

MATH 113: Abstract Algebra

Jad Damaj

Spring 2022

Contents

| | | |
|----------|---|-----------|
| 1 | Introduction | 4 |
| 1.1 | January 18 | 4 |
| 1.1.1 | What is Algebra? | 4 |
| 1.1.2 | Set Theory | 4 |
| 1.1.3 | Maps/Functions | 5 |
| 1.1.4 | Equivalence Relations | 6 |
| 1.1.5 | Properties of the Integers (\mathbb{Z}) | 6 |
| 1.2 | January 20 | 7 |
| 1.2.1 | Properties of the Integers (\mathbb{Z}) | 7 |
| 1.2.2 | Primes | 7 |
| 1.2.3 | Congruences | 8 |
| 2 | Groups | 10 |
| 2.1 | January 20 | 10 |
| 2.1.1 | Groups | 10 |
| 2.2 | January 25 | 10 |
| 2.2.1 | Groups | 10 |
| 2.2.2 | Dihedral Groups | 12 |
| 2.3 | January 27 | 13 |
| 2.3.1 | Dihedral Groups | 13 |
| 2.3.2 | Symmetric Groups | 14 |
| 2.3.3 | Composing $\sigma \circ \tau$ in S_n | 15 |
| 2.4 | February 1 | 15 |
| 2.4.1 | “Maps” between groups | 15 |
| 2.4.2 | Subgroups | 17 |
| 2.5 | February 3 | 18 |
| 2.5.1 | Subgroups | 18 |
| 2.5.2 | Centralizers, Normalizers, and Center | 18 |
| 2.6 | February 8 | 19 |
| 2.6.1 | Cyclic Groups | 19 |
| 2.7 | February 10 | 21 |
| 2.7.1 | Cyclic Groups | 21 |
| 2.7.2 | Subgroups Generated by Subsets of a Group | 21 |
| 2.7.3 | Quotient Groups | 22 |
| 2.8 | February 15 | 23 |
| 2.8.1 | Quotient Groups | 23 |
| 2.9 | February 17 | 24 |

| | | |
|----------|--|-----------|
| 2.9.1 | Quotient Groups | 24 |
| 2.10 | February 22 | 26 |
| 2.10.1 | The Isomorphism Theorems | 26 |
| 2.11 | March 3 | 28 |
| 2.12 | March 8 | 28 |
| 2.12.1 | Group Actions | 28 |
| 2.12.2 | Groups Acting on Themselves ($G = A$) | 28 |
| 2.13 | March 10 | 29 |
| 2.13.1 | Groups Acting on Themselves by Conjugation | 29 |
| 2.13.2 | Groups Acting on Themselves by Conjugation | 30 |
| 2.14 | March 15 | 32 |
| 2.14.1 | Sylow's Theorems | 32 |
| 2.15 | March 17 | 33 |
| 2.16 | March 29 | 33 |
| 2.16.1 | Finitely Generated Abelian Groups | 33 |
| 3 | Rings | 35 |
| 3.1 | March 29 | 35 |
| 3.1.1 | Rings | 35 |
| 3.2 | March 31 | 36 |
| 3.2.1 | Rings | 36 |
| 3.2.2 | Polynomial Rings | 38 |
| 3.3 | April 5 | 38 |
| 3.3.1 | Polynomial Rings | 38 |
| 3.3.2 | Ring Homomorphisms | 39 |
| 3.4 | April 14 | 41 |
| 3.4.1 | Operations with Ideals | 41 |
| 3.4.2 | Properties of Ideals | 41 |

Chapter 1

Introduction

1.1 January 18

1.1.1 What is Algebra?

High School Algebra: Solve equations (over real and complex numbers), precalculus material

Abstract Algebra: Study algebraic structures more general than the real or complex numbers

- The abstract encapsulation of our intuition for composition

Summary of first 6-7 years of math education:

- The notion of unity, eg. 1
- The natural numbers $\mathbb{N} := \{1, 2, 3, \dots\}$ with $+, \times$
- the integers $\mathbb{Z} := \{\dots, -2, -1, 0, 1, 2, \dots\}$ with $+, \times$, additive inverses exist
- the rational numbers $\mathbb{Q} := \{\frac{a}{b} | a, b \in \mathbb{Z}, b \neq 0\}$ with $+, \times$, additive and multiplicative inverses exist
- \mathbb{R} , real numbers
- \mathbb{C} , complex numbers

Adding structure at each step: $(\mathbb{Z}, +)$ - Group, $(\mathbb{Z}, +, \times)$ -Ring, $(\mathbb{Q}, +, \times)$ -Field

Goal of this class: define larger class of objects like this

1.1.2 Set Theory

Definition 1.1.1. A set is a collection of elements
Ex: Numbers, symbols shapes, turkeys

Notation: P, Q are two statements

- $P \rightarrow Q$ means if P is true then Q is true, “ P implies Q ”
- $P \leftrightarrow Q$ “ P is true if and only if Q is true”

- \forall “for all”
- \exists “there exists”, $\exists!$ “there exists unique”

Let S and T be two sets

- if s is an object in S we say s is an element of S or a member of S . Write $s \in S$ if s is in S , $s \notin S$ if s is not in S
- If S has finitely many elements we say it is a finite set. $|S| = \#$ of elements in S (cardinality)

Set notation:

- $S = \{\text{Notation for elements in } S \mid \text{properties specifying being in } S\}$
Ex: $\{x \in \mathbb{Z} \mid 2 \text{ divides } x\}$, $\{1, 2, 3, \dots\}$, $\{1, 2, 3\}$
- If every object in S is also an object in T we say “ S is contained in T ”, $S \subset T$. If S is not contained in T , $S \not\subset T$
- If $S \subset T$ and $T \subset S$, then $S = T$
- The set of objects contained in both S and T is called the intersection, $S \cap T$
- The set of objects contained in either S or T is called the union, $S \cup T$. (If S and T are disjoint $S \sqcup T$)
- $S \times T = \{(a, b) \mid a \in S, b \in T\}$ - Cartesian product of S and T
- The set that contains no objects is called the empty set, \emptyset

1.1.3 Maps/Functions

- $f : A \rightarrow B$ or $A \xrightarrow[f]{B}$ is a map or function. The value of f at a is denoted $f(a)$
- If specifying a function on elements, $f : a \mapsto b$ or $a \mapsto b$
- A is called the domain of f . B is called the codomain of f .
Ex: $S = \mathbb{N}, T = \mathbb{N} \quad f : \mathbb{N} \rightarrow \mathbb{N} \quad a \mapsto a^2$
- We say f is well defined if $a_1 = a_2 \rightarrow f(a_1) = f(a_2) \quad \forall a_1, a_2 \in A$
- The set $f(A) = \{b \in B \mid b = f(a) \text{ for some } a \in A\}$ is a subset of B called the range or image of f
- The set $f^{-1}(C) = \{a \in A \mid f(a) \in C\}$ is called the preimage of C under f ($C \subset B$)
- We say f is injective if $f(x) = f(y) \rightarrow x = y \quad \forall x, y \in A$
- We say f is surjective if given $b \in B \quad \exists a \in A$ such that $f(a) = b$
- We say f is bijective if it is both injective and surjective
- We say that f is the identity map if $A = B$ and $f(a) = a \quad \forall a \in A$. In this case we write $f = \text{Id}_A$
- if $f : A \rightarrow B$ and $g : B \rightarrow C$, the composite map $fg : A \rightarrow C$ is defined by $(gf)(a) = g(f(a))$

1.1.4 Equivalence Relations

Let A be a nonempty set. A binary relation on a set A is a subset R of $A \times A$ and we write $a \equiv b$ if $(a, b) \in R$.

We say \sim is an equivalence relation if \sim is:

- reflexive: $a \sim a \ \forall a \in A$
- symmetric: $a \sim b \rightarrow b \sim a \ \forall a, b \in A$
- transitive: $a \sim b$ and $b \sim c \rightarrow a \sim c \ \forall a, b, c \in A$

If \sim defines an equivalence relation on A , then the equivalence class of $a \in A$ is defined to be $[a] = \{x \in A \mid x \sim a\}$.

Example 1.1.2. Consider the binary relation on $\mathbb{Z} \times \mathbb{Z}$ given by $(x, y) \in R$ if $2 \mid x - y$. We will show \sim is an equivalence relation:

reflexiveness: $x - x = 0$ so $2 \mid 0 = x - x$ for all $x \in \mathbb{Z}$

symmetricness: Suppose $2 \mid x - y$. Since $(x - y) = -(y - x)$, $2 \mid y - x$ for all $x, y \in \mathbb{Z}$

transitivity: If $2 \mid x - y$ and $2 \mid y - z$ then $2 \mid x - y + y - z$ so $2 \mid x - z$

So \sim is an equivalence relation

Remark 1.1.3. The reflexive property, implies that $x \in [x]$ so equivalence classes are nonempty and their union is A

What are the equivalence classes for “ $x \sim y$ if and only if $2 \mid x - y$ ”

$$[x] = \{y \in \mathbb{Z} \mid 2 \mid x - y\}$$

- If x is even, $x = 2n$ for some $n \in \mathbb{Z}$ then $2 \mid y - 2n \rightarrow y$ is even so $y = 2m$ for some $m \in \mathbb{Z}$
- If x is odd, $x = 2n + 1$ for some $n \in \mathbb{Z}$ then $2 \mid y - 2n - 1 \rightarrow y$ is odd so $y = 2n + 1$ for some $m \in \mathbb{Z}$

Remark 1.1.4. The symmetric and transitive properties imply that $y \in [x]$ if and only if $[y] = [x]$ so two equivalence classes are either equal or disjoint

1.1.5 Properties of the Integers (\mathbb{Z})

- If $a, b \in \mathbb{Z}$, $a \neq 0$ we say a divides b if there is an element $c \in \mathbb{Z}$ such that $b = ac$. Write $a \mid b$ (if a does not divide b , write $a \nmid b$)
- If $a, b \in \mathbb{Z} \setminus \{0\}$ there is a unique positive integer d , called the greatest common divisor $\gcd(a, b)$, satisfying:
 1. $d \mid a$ and $d \mid b$
 2. If $e \mid a$ and $e \mid b$, then $e \mid d$
- If $a, b \in \mathbb{Z} \setminus \{0\}$ there is a unique positive integer l , called the least common divisor satisfying:
 1. $a \mid l$ and $b \mid l$
 2. If $a \mid m$ and $b \mid m$, then $l \mid m$

1.2 January 20

1.2.1 Properties of the Integers (\mathbb{Z})

The division algorithm: If $a, b \in \mathbb{Z}$ and $b \neq 0$ then there exists unique $q, r \in \mathbb{Z}$ such that $a = qb + r$ and $0 \leq r < |b|$.

- q is the quotient, r is the remainder

Example 1.2.1. For $a = 23, b = 7$ $23 = 7 * 3 + 2$. Here $q = 3, r = 2$

The Euclidean Algorithm: an important procedure which produces the greatest common divisor of two integers a and b by iterating the division algorithm.

If $a, b \in \mathbb{Z} \setminus \{0\}$, we obtain $a = q_0b + r_0$, $b = q_1r_0 + r_1$, $r_0 = q_2r_1 + r_2$, \dots , $r_{n-2} = q_nr_{n-1} + r_n$, $r_{n-1} = q_{n+1}r_n$ where r_n is the last nonzero remainder, $r_n = \gcd(a, b)$

Because of division algorithm, $|b| > |r_0| > |r_1| > \dots > |r_n|$ is a decreasing sequence of strictly positive integers so this cannot continue indefinitely, so r_n exists.

