alpha(1)| = 2$$

    * for rotations by 2 clicks we look at the cycles that are created (we see it creates 2 3-cycles)

      $$|\text{fix}_\alpha(2)| = 4$$

    * for rotations by 3 clicks we get 3 2-cycles so

      $$|\text{fix}_\alpha(3)| = 8$$

    * $\cdots$

      $$|\text{fix}_\alpha(4)| = 4$$

      $$|\text{fix}_\alpha(5)| = 2$$

now by PB we have

$$|\mathcal{O}_\alpha| = \frac{1}{6}\sum_{m<6} |\text{fix}_\alpha(m)| = \frac{1}{6}(84) = 14$$

there are 14 different configurations up to rotation

- now suppose we are nable to precisely detect color and only know that two holes have different colored beads: e.g. 5 blue 1 red is the same as 5 red 1 blue
  - jul 24 9:56 am
  - identify the ste of colors with $S_2 = \mathbb{Z}_2$ then

    $$\mathbb{Z}_2 \times \mathbb{Z}_6 \text{ acts on } (\mathbb{Z}_2)^{\mathbb{Z}_6}$$

    where given $i \in \mathbb{Z}_2$ and $m, n \in \mathbb{Z}_6$ with $\chi \in (\mathbb{Z}_2)^{\mathbb{Z}_2}$ we set

    $$((i, m) \cdot \chi)(n) = i + \chi(-m + n)$$

  - we will also count this action as α and now begin to count
    * when $i = 0$ we don't swap the colors so

      $$|\text{fix}_\alpha(0, 0)| = 64$$

      $$|\text{fix}_\alpha(0, 1)| = 2$$

      $$|\text{fix}_\alpha(0, 2)| = 4$$

      $$|\text{fix}_\alpha(0, 3)| = 8$$

      $$|\text{fix}_\alpha(0, 4)| = 4$$

      $$|\text{fix}_\alpha(0, 5)| = 2$$

    * when we swap colors how many will get back to where we started

      $$|\text{fix}_\alpha(1, 0)| = 0$$

      (alternating something)

      $$|\text{fix}_\alpha(1, 1)| = 2$$

      $$|\text{fix}_\alpha(1, 2)| = 0$$

      (need oppaciate holes to have oppaciate color)

      $$|\text{fix}_\alpha(1, 3)| = 8$$

      $$|\text{fix}_\alpha(1, 4)| = 0$$

      (symmatry from (1,1)???)

      $$|\text{fix}_\alpha(1, 5)| = 2$$

      where does the symmatry some from??

  - as a reuslt by PB we get

    $$|\mathcal{O}_\alpha| = \frac{1}{12}\sum_{(i,j)\in\mathbb{Z}_2\times\mathbb{Z}_6} |\text{fix}_\alpha(i.j)| = \frac{1}{12}(96) = 6$$

    if we where don't it with 3 colors we use S_3 instead of S_2 which we used here

- How many different ways are there to 3-color the edges of a regular tetrahedron up to symmetries fo a the tetrahedron?

$$\mathrm{Aut}(\text{tetrahedron}) = A_4$$

(hold one point and rotate base gets 3-cycles) (rotate 2 points get 2 2-cycles)

  - $X = \{R, B, G\}^{([4]^2)}$ $3^6 = 729$ what is $[4]^2$ and why does $|[4]^2 = 6|$

$$|\mathrm{fix}_\alpha(\mathrm{id}_4)| = 729$$

  - if we fix one point then we basically create 2 3-cycles for the edges (3 colors for each cycle and $3^2 = 9$)

$$|\mathrm{fix}_\alpha(\text{3-cycle})| = 9$$

  - todo

$$|\mathrm{fix}_\alpha(22 - \text{cycle})| = 81$$

then by PB since $A_4 = |S_4|/2 = 4!/2 = 12$ we have (also there are

$$|\mathcal{O}_\alpha| = \frac{1}{12} \sum_{g \in A_4} |\mathrm{fix}_\alpha(g)| = \frac{1}{12}(729 + 9 \cdot 8 + 81 \cdot 3) = 87$$

since there are $\frac{4 \cdot 3 \cdot 2}{3} = 8$ 3-cycles and $\frac{\frac{4 \cdot 3}{2} \cdot \frac{2 \cdot 1}{2}}{2} = 3$ 2 2-cycles