Why is $r_n = \gcd(a, b)$?

Claim: $\gcd(a, b) = \gcd(b, r_0)$

Proof. $r_0 = a - q_0b$ so if $d|b$ and $d|a$, $d|a - q_0b = r_0$

Also $r_0 + q_0b = a$ so if $d|b$ and $d|r_0$, $d|r_0 + q_0b = a$

□

Iterate this to get $r_n = \gcd(r_{n-1}, r_n) = \dots = \gcd(a, b)$

Example 1.2.2. Calculate $\gcd(35, 20)$

$25 = 20 \cdot 1 + 5$, $20 = 15 \cdot 1 + 5$, $15 = 5 \cdot 3 + 0$ so $\gcd(35, 20) = \gcd(15, 5) = 5$

Theorem 1.2.3. Given any $a, b \in \mathbb{Z}$, $\exists u, v \in \mathbb{Z}$ such that $au + bv = \gcd(a, b)$.

Proof. Work backwards through Euclidean Algorithm

Example 1.2.4. Write \gcd from example 2 in terms of 20 and 35.

$20 = 15 \cdot 1 + 5$ so $5 = 20 - 15 \cdot 1$

$15 = 35 - 20 \cdot 1$ so $5 = 20 - (35 - 20)$ so $5 = 20 \cdot 2 - 35 \cdot 1$

1.2.2 Primes

Definition 1.2.5. An integer $p > 1$ is prime if its only positive divisors are 1 and p itself

Lemma 1.2.6. Euclid's Lemma $a, b \in \mathbb{Z}, p$ is primes. If $p|ab$ then $p|a$ or $p|b$.

Remark 1.2.7. Primality is important. $15|3 \cdot 5$ but $15 \nmid 3, 15 \nmid 5$

Proof. If $p \nmid a$ then $\gcd(p, a) = 1$, thus there exists $u, v \in \mathbb{Z}$ such that $au + pv = 1$ but then $b = b(au + pv) = bau + bpv$. By assumption $p|ab$ so $p|bau$ and $p|p$ so $p|bpv$ so $p|bau + bpv$ so $p|b$.

The fundamental Theorem of Arithmetic: if $n \in \mathbb{Z}, n > 1$ then n can be factored uniquely into the product of primes. In other words, there are distinct primes p_1, \dots, p_s and positive integers d_1, \dots, d_s such that $n = p_1^{d_1} p_2^{d_2} \cdots p_s^{d_s}$. Such a factorization is unique up to ordering.

Theorem 1.2.8. There are infinitely many primes

Proof. Suppose not, then there are finitely many primes, p_1, \dots, p_n . Consider $p_1 \cdots p_n + 1$ by FTA there is a prime factorization so at least one prime divides it. Can't be p_1, \dots, p_n so must be prime not listed.

1.2.3 Congruences

Fix $m \in \mathbb{N}$, by division algorithm, for $a \in \mathbb{Z}$, there exists unique q, r such that $a = qm + r$ and $0 \leq r < m$. We call r the remainder of a modulo m .

This gives a natural equivalence relation on \mathbb{Z} : $a \sim b \leftrightarrow a$ and b have the same remainder modulo $m \leftrightarrow m|(a-b)$

Definition 1.2.9. a and b are congruent modulo $m \leftrightarrow m|(a-b)$. We write $a \equiv b \pmod{m}$.

Remark 1.2.10. The equivalence classes of \mathbb{Z} under this relation are indexed by the possible remainders modulo m . We call these residue classes: $\mathbb{Z}/m\mathbb{Z} = \{[0], [1], \dots, [m-1]\}$

- We have a natural surjective map $[\] : \mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z} \quad a \mapsto [a]$

Definition 1.2.11. We define addition and multiplication on $\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$ by $[a] \times [b] = [a \times b] \ \forall a, b \in \mathbb{Z}$ and $[a] + [b] = [a + b] \ \forall a, b \in \mathbb{Z}$

- This doesn't depend on choice of representatives for the class

Proof. Suppose $a_1 \equiv b_1 \pmod{m}$, then $m|a_1 - b_1$ so $a_1 = b_1 + sm$ for $s \in \mathbb{Z}$

Also $a_2 \equiv b_2 \pmod{m}$ so $a_2 = b_2 + tm$ for $t \in \mathbb{Z}$

$(a_1 + a_2) = b_1 + b_2 + (s+t)m$ so $a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$ also $a_1 a_2 = (b_1 + sm)(b_2 + tm) = b_1 b_2 + (b_1 t + b_2 s + stm)m$ so $a_1 a_2 \equiv b_1 b_2 \pmod{m}$ \square

- $[0] \in \mathbb{Z}/m\mathbb{Z}$ behaves like 0 in \mathbb{Z} : $[0] + [a] = [a]$ for $[a] \in \mathbb{Z}/m\mathbb{Z}$
- $[1] \in \mathbb{Z}/m\mathbb{Z}$ behaves like 1 in \mathbb{Z} : $[1] \times [a] = [a]$ for $[a] \in \mathbb{Z}/m\mathbb{Z}$
but $\underbrace{[1] + \cdots + [1]}_{m \text{ times}} = [0]$ and $[r][s] = [rs] = [m] = [0]$ for some r, s

Proposition 1.2.12. For every $m \in \mathbb{N}, a \in \mathbb{Z}$ the congruence $ax \equiv 1 \pmod{m}$ has a solution in \mathbb{Z} if and only if a and m are coprime.

Proof. If a and m are coprime, $\gcd(a, m) = 1$ so $\exists u, v \in \mathbb{Z}$ such that $au + mv = 1$ so $au \equiv 1 \pmod{m}$

Chapter 2

Groups

2.1 January 20

2.1.1 Groups

Definition 2.1.1. Let G be a set. A binary operation is a map of sets $*$: $G \times G \rightarrow G$. Write $a * b$ for $*(a, b)$ for $a, b \in G$ or ab when $*$ is clear.

Definition 2.1.2. A group is a set G with a binary operation $*$ such that the following hold:

1. (Associativity): $(a * b) * c = a * (b * c) \forall a, b, c \in G$
2. (Identity): $\exists e \in G$ such that $a * e = e * a = a \forall a \in G$
3. (Inverses): Given $a \in G$, $\exists b \in G$ such that $a * b = b * a = e$

2.2 January 25

2.2.1 Groups

Example 2.2.1.

- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/n\mathbb{Z}$ under $+$, $e = 0, [0]$, for $a \in G$, $a^{-1} = -a$
- $\mathbb{Q} \setminus \{0\}, \mathbb{R} \setminus \{0\}, \mathbb{C} \setminus \{0\}$, under \times , $e = 1$, $a^{-1} = \frac{1}{a}$

Example 2.2.2 (Non-Example).

$(\mathbb{Z} \setminus \{0\}, \times)$ not group since no inverses.

Example 2.2.3. $\mathbb{Z}/n\mathbb{Z}^\times :=$ elements in $\mathbb{Z}/n\mathbb{Z}$ that have inverses ($[a]$ such that $\gcd(a, n) = 1$). $\mathbb{Z}/n\mathbb{Z}^\times$ is a group.

Example 2.2.4.

- If $(A, *)$ and (B, \diamond) are groups. We can form the group $(A \times B, (*, \diamond))$ where $A \times B = \{(a, b) | a \in A, b \in B\}$ whose operation is defined componentwise $(a_1, b_1)(*, \diamond)(a_2, b_2) = (a_1 * a_2, b_1 \diamond b_2)$

- The trivial group: a set with a single element e , $e * e = e$ is the definition of the binary operation. No choice but to be associative. e is the identity and its own inverse.

A set with a binary operation $*$ is called a monoid if the first two properties of a group hold (no need for inverses.)

Example 2.2.5. (\mathbb{Z}, \times) is a monoid.

- All groups are monoids but not all monoids are groups.

Definition 2.2.6. A group $(G, *)$ is called abelian if it satisfies

$$a * b = b * a \forall a, b \in G \text{ (commutative).}$$

Example 2.2.7. $(\mathbb{Z}, +)$ is an abelian group.

Example 2.2.8. Non Abelian group $= GL_n(\mathbb{R}) := \{M \in M_n(\mathbb{R}) \mid \det(M) \neq 0\}$.

A square matrix has a nonzero determinant iff it is invertible so every element has an inverse under matrix multiplication. Matrix multiplication is associative and we have $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ as the identity matrix. So $\{GL_n(\mathbb{R}), \times\}$ is a group and for $n \geq 2$ is non-abelian.

Proposition 2.2.9. If G is a group under $*$ then,

- 1) The identity of G is unique.
- 2) For each $a \in G$, a^{-1} is uniquely determined.
- 3) $(a^{-1})^{-1} = a$ for all $a \in G$.
- 4) $(a * b)^{-1} = (b^{-1}) * (a^{-1})$.

Proof. 1) If e_1, e_2 are both identities, by axiom of identity $e_1 * e_2 = e_1$, but also $e_1 * e_2 = e_2$ so $e_1 = e_2$.

2) Assume b and c are both inverses of a . Let e be the identity of G . By inverse axiom, $a * b = e$, and $a * c = e$ so $c = c * e$ by identity axiom so $c = c * (a * b) = (c * a) * b$ by associativity axiom so $c = e * b = b$ by identity axiom.

3) To show $(a^{-1})^{-1} = a$ we need to show that a is the inverse of a^{-1} (By (2) the inverse is unique.) Since a^{-1} is the inverse of a , we have $a * a^{-1} = a^{-1} * a = e$ but this is the same as $a^{-1} * a = a * a^{-1} = e$ so a is the inverse of a^{-1} .

4) Let $c = (a * b)^{-1}$, then $(a * b) * c = e$. By associativity, $a * (b * c) = e$. “multiply” by a^{-1} to get $a^{-1} * (a * (b * c)) = a^{-1} * e$ so by the associativity and inverse axioms $(a^{-1} * a) * (b * c) = a^{-1}$ so $e * (b * c) = a^{-1}$ so $b * c = a^{-1}$. Now, “multiply” by b^{-1} to get $b^{-1} * (b * c) = b^{-1} * a^{-1}$ so $(b^{-1} * b) * c = b^{-1} * a^{-1}$ so $e * c = b^{-1} * a^{-1}$ so $c = b^{-1} * a^{-1}$.

Proposition 2.2.10. Let G be a group and $a, b \in G$. The equality $ax = b$ and $ya = b$ have unique solutions for $x, y \in G$. In particular,

- (1) if $au = av$ then $u = v$

(2) if $ub = vb$ then $u = v$

Proof. Existence - multiply by inverses
Uniqueness - because inverses are unique

Definition 2.2.11. For G a group and $x \in G$, the order of x is the smallest positive integer n such that $x^n = 1$ ($:= \underbrace{x * \cdots * x}_{n \text{ times}}$), where 1 is the identity of G . We denote this by $|x|$ and x is said to be of order n . If no positive power of x is 1, then $|x| = \infty$.

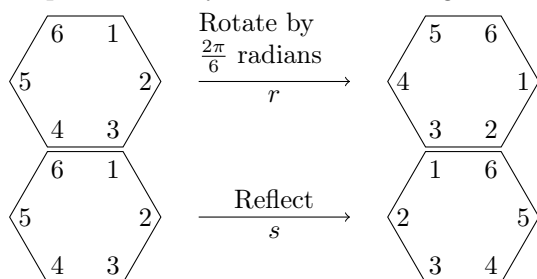
Example 2.2.12.

- Elements of $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ (additive): All nonzero elements have order ∞ .
- $(\mathbb{Z}/9\mathbb{Z}, +) = \{[0], \dots, [8]\}$: $[6] + [6] + [6] = [18] = 0$ so $[6]$ has order 3 in $\mathbb{Z}/9\mathbb{Z}$.

2.2.2 Dihedral Groups

- The elements are symmetries of geometric objects
- Consider regular n -gons for $n \geq 3$

Example 2.2.13. Symmetries of a hexagon:

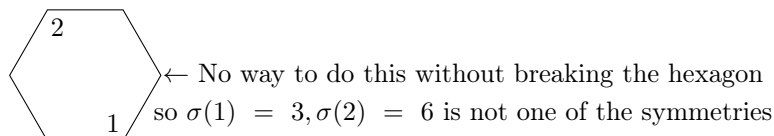


- We describe these symmetries by labeling the vertices

Observe: A symmetry of a hexagon gives you a function $\{1, \dots, 6\} \rightarrow \{1, \dots, 6\}$. if σ is a symmetry, $\sigma(i) = j$ means σ sends i to the place where j used to be.

eg: $r(1) = 2, s(3) = 5$

Note that not every such function gives you a symmetry



Let D_{2n} be the set of symmetries of the n -gon. Define $t_1 t_2$ to be the symmetry reached by applying t_2 then applying t_1 for t_1, t_2 symmetries of the n -gon ($t_1, t_2 \in D_{2n}$). This operation is associative because composition of functions is associative. The identity symmetry is do nothing, denoted by 1. The inverse of a symmetry is to undo the symmetry. Under these operations, D_{2n} is the dihedral group of order $2n$.

Why is $|D_{2n}| = 2n$?

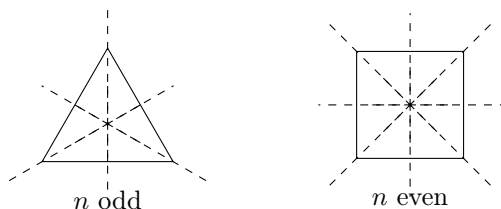
For any vertex i , there is a symmetry that sends 1 to the vertex i . The vertex 2 (next to 1) must go either to the vertex $i+1$ or $i-1$. So you have n choices for where to send the vertex “1” and 2 choices for where to send to vertex “2”. So there are $n \cdot 2$ choices for symmetries of an n -gon. So $|D_{2n}| = 2n$.

2.3 January 27

2.3.1 Dihedral Groups

Explicitly, what are these symmetries?

- n rotations about the center through $2\pi/n$ radians (clockwise)
- n reflections through n lines of symmetry



- If n odd: symmetry lines pass through the vertex, midpoint of opposite side.
- if n even: $n/2$ symmetry lines pass through opposite edges.
 $n/2$ symmetry lines pass through opposite vertices.

Fix Notation:

- r - rotation clockwise about the origin through $2\pi/n$ radians
- s - reflection (through 1 and the origin)

Example 2.3.1. D_{12} $2n = 12$ so $n = 6$

$$(i) \ 1, r(\frac{2\pi}{6}), r^2(\frac{4\pi}{6}), r^3(\pi), r^4(\frac{8\pi}{6}), r^5(\frac{10\pi}{6}), r^6(2\pi) = 1$$

$1, r, \dots, r^5$ all distinct so $|r| = 6$

$$(ii) \ s^2 = 1 \text{ so } |s| = 2$$

$$(iii) \ s \neq r^i \text{ for any } i$$

$$(iv) \ sr^i \neq sr^j \ 0 \leq i, j < 6$$

$$(v) \ r^i \neq sr^j \text{ for any } i, j$$

Thus, $D_{12} = \{1, r, r^2, r^3, r^4, r^5, s, sr, sr^2, sr^3, sr^4, sr^5\}$ all distinct, and there are 12 so this is all the elements.
 $D_{12} = \{r^i s^j | i = 0, \dots, n-1 \ j = 0, 1\}$ or equivalently $D_{12} = \{r, s | r^n = s^2 = 1, rs = sr^{-1}\}$

2.3.2 Symmetric Groups

- Let Ω be a nonempty set and let S_Ω be the set of bijections from Ω to itself (ie. permutations.)
- Let σ, τ be elements of S_Ω , $\sigma : \Omega \rightarrow \Omega$, $\tau : \Omega \rightarrow \Omega$, then $\sigma \circ \tau$ is a bijection $\Omega \rightarrow \Omega$.
- The identity of S_Ω is the permutation 1 defined by $1(a) = a \forall a \in \Omega$.
- Every permutation has an inverse $\sigma^{-1} : \Omega \rightarrow \Omega$ such that $\sigma^{-1}\sigma = \sigma \circ \sigma^{-1} = 1$.
- Composition of functions is associative so \circ is associative.
- Thus, (S_Ω, \circ) is a group called the symmetric group of S_Ω
- Often we will use $\Omega = \{1, \dots, n\}$ - will write S_n instead of S_Ω

Example 2.3.2. $\Omega = \{1, 2, 3\}$

Let σ be in S_Ω sending $\sigma(1) = 2$, $\sigma(2) = 3$, $\sigma(3) = 1$.

$\begin{pmatrix} \sigma : & 1 \rightarrow 2 \\ & 2 \rightarrow 3 \\ & 3 \rightarrow 1 \end{pmatrix}$ We write $(1\ 2\ 3)$ to represent σ .

$\tau \in S_\Omega$ by $\tau(1) = 2$, $\tau(2) = 1$, $\tau(3) = 3$

$\begin{pmatrix} \tau : & 1 \rightarrow 2 \\ & 2 \rightarrow 1 \\ & 3 \rightarrow 3 \end{pmatrix} = (1\ 2)(3)$. Often we will leave out 1 element cycles and write $(1\ 2)$

- A cycle is a string of integers representing an element of S_n which cyclically permutes the integers
- The length of a cycle is the number of integers that appear in it
- Two cycles are disjoint if they have no numbers in common

Example 2.3.3. The Group S_3

| | |
|---|-----------------|
| $\sigma_1(1) = 1, \sigma_1(2) = 2, \sigma_1(3) = 3$ | $1 = (1)(2)(3)$ |
| $\sigma_2(1) = 1, \sigma_2(2) = 3, \sigma_2(3) = 2$ | $(2\ 3)$ |
| $\sigma_3(1) = 3, \sigma_3(2) = 2, \sigma_3(3) = 1$ | $(1\ 3)$ |
| $\sigma_4(1) = 2, \sigma_4(2) = 1, \sigma_4(3) = 3$ | $(1\ 2)$ |
| $\sigma_5(1) = 2, \sigma_5(2) = 3, \sigma_5(3) = 1$ | $(1\ 2\ 3)$ |
| $\sigma_6(1) = 3, \sigma_6(2) = 1, \sigma_6(3) = 2$ | $(1\ 3\ 2)$ |

- For any $\sigma \in S_n$ the cycle decomposition of σ^{-1} is obtained by writing the number sin each cycle of the decomposition of σ in reverse order.

Example 2.3.4. $\sigma = (1\ 12\ 8\ 10\ 4)(2\ 13)(5\ 11\ 7)(6, 9) \in S_{13}$

$\sigma^{-1} = (4\ 10\ 8\ 12\ 1)(13\ 2)(7\ 11\ 5)(9, 6)$

Remark 2.3.5. $(2\ 13) = (13\ 2)$ since they permute cyclically.

More generally, $(a_1\ a_2\ a_3) = (a_3\ a_1\ a_2) = (a_2\ a_3\ a_1)$

By convention, we put the smallest number first.

2.3.3 Composing $\sigma \circ \tau$ in S_n

- Go from right to left

Example 2.3.6. $(1\ 2\ 3) \circ (1\ 2)(3\ 4)$

$\tau : 1 \rightarrow 2$ $\sigma : 2 \rightarrow 1$ so $\sigma \circ \tau : 1 \rightarrow 3$
 $\tau : 3 \rightarrow 4$ $\sigma : 4 \rightarrow 4$ so $\sigma \circ \tau : 4 \rightarrow 4$
 $\tau : 4 \rightarrow 4$ $\sigma : 3 \rightarrow 1$ so $\sigma \circ \tau : 4 \rightarrow 1$
 $\tau : 2 \rightarrow 1$ $\sigma : 1 \rightarrow 2$ so $\sigma \circ \tau : 2 \rightarrow 2$
 so $\sigma \circ \tau = (1\ 3\ 4)$

Remark 2.3.7.

- S_n is non abelian for $n \geq 3$
 ex: $(1\ 2) \circ (1\ 3) = (1\ 3\ 2)$ but $(1\ 3) \circ (1\ 2) = (1\ 2\ 3)$
- The order of a permutation is the lcm of the lengths of the cycles in its decomposition
- A transposition is a cycle of length 2
- The order of S_n is $n!$

2.4 February 1

2.4.1 “Maps” between groups

Definition 2.4.1. Let $(G, *)$ and (H, \diamond) be groups. A map $\varphi : G \rightarrow H$ such that

$$\varphi(x * y) = \varphi(x) \diamond \varphi(y),$$

is called a homomorphism.

Remark 2.4.2. When the group operations are not explicitly written

$$\underbrace{\varphi(xy)}_{\text{“multiplication” in } G} = \underbrace{\varphi(x)\varphi(y)}_{\text{“multiplication in” } H}$$

Think: a map of sets that respects the group structure (is compatible with the group operations.)

Definition 2.4.3. The map $\varphi : G \rightarrow H$ is called an isomorphism (G, H are isomorphic, denoted $G \cong H$) if:

- 1) $\varphi(xy) = \varphi(x)\varphi(y) \quad \forall x, y \in G$
- 2) φ is a bijection

Definition 2.4.4. A homomorphism from a group to itself is called an endomorphism. Further, if an endomorphism is an isomorphism then it is called an automorphism.

Example 2.4.5.

- (1) $\varphi : (\mathbb{Z}, +) \rightarrow (\mathbb{Q}, +)$ by $x \mapsto x$ is a homomorphism since $\varphi(x + y) = x + y = \varphi(x) + \varphi(y)$. It is injective but not surjective so not an isomorphism.
- (2) $\varphi : (\mathbb{Z}, +) \rightarrow (\mathbb{Z}/m\mathbb{Z}, +)$ by $x \mapsto [x]$ is a homomorphism since $\varphi(x + y) = [x + y] = [x] + [y] = \varphi(x) + \varphi(y)$. It is surjective but not injective so not an isomorphism.
- (3) For any group G , the identity map $\varphi : G \rightarrow G$ by $x \mapsto x$ is an isomorphism (also an automorphism.)
- (4) Let $\mathbb{R} := \{x \in \mathbb{R} | x > 0\}$. The exponential map, $\exp : (\mathbb{R}, +) \rightarrow (\mathbb{R}^+, \times)$ by $x \mapsto e^x$ is an isomorphism since $\exp(x + y) = e^{x+y} = e^x e^y = \exp(x) \exp(y)$. Also $\log_e e^x = x$ is an inverse.
- (5) For any group G and any group H , the map $\varphi : G \rightarrow H$ by $g \mapsto e_H$ is called the trivial homomorphism since $\varphi(g_1 g_2) = e_H = e_H e_H = \varphi(g_1) \varphi(g_2)$

Proposition 2.4.6. Let $(G, *)$, (H, \circ) , (M, \square) be three groups. Let $f : G \rightarrow H$ and $g : H \rightarrow M$ be homomorphisms. Then $g \circ f : G \rightarrow M$ is a homomorphism.

Proof. $g(f(x * y)) = g(f(x) \circ f(y)) = g(f(x)) \square g(f(y))$

Proposition 2.4.7. If $\varphi : G \rightarrow H$ is an isomorphism,

- (1) $|G| = |H|$
- (2) G is abelian iff H is abelian
- (3) $\forall x \in G, |x| = |\varphi(x)|$

Proof (Proof of (1) and (2)).

- (1) This is true since a bijection between two sets means they have the same cardinality.
- (2) \rightarrow) Assume G is abelian. Let $x, y \in H$ be arbitrary. Since φ is an isomorphism, there exists $x', y' \in G$ such that $\varphi(x') = x$ and $\varphi(y') = y$. Then $xy = \varphi(x')\varphi(y') = \varphi(x'y')$. Since G is abelian $x'y' = y'x'$ so $xy = \varphi(y'x') = \varphi(y')\varphi(x') = yx$ so H is abelian.
 \leftarrow) Assume H is abelian. Let x, y in G be arbitrary. Consider $\varphi(xy) = \varphi(x)\varphi(y)$. Since H is abelian, $\varphi(xy) = \varphi(y)\varphi(x) = \varphi(yx)$. Since φ is an isomorphism, it is injective so it follows that $xy = yx$. Thus, G is abelian.

Lemma 2.4.8. Let $\varphi : G \rightarrow H$ be a homomorphism then $\varphi(x^n) = \varphi(x)^n \forall n \in \mathbb{Z}$.

Proof. To show this for all nonnegative integers we will proceed by induction.

Basis: $\varphi(x^0) = \varphi(e_G) = e_H = \varphi(x)^0$. We will show this below.

Induction: Assume $\varphi(x^n) = \varphi(x)^n$. Then, $\varphi(x^{n+1}) = \varphi(x^n)\varphi(x) = \varphi(x)^n\varphi(x) = \varphi(x)^{n+1}$.

To show this for negative integers we claim that $\varphi(x^{-1}) = \varphi(x)^{-1}$. To see this observe that

$$\varphi(x)\varphi(x^{-1}) = \varphi(xx^{-1}) = \varphi(e_G) = e_H = \varphi(e_G) = \varphi(x^{-1}x) = \varphi(x^{-1})\varphi(x)$$

Also note that $(x^n)^{-1} = x^{-n}$ so by the above induction we have $\varphi(x^{-n})\varphi(x)^n = \varphi(x^{-n}x^n) = e_H = \varphi(x^n x^{-n}) = \varphi(x)^n \varphi(x^{-n})$ so $\varphi(x^{-n}) = (\varphi(x)^n)^{-1} = \varphi(x)^{-n}$.

Fact: If $\varphi : G \rightarrow H$ is an homomorphism, $\varphi(e_G) = e_H$.

Proof. $e_G e_G = e_G$ so $\varphi(e_G e_G) = \varphi(e_G)$ so $\varphi(e_G)\varphi(e_G) = \varphi(e_G)$. Multiplying both sides by $\varphi(e_G)^{-1}$ yields $\varphi(e_G)^{-1}\varphi(e_G)\varphi(e_G) = \varphi(e_G)^{-1}\varphi(e_G)$ so $e_H\varphi(e_G) = e_H$ so $\varphi(e_G) = e_H$. \square

Proof (Proof of (3)). Suppose $|\varphi(x)| = \infty$, $|x| = n < \infty$, then $\varphi(x)^n = \varphi(x^n) = \varphi(e_G) = e_H$ so $|\varphi(x)| \leq n < \infty$ which is a contradiction.

Similarly if $|x| = \infty$, $|\varphi(x)| = n < \infty$, then $\varphi(x^n) = \varphi(x)^n = e_H = \varphi(e_G)$. Since φ is an isomorphism, φ is injective so $x^n = e_G$ so $|x| \leq n < \infty$ which is a contradiction.

This implies that $|x|$ and $|\varphi(x)|$ must both be finite or infinite. If they are both infinite we are done so suppose $|x| = n$, $|\varphi(x)| = m$.

Then $\varphi(x)^n = \varphi(x^n) = \varphi(e_G) = e_H$ so $m \leq n$.

Also, $\varphi(e_G) = e_H = \varphi(x)^m = \varphi(x^m)$ so $e_H = x^m$ and $m \leq n$.

Thus $m = n$

Example 2.4.9.

- Consider S_3 and $\mathbb{Z}/6\mathbb{Z}$. These groups are not isomorphic since S_3 is non-abelian and $\mathbb{Z}/6\mathbb{Z}$ is.
- $D_6 \cong S_3$. $D_5 = \{r, s, |r^3 = s^2 = 1, rs = sr^{-1}\}$ so sending $a = (1\ 2\ 3) \mapsto r$ and $b = (1\ 2) \mapsto s$, we see that $a^3 = b^2 = 1$ and $ba = a^{-1}b$ so the group generated by a and b is isomorphic to D_6 . Finally, since a and b generate S_3 , $S_3 \cong D_6$.

2.4.2 Subgroups

Definition 2.4.10. Let $(G, *)$ be a group. A subgroup H of G is a subset $H \subseteq G$ such that:

1. $e \in H$
2. if $x, y \in H$, $x * y \in H$
3. if $x \in H$, $x^{-1} \in H$

Think: A subgroup H of $(G, *)$ is a subset of G that is a group under the same operation.

Example 2.4.11.

- 1) $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Q}, +)$
- 2) $(\mathbb{Q}, +)$ is a subgroup of $(\mathbb{R}, +)$
- 3) $(\mathbb{Q} \setminus \{0\}, \times)$ is a subgroup of $(\mathbb{R} \setminus \{0\}, \times)$
- 4) If G is a group then $H = G$ and $H = \{e\}$ are both subgroups of G .
- 5) If $m \in \mathbb{Z}$, the subset $m\mathbb{Z} = \{ma | a \in \mathbb{Z}\}$ is a subgroup of $(\mathbb{Z}, +)$

2.5 February 3

2.5.1 Subgroups

Example 2.5.1 (Non-Example).

- 1) $(\mathbb{Z}, +)$ is not a subgroup of $(\mathbb{Z}, +)$. For $x \in \mathbb{Z}^+$, $x \notin \mathbb{Z}^+$ no inverses. Also $0 \notin \mathbb{Z}^+$ so no identity.
- 2) $(\mathbb{Z} \setminus \{0\}, \times)$ is not a subgroup of $(\mathbb{Q} \setminus \{0\}, \times)$ since in general $x \in \mathbb{Z} \setminus \{0\}$ but $\frac{1}{x} \notin \mathbb{Z} \setminus \{0\}$ so inverses fail.

Remark 2.5.2. The relation “is a subgroup of” is transitive so if $H \leq G$ and $k \leq H$, then $k \leq G$.

Proposition 2.5.3. Let H, K be subgroups of G , then $H \cap K \leq G$.

Proof. $e \in H, e \in K$ so $e \in H \cap K$. If $x \in H \cap K$, then $x^{-1} \in H, x^{-1} \in K$ so $x^{-1} \in H \cap K$. If $x, y \in H \cap K$, then $xy \in H \cap K$, then $xy \in H, xy \in K$ so $xy \in H \cap K$.

Proposition 2.5.4 (The Subgroup Criterion). A subset H of a group G is a subgroup if

1. $H \neq \emptyset$
2. if $x, y \in H$, then $xy^{-1} \in H$

Proof. If H is a subgroup then $e \in H$ so $H \neq \emptyset$ and if $x, y \in H$, then $x, y^{-1} \in H$ so $xy^{-1} \in H$ so (1) and (2) hold.

Now, suppose (1) and (2) hold. Let $x \in H$ (we know there is such an x since $H \neq \emptyset$). Apply (2) to x so $xx^{-1} = e \in H$. Apply (2) to e and x so $ex^{-1} = x^{-1} \in H$. If $x, y \in H$, apply (2) to x and y^{-1} so $x(y^{-1})^{-1} = xy \in H$. Thus H is a subgroup.

2.5.2 Centralizers, Normalizers, and Center

- An important Class of Subgroups
- Let A be a nonempty subset of G

Definition 2.5.5. $C_G(A) = \{g \in G \mid gag^{-1} = a \forall a \in A\}$. $C_G(A)$ is called the centralizer of A . It consists of the set of elements in G that commute with all elements of A .

- $C_G(A) \subseteq G$

Proposition 2.5.6. $C_G(A)$ is a subgroup of G .

Proof. $eae^{-1} = a \forall a \in A$ so $e \in C_G(A)$.

If $x, y \in C_G(A)$, $xax^{-1} = a$ and $yay^{-1} = a \forall a \in A$

so $y^{-1}yay^{-1}y = y^{-1}ay$ so $a = y^{-1}ay$ so $y^{-1} \in C_G(A)$. Also, $xya(xy)^{-1} = xyax^{-1}x^{-1} = x(yay^{-1})x^{-1} =$

$| \quad xax^{-1} = a \text{ so } xy \in C_G(A).$

Definition 2.5.7. $Z(G) = \{g \in G | gx = xg \forall x \in G\}$ is called the center of G and is the set of elements commuting with all elements of G .

Note: $Z(G) = C_G(G)$ so $Z(G) \leq G$.

Definition 2.5.8. $gAg^{-1} = \{gag^{-1} | a \in A\}$

Definition 2.5.9. $N_G(A) = \{g \in G | gAg^{-1} = A\}$ is the normalizer of A in G .

Note: If $g \in C_G(A)$, $g \in N_G(A)$. Also $C_G(A) \leq N_G(A)$ and $N_G(A) \leq G$.

Example 2.5.10. If G is abelian, $Z(G) = C_G(A) = N_G(A) = G$ since $gag^{-1} = gg^{-1}a = a \forall a \in A, g \in G$.

Example 2.5.11. Let $G = D_8 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$. Let $A = \{1, r, r^2, r^3\}$.

Claim: $C_{D_8}(A) = A$.

Proof. $r^i r^j = r^{i+j} = r^{j+i} = r^j r^i$ so $A \subset C_{D_8}(A)$. $rs = sr^{-1} \neq sr$ so $s \notin C_{D_8}(A)$. Suppose that $sr^i \in C_{D_8}(A)$ for $i = 1, 2, 3$. Since $C_{D_8}(A)$ is a group and $r^{-i} \in C_{D_8}(A)$ so $sr^i sr^{-1} = s \in C_{D_8}(A)$ which is a contradiction. \square

Claim: $N_{D_8}(A) = D_8$

Proof. Note $r^i = sr^{-1}$. Since $C_{D_8}(A) \subseteq N_{D_8}(A)$, $A \subseteq N_{D_8}(A)$. $sAs^{-1} = \{s1s^{-1}, srs^{-1}, sr^2s^{-1}, sr^3s^{-1}\} = \{1, r^3, r^2, r\} = A$ so $s \in N_{D_8}(A)$. Since $N_{D_8}(A)$ is a group, $sr^i \in N_{D_8}(A)$ for $i = 1, 2, 3$ so $N_{D_8}(A) = D_8$. \square

Claim: $Z(D_8) = \{1, r^2\}$

Proof. $Z(D_8) \subset C_{D_8}(A) = A$ so we need to check if $\{1, r, r^2, r^3\}$ are in $Z(D_8)$. $1 \in Z(D_8)$. $rs = sr^{-1} \neq sr$ so $r \notin Z(D_8)$, also $r^3s = sr^{-3} \neq sr^3$. $r^2s = sr^{-2} = sr^2$ so r^2 and s commutes. Also $r^2sr^i = sr^2r^i = sr^i r^2$ so r^2 commutes with D_8 . Thus $Z(D_8) = \{1, r^2\}$. \square

2.6 February 8

2.6.1 Cyclic Groups

Definition 2.6.1. A group is cyclic if it is generated by one element. $H = \langle x \rangle = \{x^n | n \in \mathbb{Z}\}$. x is called a generator for H .

Example 2.6.2.

- 1) \mathbb{Z} under addition: $(\mathbb{Z}, +) = \langle 1 \rangle = \{n \cdot 1 | n \in \mathbb{Z}\} = \langle -1 \rangle = \{n \cdot -1 | n \in \mathbb{Z}\}$
- 2) $(\mathbb{Z}/m\mathbb{Z}, +) = \langle [1] \rangle = \{[1], [2], \dots, [m-1], [0]\}$

Remark 2.6.3. Generators need not be unique.

Cyclic groups are abelian.

Proof. if $a, b \in H = \langle x \rangle$. $a = x^\alpha, b = x^\beta$ for $\alpha, \beta \in \mathbb{Z}$ so $ab = x^\alpha x^\beta = x^{\alpha+\beta} = x^{\beta+\alpha} = x^\beta x^\alpha = ba$

\square

Proposition 2.6.4. Let $H = \langle x \rangle$, then $|x| = |H|$. (the order of a group is the same as the order of its generator)

Proof. If $|x| = n$, $\{1, x, \dots, x^{n-1}\}$ are all distinct so H has at least n elements. Suppose $x^t \in H$, then by the division algorithm $t = nq + r$ for $0 \leq r < n$. So $x^t = x^{nq+r} = (x^n)^q x^r = 1^q x^r = x^r \in \{1, x, \dots, x^{n-1}\}$. If $|x| = \infty$, then there is no positive integer such that $x^n = 1$. If $x^a = x^b$ for $a < b$, then $x^{b-a} = 1$ which contradicts our assumption so all x^n must be distinct.

Proposition 2.6.5. If $|x| = n$, $x^a = 1$ iff $n|a$.

Proof. If $x^a = 1$, and $n \nmid a$, then $\gcd(n, a) = d$ for some $0 < d \leq n$. By euclidean algorithm, $\exists u, v$ such that $nu + av = d$. $x^d = x^{nu} x^{av} = (x^n)^u (x^a)^v = 1^u 1^v$ so $x^d = 1$. Thus, by the minimality of n we must have $d = n$ so $n|a$.

Suppose $n|a$, then $a = bn$ for $b \in \mathbb{Z}$ so $x^a = x^{bn} = (x^n)^b = 1^b = 1$.

Theorem 2.6.6. Let G be a cyclic group.

1. If G is infinite, $G \cong (\mathbb{Z}, +)$
2. If G is finite and $|G| = m$, $G \cong (\mathbb{Z}/m\mathbb{Z}, +)$

Proof.

- (1) Let $G = \langle x \rangle$, $\varphi : G \rightarrow \mathbb{Z}$ by $x^n \mapsto n$
 Well defined: $x^a = x^b \rightarrow a = b$ by previous proposition
 Injective: $a = b \rightarrow x^a = x^b$
 Surjective: By def of G , it contains all integral powers of x so for $n \in \mathbb{Z}$, take x^n .
 Homomorphism: $\varphi(x^a x^b) = \varphi(x^{a+b}) = a + b = \varphi(x^a) + \varphi(x^b)$
- (2) Let $|G| = m$, $G = \langle x \rangle$, $\varphi : G \rightarrow \mathbb{Z}/m\mathbb{Z}$ by $x^n \mapsto [n]$
 Homomorphism: $\varphi(x^a x^b) = \varphi(x^{a+b}) = [a + b] = [a] + [b] = \varphi(x^a) + \varphi(x^b)$. Well defined: WTS $x^r = x^s \rightarrow \varphi(x^r) = \varphi(x^s)$ eg. $[r] = [s]$
 $x^{r-s} = 1$ so $m|r-s$ so $r-s = tm$ $t \in \mathbb{Z}$ so $\varphi(x^r) = \varphi(x^{tm+s}) = [tm + s] = [s] = \varphi(x^s)$
 Surjective: $|G| = m$ so $|x| = m$ so $\{1, x, \dots, x^{m-1}\}$ are all distinct so $G = \{1, x, \dots, x^{m-1}\}$ and $\mathbb{Z}/m\mathbb{Z} = \{[0], [1], \dots, [m-1]\}$. So each element in $\mathbb{Z}/m\mathbb{Z}$ has a preimage.
 Injective: WTS $[a] = [b] \rightarrow x^a = x^b$. Suppose $x^a \neq x^b$, then $x^{a-b} \neq 1$ so $m \nmid a-b$ so $a \not\equiv b \pmod{m}$ so $[a] \neq [b]$ which contradicts our assumption. Thus, they must be equal.

Corollary 2.6.7. Any two cyclic groups of the same order are isomorphic.

Proposition 2.6.8. Let G be a group $x \in G$, $a \in \mathbb{Z} \setminus \{0\}$. If $|x| = n < \infty$, then $|x^a| = \frac{n}{\gcd(n, a)}$.

Proof. Let $y = x^a$, $\gcd(a, n) = d$, $n = db$, $a = dc$, $b, c \in \mathbb{Z}$. Then $\gcd(b, c) = 1$. WTS $|y| = b$ ($|x|^a = \frac{n}{\gcd(a, b)} = \frac{db}{d} = b$)
 $y^b = x^{ab} = x^{dcb} = x^{nc} = (x^n)^c = 1^c = 1$ so $|y| \mid b$.
 Let $k = |y|$, we have $k \mid b$, WTS $b \mid k$. $x^{ak} = y^k = 1$ so $n \mid ak$ so $db \mid dck$ so $b \mid ck$. Since $\gcd(b, c) = 1$, $b \mid k$.

$\mathbb{Z}/m\mathbb{Z} = \{[0], [1], \dots, [5]\}$ and $|[0]| = 1$, $|[1]| = |[5]| = 6$, $|[2]| = |[4]| = 3$, $|[3]| = 2$.

Consider D_{16} . Let $R = \{1, r, \dots, r^7\}$. Observe $\langle r \rangle = R$. also $\langle r^2 \rangle = \{r^2, r^4, r^6, 1\}$, $\langle r^3 \rangle = \{r^3, r^6, r^4, r^7, r^2, r^5, 1\}$.
 More generally, $R = \langle r \rangle = \langle r^3 \rangle = \langle r^5 \rangle = \langle r^7 \rangle$.

2.7 February 10

2.7.1 Cyclic Groups

Corollary 2.7.1. Let $H = \langle x \rangle$. Assume $|x| = n < \infty$, then $H = \langle x^a \rangle$ iff $\gcd(a, n) = 1$

- # of generators of H is $\varphi(n) = \#$ integers $< n$ relatively prime to n .

Example 2.7.2. $\mathbb{Z}/12\mathbb{Z} = \{[0], [1], \dots, [11]\}$.

$[1]$ - generator, $[2] = [1] + [1] = "[1]^2"$. For which a is $\gcd(a, \mathbb{Z}) = 1$?

$\varphi(12) = 4$ so $[1], [5], [7], [11]$ are generators of $\mathbb{Z}/12\mathbb{Z}$.

Theorem 2.7.3. If $H = \langle x \rangle$ is a cyclic group

- Every subgroup of H is cyclic.
- If $|H| = n < \infty$, for each positive integer a dividing n , there is a unique subgroup of H of order a .

Proof.

- Let $K = \langle x \rangle$. If $K = \{1\}$ we are done.
 Otherwise, let $a = \min\{k > 0 \text{ such that } x^k \in K\}$. Claim: $K = \langle x^a \rangle$
 Suppose not (suppose $\exists x^b \in K$ with $a \nmid b$). The division algorithm gives us $bq + r$ with $0 < r < a$.
 Then since $x^b, x^a \in K$, $x^{b-aq} = x^r \in K$. This contradicts the minimality of a so $a \mid b \forall b$ with $x^b \in K$.
- $|H| = n < \infty$, $a \mid n$. $x^{n/a}$ has order a so $\langle x^{n/a} \rangle$ has order a since $\gcd(n/a, n) = n/a$. Suppose there is another k such that $\gcd(k, n) = n/a$, then there exists u, v such that $ku + nv = n/a$ so $x^{ku} = x^{ku+nv} = x^{n/a} \in \langle x^k \rangle$. Since a/n is the smallest element with $\gcd(b, n) = a/n$, $\langle x^k \rangle = \langle x^{a/n} \rangle$.

Example 2.7.4. $\mathbb{Z}/12\mathbb{Z} = \langle [1] \rangle = \langle [5] \rangle = \langle [7] \rangle = \langle [11] \rangle$ order 12

$\langle [2] \rangle = \langle [6] \rangle$ order 6, $\langle [3] \rangle = \langle [9] \rangle$ order 4, $\langle [4] \rangle = \langle [8] \rangle$ order 3, $\langle [6] \rangle$ order 2, $\langle [0] \rangle$ order 1.

Inclusion between subgroups: $\langle [a] \rangle \subseteq \langle [b] \rangle$ iff $\gcd(b, 12) \mid \gcd(a, 12)$.

2.7.2 Subgroups Generated by Subsets of a Group

- Cyclic subgroups $\{x\}$, take one element, take all possible products (close under multiplication and taking inverses)

- This is the smallest subgroup of G containing x
- Want to generalize this to the setting where your generating set has more than one element

Proposition 2.7.5. For any nonempty collection of subgroups of G , the intersection of all their members is also a subgroup of G .

Definition 2.7.6. If A is any subset of the group G ,

$$\langle A \rangle = \bigcap_{\substack{A \subseteq H \\ H \leq G}} H$$

called the subgroup of G generated by A . “intersection of all subgroups of G containing A ”

- $\langle A \rangle$ is the minimal subgroup of G containing A
- Let’s see a more concrete definition

Another way to define $\langle A \rangle$ is in terms of generators.

$$\overline{A} = \{a_1^{\varepsilon_1} a_2^{\varepsilon_2} \cdots a_n^{\varepsilon_n} \mid n \in \mathbb{Z}, n \geq 0, \varepsilon_i = \pm 1\}$$

$\overline{A} = \{1\}$ if $A = \emptyset$

Proposition 2.7.7. $\overline{A} = \langle A \rangle$

Proof. Using the subgroup criterion we will show \overline{A} is a subgroup.

$\overline{A} \neq \emptyset$ since $A \neq \emptyset \rightarrow \overline{A} = \{1\}$. If $a, b \in \overline{A}$. $a = a_1^{\varepsilon_1} a_2^{\varepsilon_2} \cdots a_n^{\varepsilon_n}$, $b = b_1^{\delta_1} b_2^{\delta_2} \cdots b_m^{\delta_m}$ then $ab^{-1} = a_1^{\varepsilon_1} \cdots a_n^{\varepsilon_n} b_m^{-\delta_m} \cdots b_1^{-\delta_1}$ so ab^{-1} is of the form we wanted (elements of A raised to ± 1) so $\overline{A} \leq G$. Now, since $a \in A$ can be written as a^1 , $A \subseteq \overline{A}$ so $\langle A \rangle \subseteq \overline{A}$ because $\langle A \rangle$ was minimal among subgroups containing A .

Now, $\langle A \rangle$ contains \overline{A} because it contains A and is closed under multiplication and taking inverses.

Example 2.7.8. $\langle (12), (13)(24) \rangle \leq S_4$ is isomorphic to D_8 .

2.7.3 Quotient Groups

Definition 2.7.9. If $\varphi : G \rightarrow H$ is a homomorphism, the kernel of φ is the set $\ker \varphi = \{g \in G : \varphi(g) = e_H\}$. The image of φ is the set $\text{im}(\varphi) = \{\varphi(x) \mid x \in G\}$

Proposition 2.7.10. Let H, G be groups, $\varphi : G \rightarrow H$ a homomorphism, the kernel of φ is a subgroup of G and $\text{im} \varphi$ is a subgroup of H .

Proof ((Kernel)). Since e_G is such that $\varphi(e_G) = e_H$, $e_G \in \ker \varphi$ so $\ker \varphi \neq \emptyset$.

Now, let $x, y \in \ker \varphi$ so that $\varphi(x) = \varphi(y) = e_H$. Then $\varphi(xy^{-1}) = \varphi(x)\varphi(y^{-1}) = \varphi(x)\varphi(y^{-1}) = \varphi(x)\varphi(y)^{-1} = e_H e_H^{-1} = e_H$ so $xy^{-1} \in \ker \varphi$ so $\ker \varphi \leq G$.

Proof ((Image)). $\varphi(e_G) = e_H \in \text{im} \varphi$ so $\text{im} \varphi \neq \emptyset$.

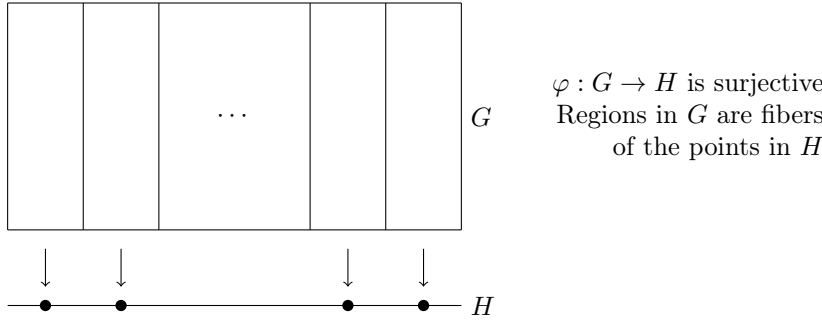
If $x, y \in \text{im} \varphi$, say $x = \varphi(a)$, $y = \varphi(b)$ $a, b \in G$ then $y^{-1} = (\varphi(b))^{-1} = \varphi(b^{-1})$, so $xy^{-1} = \varphi(a)\varphi(b^{-1}) = \varphi(ab^{-1})$ so $xy^{-1} \in \text{im} \varphi$ so $\text{im} \varphi \leq H$.

2.8 February 15

2.8.1 Quotient Groups

Another way to make a (smaller) group out of a given group.

Think: $H \leq G$, $H \hookrightarrow G$ (injective homomorphism), then the quotient group $G \twoheadrightarrow H$ (surjective homomorphism).

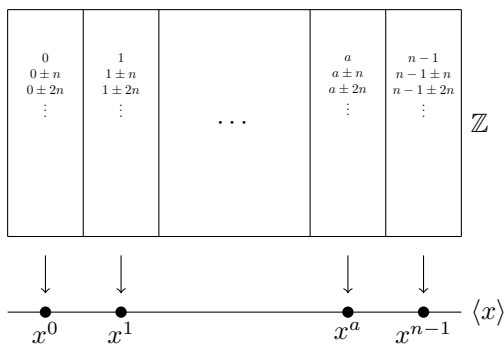


Example 2.8.1. $G = \mathbb{Z}$, $H = \langle x \rangle$, $|x| = m$. $\varphi : \mathbb{Z} \rightarrow \langle x \rangle$ by $a \mapsto x^a$.

$\varphi(a+b) = x^{a+b} = x^a x^b = \varphi(a)\varphi(b)$ so homomorphism.

Can see φ is surjective since $\{n, 1, \dots, n-1\} \rightarrow \{1, x^1, \dots, x^{n-1}\}$

The fiber of φ over x^a : $\varphi^{-1}(x^a) = \{m \in \mathbb{Z} | x^m = x^a\} = \{m \in \mathbb{Z} | x^{m-a} = 1\} = \{m \in \mathbb{Z} | n | m - a\} = \{m \in \mathbb{Z} | m \equiv a \pmod{n}\} = [a]$



Multiplication in $\langle x \rangle$:

$x^a x^b = x^{a+b}$. Fibers over $[a], [b], [a+b]$. Operation should be $[a] * [b] = [a+b]$. So the group is $(\mathbb{Z}/n\mathbb{Z}, +)$.

Identity of the group is $[0]$ ($0 + n\mathbb{Z}$).

The equivalence classes are $a + n\mathbb{Z}$.

Definition 2.8.2. Let $\varphi : G \rightarrow H$ be a homomorphism with kernel K . Then the quotient group “ $G \bmod K$ ” is the group whose elements are the fibers of φ . The group operation is inherited from H .

Remark 2.8.3. This requires knowing the map explicitly.

Proposition 2.8.4. Let $\varphi : G \rightarrow H$ be a homomorphism with kernel K , let $X \in G/K$ be the fiber above $a \in H$ ($X = \varphi^{-1}(a)$). For any $u \in X$, $X = \{uk | k \in K\}$ ($X = \{ku | k \in K\}$).

Proof. Let $u \in X$ be such that $\varphi(u) = a$. Let $uK = \{uk | k \in K\}$. Want to show $X = uK$. First show $uK \subseteq X$.

For $uk \in uK$, $\varphi(uk) = \varphi(u)\varphi(k) = ae = a$ so $uk \in X$.

Want to show $X \subseteq uK$. Let $g \in X$, let $k \in u^{-1}g$. $\varphi(k) = \varphi(u^{-1})\varphi(g) = \varphi(u)^{-1}a = a^{-1}a = e$ so $k \in \ker \varphi$. Since $k = u^{-1}g$, $g = uk \in uK$.

Definition 2.8.5. For any $N \leq G$ and $g \in G$, $gN = \{gn | n \in N\}$ is called the left coset of N in G . ($Ng = \{ng | n \in N\}$ is called the right coset of N in G)

The proposition says the fibers of a homomorphism are cosets of the kernel. $X \in G/K \rightarrow X = gK$.

We can define multiplication by choosing coset representatives.

Theorem 2.8.6. $\varphi : G \rightarrow H$ is a homomorphism with kernel K . The set of cosets of K in G (gK) with the operation $uKvK = uvK$ forms a group (the quotient group G/K).

Multiplication does not depend on representative.

Proof. Let $X, Y \in G/K$, $Z = XY \in G/K$. $X = \varphi^{-1}(a), Y = \varphi^{-1}(b)$ for some $a, b \in H$. Then $Z = \varphi^{-1}(ab)$. Let u, v be representatives of X and Y . Want to show $uv \in Z$. $\varphi(u) = a, \varphi(v) = b$, $X = uK, Y = vK$ so $uv \in Z \iff uv \in \varphi^{-1}(ab) \iff \varphi(uv) = ab \iff \varphi(u)\varphi(v) = ab$. Last statement is true so $uv \in Z$, $Z = uvK$. \square

Question: Can you define a quotient group G/N for any subgroup N in this way?

A: No.

2.9 February 17

2.9.1 Quotient Groups

Two views of quotient groups:

- Fibers of homomorphism with group structure seen in target space
- Cosets of the kernel of $\varphi : G \rightarrow H$ uK, vK with $uKvK = uvK$

Can we generalize quotient groups to any subgroup N ?

Claim: If $\varphi : G \rightarrow H$ is a homomorphism with kernel K then $gKg^{-1} \subseteq K \forall g \in G$.

Proof. WTS $\varphi(gkg^{-1}) = e \forall k \in K, \forall g \in G$.

Observe $\varphi(gKg^{-1}) = \varphi(g)e\varphi(g^{-1}) = \varphi(g)e\varphi(g)^{-1} = e$ \square

If we have a subgroup N of G such that $gNg^{-1} \subseteq N \forall g \in G$ then we can show multiplication of G/N is well defined (doesn't depend on representative)

eg. If $x_1N = x_2N$, $y_1N = y_2N$, then $x_1y_1N = x_2y_2N$

Proof. We know $x_1^{-1}x_2, y_1^{-1}y_2 \in N$. Let $u = (x_1y_1)^{-1}(x_2y_2) = y_1^{-1}x_2^{-1}x_2y_2$.
 $uy_2^{-1}y_1 = y_1^{-1}x_1x_2y_1$ and since $y_1 \in G$, $gNg^{-1} \subseteq N$ then $ux_1^{-1}x \in N$. Since $y_2^{-1}, y_1 \in N$, $uy_2^{-1}y_1y_1^{-1}y_2 = u \in N$ so $x_1y_1N = x_2y_2N$. \square

Definition 2.9.1. A subgroup $N \leq G$ is called normal if for all $g \in G$, $gNg^{-1} = \{gng^{-1} | n \in N\} = N$. We write $H \trianglelefteq G$.

Claim: If $gNg^{-1} \subseteq N \forall g \in G$, then $gNg^{-1} = N$

Proof. WTS: $N \subseteq gNg^{-1}$. Let $n \in N$ be arbitrary. Since by assumption $g^{-1}ng \in N$, we see that $g(g^{-1}ng)g^{-1} = n$ is an element of gNg^{-1} , as desired. \square

Remark 2.9.2.

- (a) Same as saying every element of G normalizes N . ($N_G(N) = G$)
- (b) We are not saying $gng^{-1} = n$, just that $gng^{-1} \in N$
- (c) If G is abelian, every subgroup of G is normal (because $gng^{-1} = n \forall g, n \in G$)

Claim from before implies that for $\varphi : G \rightarrow H$, $\ker(\varphi) \trianglelefteq G$.

Any normal subgroup can be realized as the kernel of a homomorphism.

Proposition 2.9.3. For $H \trianglelefteq G$, the map $\varphi : G \rightarrow G/H$ by $x \mapsto xH$ is a homomorphism with $\ker(\varphi) = H$.

Proof. $\varphi(xy) = xyH = xHyH = \varphi(x)\varphi(y)$ so φ is a homomorphism.
 The identity of G/H is H . If $x \in \ker(\varphi)$, $\varphi(x) = xH = H \iff x \in H$ so $\ker \varphi = H$.

Remark 2.9.4. 3 perspectives on quotient groups:

- Groups of fibers of a homomorphism.
- Groups of cosets of a normal subgroup.
- Image of a surjective homomorphism (the image of the quotient map)

Theorem 2.9.5 (Lagrange). If G is a finite group and H is a subgroup of G . then $|H| \mid |G|$ and the number of cosets of H in G is $\frac{|G|}{|H|}$.

Proof. Let $|H| = n$, let the number of cosets of H in G be k . The set of cosets partitions G and the map $H \rightarrow gH$ by $h \mapsto gh$ is a bijection so $|H| = |gH| = n$. Thus, $|G| = nk$ so $|H| \mid |G|$ and $k = \frac{|G|}{n} = \frac{|G|}{|H|}$.

Definition 2.9.6. The number of cosets of H in G is called the index of H in G , $[G : H]$.

Corollary 2.9.7. If G is a finite group and $x \in G$, then $|x| \mid |G|$ and $x^{|G|} = 1$.

Proof. $|x| = |\langle x \rangle|$. Since $\langle x \rangle$ is a subgroup of G , by Lagrange, $|\langle x \rangle| \mid |G|$ so $|x| \mid |G|$. $x^{|G|} = 1$ since $x^{|a|} = 1$ iff $|x| \mid a$.

Corollary 2.9.8. Every group of prime order is cyclic.

Proof. Let $x \in G$, $x \neq 1$. Then $|\langle x \rangle| = |x| > 1$ and $|\langle x \rangle| \mid |G|$ so $|\langle x \rangle| = p = |G|$ so $G = \langle x \rangle$ so G is cyclic.

Proposition 2.9.9. Every subgroup of index 2 is normal. eg. If $H \leq G$, $[G : H] = 2$, then $H \trianglelefteq G$.

Proof. Let $g \in G \setminus H$. The two left cosets of H in G are gH and $eH = H$. Similarly, the right cosets of H in G are Hg and $He = H$. So $gH = Hg$ so $gHg^{-1} = H \forall g \in G$ so H is normal.

Remark 2.9.10. The full converse of Lagrange's theorem is false, $n \mid |G|$ then G need not have a subgroup of order n .

Note: If $p \mid |G|$ then G has an element of order p .

Sylow's Thm: If $|G| = p^\alpha m$, $p \nmid m$ then G has a subgroup of order p^α .

2.10 February 22

2.10.1 The Isomorphism Theorems

Let G, H be groups with $e_H, e_G \in H$. Let $\varphi : G \rightarrow H$ be a homomorphism, $\ker \varphi \trianglelefteq G$. It makes sense to form $G / \ker \varphi = \{g \ker \varphi \mid g \in G\}$, the quotient group.

Let x, y be in the same coset of φ then $x \ker \varphi = y \ker \varphi \leftrightarrow x^{-1}y \ker \varphi \leftrightarrow e_H = \varphi(x^{-1})\varphi(y) \leftrightarrow \varphi(x^{-1})\varphi(y) \leftrightarrow \varphi(x)^{-1}\varphi(y) = e_H \leftrightarrow \varphi(y) = \varphi(x)$, so φ is constant on cosets (of $\ker \varphi$).

Theorem 2.10.1 (First Isomorphism Theorem). Let G, H be groups, $\varphi : G \rightarrow H$ a homomorphism, then $G / \ker(\varphi) \cong \text{im} \varphi$.

Proof. Consider $\psi : G / \ker \varphi \rightarrow \text{im} \varphi$ by $x \ker \varphi \mapsto \varphi(x)$. WTS ψ is an isomorphism. By def of $\text{im} \varphi$, ψ is surjective. Also, given $x, y \in G$, $\psi(x \ker \varphi) = \psi(y \ker \varphi) \leftrightarrow \varphi(x) = \varphi(y) \leftrightarrow x \ker \varphi = y \ker \varphi$ so ψ is injective.

Also $\psi(x \ker \varphi y \ker \varphi) = \psi(xy \ker \varphi) = \varphi(xy) = \varphi(x)\varphi(y) = \psi(x \ker \varphi)\psi(y \ker \varphi)$ so ψ is a homomorphism.

Example 2.10.2.

- (a) $(\mathbb{Z}, +) \hookrightarrow (\mathbb{Q}, +)$, $\varphi : \mathbb{Z} \rightarrow \mathbb{Q}$ by $x \mapsto x$.
 $\ker \varphi = 0 = e_{\mathbb{Z}}$, $\text{im} \varphi = \mathbb{Z}$ so $\mathbb{Z}/e_{\mathbb{Z}} \cong \mathbb{Z}$.
- (b) $(\mathbb{Z}, +) \twoheadrightarrow (\mathbb{Z}/m\mathbb{Z}, +)$, $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$ by $a \mapsto [a]$
 $\ker \varphi = m\mathbb{Z}$, $\text{im} \varphi = \mathbb{Z}/m\mathbb{Z}$ so $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z}$.
- (c) $\varphi : G \rightarrow H$ by $g \mapsto e_H$. $\ker \varphi = G$, $\text{im} \varphi = e_H$ so $G/G \cong e_H$.

Corollary 2.10.3. If $\varphi : G \rightarrow H$ is a homomorphism:

- (a) φ is injective iff $\ker \varphi = e$
 (b) $[G : \ker \varphi] = |\text{im} \varphi|$

Proof (Proof of (2)). $G/\ker \varphi \cong \text{im} \varphi$ so $|G/\ker \varphi| = |\text{im} \varphi|$ so $[G : \ker \varphi] = |\text{im} \varphi|$.

Proof (Proof of (1) - Old Fashion Way). \rightarrow If φ injective, WTS $\ker \varphi = e$. Observe that $\varphi(e_G) = e_H$, also if $g \in \ker \varphi$, $\varphi(g) = e_H$ so $\varphi(e_G) = \varphi(g)$. Since φ is injective, $g = e_G$ so $\ker \varphi = e_G$.
 \leftarrow If $\ker \varphi = e$, WTS φ is injective. Observe that $\varphi(g_1) = \varphi(g_2) \leftrightarrow \varphi(g_1)\varphi(g_2)^{-1} = e \leftrightarrow \varphi(g_1)\varphi(g_2^{-1}) = e \leftrightarrow \varphi(g_1g_2^{-1}) = e \leftrightarrow g_1g_2^{-1} \in \ker \varphi$ so $g_1g_2^{-1} = e$ so $g_1 = g_2$.

Proof (Proof of (1) - Using First Isomorphism Theorem.). $\ker \varphi = e \leftrightarrow G/e \cong \varphi(G) \leftrightarrow G \cong \varphi(G) \leftrightarrow \varphi$ is injective.

Theorem 2.10.4 (Third Isomorphism Theorem). Let G be a group, H, K normal subsets of G , $H \leq K$. Then $K/H \trianglelefteq G/H$ and $G/H / K/H \cong G/K$.

Proof. $K/H \leq G/H$:

Since K/H is a group, it suffices to show $K/H \subseteq G/H$. For $kH \in K/H$, $k \in K$ so $k \in G$ so $kH \in G/H$, as desired.

$K/H \trianglelefteq G/H$:

WTS $gHkH(gH)^{-1} \in K/H \forall g \in H \in G/H$. Observe that $gHkHg^{-1}H = gkg^{-1}H$ and since $K \trianglelefteq G$, $gkg^{-1} \in K \forall g \in G$ so $gkg^{-1} \in K/H \forall gH \in G/H$.

Finally, consider $\varphi : G/H \rightarrow G/K$ by $gH \mapsto gK$. Suppose $g_1H = g_2H$, then $g_2^{-1}g_1 \in H$ so $g_2^{-1}g_1 \in K$ so $g_1K = g_2K$. Thus $\varphi(g_1H) = \varphi(g_2H)$ so φ is well defined. Also, φ is surjective since so $\text{im} \varphi = G/K$.

$\ker \varphi = \{gH \in G/H \mid \varphi(gH) = eK\} = \{gH \in G/H \mid gK = eK\} = \{gH \in G/H \mid g \in K\} = K/H$. So by the first isomorphism theorem, $G/H / K/H \cong G/K$.

Theorem 2.10.5 ("Third" Isomorphism / Fourth Isomorphism / Correspondence Theorem). Let G be a group, $N \trianglelefteq G$, then there is a bijection between the subgroups of G containing N and subgroups of G/N .

2.11 March 3

To Do

2.12 March 8

2.12.1 Group Actions

Definition 2.12.1. Let G be a group acting on a set A

- (1) The equivalence class $\{g \cdot a | g \in G\} = \text{orb } a$ is called the orbit of a (orbit containing a in G)
- (2) The action of G on A is called transitive if there is only one orbit. (given $a, b \in A \exists g$ such that $a = g \cdot b$)

Example 2.12.2.

- D_8 acts on $\{1, 2, 3, 4\}$ transitively.
- If G_A acts trivially on A $G_a = A \forall a \in A$ ($g \cdot a = a$) the orbits are the elements of A . If $|A| = 1$ the action is transitive, otherwise not.

2.12.2 Groups Acting on Themselves ($G = A$)

Let G be a group and consider the action of G on itself by left multiplication.

$$g \cdot a = ga \quad \forall a, g \in G$$

This is a group action.

Now, generalize a bit let G be a group $H \leq G$, $A = \{gH | g \in G\}$. Define the action of G on A by left multiplication

$$g \cdot aH = gaH \quad \forall g \in G \quad \forall aH \in A$$

Suppose A has n elements a_1H_1, \dots, a_nH_n (labels)

Can define σ_g as $\sigma_g(i) = j$ iff $g \cdot a_iH = a_jH$.

Example 2.12.3. $G = D_8$, $H = \langle s \rangle = \{1, s\}$, $A = \{1H, rH, r^2H, r^3H\}$ \leftarrow labels

Computing σ_s :

$$\begin{aligned} s \cdot 1H &= s1H = H = 1H & \sigma_s(4) &= 4 \\ s \cdot rH &= srH = r^{-1}sH = r^{-1}H = r^3H & \sigma_s(1) &= 3 \\ s \cdot r^2H &= sr^2H = r^{-2}sH = r^{-2}H = r^2H & \sigma_s(2) &= 2 \\ s \cdot r^3H &= sr^3H = r^{-3}sH = r^{-3}H = r^1H & \sigma_s(3) &= 1 \end{aligned}$$

so $\sigma_s = (13)$. Similarly, $\sigma_r = (1234)$.

Theorem 2.12.4. Let G be a group, let $H \leq G$, let $A = \{gH | g \in G\}$, let G act on A by left multiplication.

- (1) The action is transitive.
- (2) The stabilizer of $1H = H$.
- (3) The kernel of the action is $\bigcap_{x \in G} xHx^{-1}$.

Proof.

- (1) Let $aH, bH \in A$, let $g = ba^{-1}$. $g \cdot aH = ba^{-1} \cdot aH = baa^{-1}H = bH$. Since aH, bH were arbitrary and they are in the same orbit, G acts transitively on A .
- (2) The stabilizer of $1H = G_{1H} = \{g \in G | g \cdot 1H = H\} = \{g \in G | gH = H\} = \{g \in G | g \in H\} = H$.
- (3) The kernel of the action is $\text{kernel} = \{g \in G | g \cdot xH = xH \ \forall x \in G\} = \{g \in G | xgx^{-1}H = H \ \forall x \in G\} = \{g \in G | x^{-1}gx \in H \ \forall x \in G\} = \{g \in G | g \in xHx^{-1} \ \forall x \in G\} = \bigcap_{x \in G} xHx^{-1}$.

Corollary 2.12.5 (Cayley's Theorem). Every group is isomorphic to a subgroup of some symmetric group. If $|G| = n$, G is isomorphic to a subgroup of S_n .

Proof. Let $H = 1$ and apply the above theorem. Take the permutation representation of $\varphi : G \rightarrow S_n$. $\ker \varphi \leq H$, H is trivial so $\ker \varphi = 1$. By the first isomorphism theorem, $G/\ker \varphi \cong \text{im} \varphi \leq S_G$ so $G/1 \cong G \cong \text{im} \varphi \leq S_G$.

Corollary 2.12.6. If G is a finite group of order n and p is the smallest prime dividing $|G|$ then any subgroup of order p is normal.

Proof. $H \leq G$ $[G : H] = p$. Consider the permutation representation of G acting by left multiplication on $\{gH\}$. $\varphi : G \rightarrow S_p$. Let $K = \ker \varphi$ $[H : K] = k$, $[G : H][H : K]$. H has p cosets so $G/K \cong \text{subgroup } S_p$ so $|G/K| \mid p!$. $|G/K| = pk$ so $pk \mid p!$ so $k \mid (p-1)!$. Since $|G|$ has no prime divisors less than p , $|G/K|$ has no prime divisors less than p . $(p-1)!$ has no prime divisors greater than or equal to p so $k = 1$ so $[H : K] = 1$ so $H = K$, $H \trianglelefteq G$.

2.13 March 10

2.13.1 Groups Acting on Themselves by Conjugation

Let G be a group, let $G = A$, let G act via $g \cdot a = gag^{-1} \ \forall a \in A, \forall g \in G$. Check this is a group action:

- $g_1 \cdot (g_2 \cdot a) = g_1 \cdot (g_2 a g_2^{-1}) = g_1 g_2 a g_2^{-1} g_1^{-1} = (g_1 g_2) a (g_1 g_2)^{-1} = g_1 g_2 \cdot a$
- $1 \cdot a = 1a1^{-1} = a \ \forall a \in A$.

Definition 2.13.1. Two elements a and b are said to be conjugate in G if $\exists g \in G$ such that $b = gag^{-1}$ (a and b are in the same orbit under the conjugation action)

Orbits under this action are called conjugacy classes.

Remark 2.13.2.

- (a) If G is abelian, this action is trivial since $gag^{-1} = a \ \forall g \in G$ ($ga = ag \ \forall a, g \in G$)
- (b) If $|G| > 1$, this action is not transitive because $geg^{-1} = e \ \forall g \in G$ so $\text{orb}(e) = \{e\}$. If $a \in Z(G)$, $gag^{-1} = a \ \forall a \in A$ so $\text{orb}(a) = \{a\}$

Generalize this to subgroups of G .

$S \leq G$, $gSg^{-1} = \{gsg^{-1} | s \in S\}$. G acts on the set of subsets of G ($P(G)$). $g \cdot S = gSg^{-1}$ for any $g \in G$, $S \in P(G)$.

Definition 2.13.3. Two subsets S and T are conjugate in G if $\exists g \in G$ such that $gSg^{-1} = T$. The stabilizer of this action is $G_S = \{g \in G | gSg^{-1} = S\} = N_G(S)$.

Proposition 2.13.4. The number of conjugates of a subset S in a group is $[G : G_S] = [G : N_G(S)]$. In particular, the number of conjugates of a single element $s \in G$ is $[G : C_G(s)]$.

Theorem 2.13.5 (The Class Equation). Let G be a finite group. g_1, \dots, g_r representatives of non central conjugacy classes (classes not in $Z(G)$). Then $|G| = |Z(G)| + \sum_{i=1}^r [G : C_G(g_i)]$.

Proof. Write $Z(G) = \{1, z_2, \dots, z_m\}$, let g_i be a representative of K_i with K_1, \dots, K_r list of all noncentral conjugacy classes (more than 1 element).

$\{1\}, \{z_2\}, \dots, \{z_m\}, K_1, \dots, K_r$ list of all conjugacy classes so they partition G . $|G| = \sum_{i=1}^m 1 + \sum_{i=1}^r |K_i| = |Z(G)| + \sum_{i=1}^r [G : C_G(g_i)]$.

Example 2.13.6.

(0) If G is abelian $|G| = |Z(G)|$.

(1) $D_8 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$.
 $\text{orb}(r) = \text{orb}(r^3) = \{r, r^3\}$ $\text{orb}(sr) = \text{orb}(sr^3) = \{sr, sr^3\}$
 $\text{orb}(s) = \text{orb}(sr^2) = \{s, sr^2\}$ $Z(D_8) = \{1, r^2\}$
 so $|D_8| = |Z(D_8)| + \sum_{s, sr} [G : C_G(x)]$ so $8 = 2 + \frac{8}{4} + \frac{8}{4} + \frac{8}{4}$.

Theorem 2.13.7. If p is prime and G is a group of order p^a $a \geq 1$, G has a nontrivial center.

Proof. If $a = 1$, $|G| = p$, G has prime order so G is a cyclic group and hence abelian.

If $a > 1$, $|G| = |Z(G)| + \sum_{i=1}^r [G : C_G(g_i)]$ with r representatives of non central conjugacy classes.
 $[G : C_G(g_i)] = \frac{|G|}{|C_G(g_i)|} = \frac{p^a}{p^n}$. $C_G(g_i) \neq G$ so $n < a$ so $p \mid [G : C_G(g_i)] \forall i$ so $p \mid \sum_{i=1}^r [G : C_G(g_i)]$ and $p \mid |G|$ so $p \mid |Z(G)|$ so $Z(G)$ is nontrivial.

Corollary 2.13.8. If $|G| = p^2$ (p prime) then G is abelian. ($G \cong \mathbb{Z}/p^2\mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$)

2.13.2 Groups Acting on Themselves by Conjugation

Proof. $|G| = p^2$ so by previous theorem $|Z(G)| = p$ or p^2 . If $|Z(G)| = p^2$ then $G = Z(G)$ so G is abelian. Otherwise, $|G/Z(G)| = \frac{p^2}{p} = p$ so $G/Z(G)$ is cyclic which implies G is abelian.

Let G be a group, let $G = A$, let G act via $g \cdot a = gag^{-1} \forall a \in A, \forall g \in G$. Check this is a group action:

- $g_1 \cdot (g_2 \cdot a) = g_1 \cdot (g_2 a g_2^{-1}) = g_1 g_2 a g_2^{-1} g_1^{-1} = (g_1 g_2) a (g_1 g_2)^{-1} = g_1 g_2 \cdot a$
- $1 \cdot a = 1 a 1^{-1} = a \forall a \in A$.

Definition 2.13.9. Two elements a and b are said to be conjugate in G if $\exists g \in G$ such that $b = gag^{-1}$ (a and b are in the same orbit under the conjugation action)

Orbits under this action are called conjugacy classes.

Remark 2.13.10.

- If G is abelian, this action is trivial since $gag^{-1} = a \forall g \in G$ ($ga = ag \forall a, g \in G$)
- If $|G| > 1$, this action is not transitive because $geg^{-1} = e \forall g \in G$ so $\text{orb}(e) = \{e\}$. If $a \in Z(G)$, $gag^{-1} = a \forall a \in A$ so $\text{orb}(a) = \{a\}$

Generalize this to subgroups of G .

$S \leq G$, $gSg^{-1} = \{gsg^{-1} | s \in S\}$. G acts on the set of subsets of G ($P(G)$). $g \cdot S = gSg^{-1}$ for any $g \in G$, $S \in P(G)$.

Definition 2.13.11. Two subsets S and T are conjugate in G if $\exists g \in G$ such that $gSg^{-1} = T$. The stabilizer of this action is $G_S = \{g \in G | gSg^{-1} = S\} = N_G(S)$.

Proposition 2.13.12. The number of conjugates of a subset S in a group is $[G : G_S] = [G : N_G(S)]$. In particular, the number of conjugates of a single element $s \in G$ is $[G : C_G(s)]$.

Theorem 2.13.13 (The Class Equation). Let G be a finite group. g_1, \dots, g_r representatives of non central conjugacy classes (classes not in $Z(G)$). Then $|G| = |Z(G)| + \sum_{i=1}^r [G : C_G(g_i)]$.

Proof. Write $Z(G) = \{1, z_2, \dots, z_m\}$, let g_i be a representative of K_i with K_1, \dots, K_r list of all noncentral conjugacy classes (more than 1 element). $\{1\}, \{z_2\}, \dots, \{z_m\}, K_1, \dots, K_r$ list of all conjugacy classes so they partition G . $|G| = \sum_{i=1}^m 1 + \sum_{i=1}^r |K_i| = |Z(G)| + \sum_{i=1}^r [G : C_G(g_i)]$.

Example 2.13.14.

- If G is abelian $|G| = |Z(G)|$.
- $D_8 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$.
 $\text{orb}(r) = \text{orb}(r^3) = \{r, r^3\}$ $\text{orb}(sr) = \text{orb}(sr^3) = \{sr, sr^3\}$
 $\text{orb}(s) = \text{orb}(sr^2) = \{s, sr^2\}$ $Z(D_8) = \{1, r^2\}$
 so $|D_8| = |Z(D_8)| + \sum_{i=r, sr, sr^2} [G : C_G(x)]$ so $8 = 2 + \frac{8}{4} + \frac{8}{4} + \frac{8}{4}$.

Theorem 2.13.15. If p is prime and G is a group of order p^a $a \geq 1$, G has a nontrivial center.

Proof. If $a = 1$, $|G| = p$, G has prime order so G is a cyclic group and hence abelian.

If $a > 1$, $|G| = |Z(G)| + \sum_{i=1}^r [G : C_G(g_i)]$ with r representatives of non central conjugacy classes. $[G : C_G(g_i)] = \frac{|G|}{|C_G(g_i)|} = \frac{p^a}{p^n}$. $C_G(g_i) \neq G$ so $n < a$ so $p \nmid [G : C_G(g_i)] \forall i$ so $p \nmid \sum_{i=1}^r [G : C_G(g_i)]$ and $p \mid |G|$ so $p \mid |Z(G)|$ so $Z(G)$ is nontrivial.

Corollary 2.13.16. If $|G| = p^2$ (p prime) then G is abelian. ($G \cong \mathbb{Z}/p^2\mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$)

Proof. $|G| = p^2$ so by previous theorem $|Z(G)| = p$ or p^2 . If $|Z(G)| = p^2$ then $G = Z(G)$ so G is abelian. Otherwise, $|G/Z(G)| = \frac{p^2}{p} = p$ so $G/Z(G)$ is cyclic which implies G is abelian.

2.14 March 15

2.14.1 Sylow's Theorems

Recall Langrange's Theorem (subgroup order divides group order).

Full converse not true, $|G| = n$, $d \mid n \nrightarrow \exists$ subgroup of G of order d .

Sylow's Theorems come close to this

Lemma 2.14.1 (Cauchy's Theorem for Abelian Groups). If G is a finite abelian group and p is a prime dividing $|G|$ then $|G|$ has an element of order p .

Proof. We will use induction on $|G|$. We know $|G| > 1$ since $p \mid |G|$ so $x \in G$ such that $x \neq 1$. If $|G| = p$, then x has order p .

So assume $|G| > p$ and let $x \in G$, $x \neq 1$

- Suppose $p \mid |x|$, then $|x| = np$ for some n . Then $|x^n| = \left(\frac{np}{\gcd(n, np)} \right) = \frac{np}{n} = p$ so $|x^n| = p$.
- Now, suppose $p \nmid |x|$. Let $N = \langle x \rangle$. Since G abelian $N \trianglelefteq G$ so by Langrange's thm, $|G/N| = \frac{|G|}{|N|}$, $x \neq 1$ so $|N| > 1$ so $|G/N| < |G|$. Since $p \nmid |N|$, $p \mid |G/N|$. By IH, G/N (smaller than G) contains an element of order p , $\bar{y} = yN$. $\bar{y} \neq \bar{1}$ so $y \notin N$. Also, $\bar{y}^p = \bar{1}$ so $\bar{y}^p \in N$ so $\langle y^p \rangle \neq \langle y \rangle$ so $|y^p| < |y|$. But $|y^p| = \frac{|y|}{\gcd(p, |y|)} = \frac{|y|}{p}$ so $p \mid |y|$. We already now how to find an element of order p in this case.

Definition 2.14.2. Let G be a group, let p be prime.

- (1) A group of order p^α for $\alpha \geq 0$ is called a p -group. Subgroups of G that are also p -groups are called p -subgroups.
- (2) If G is a group of order $p^\alpha m$ where $p \nmid m$ then a subgroup of order p^α is called a Sylow p -subgroup of G .

- (3) The set of Sylow p -subgroups of G will be denoted $Syl_p(G)$ and the number of Sylow p -subgroups will be denoted $n_p(G)$.

Theorem 2.14.3 (Sylow 1). Let G be a group of order $p^\alpha m$ where p is prime and does not divide m , then there exists a Sylow p -subgroup. (\exists a subgroup of order p^α , $Syl_p(G) \neq \emptyset$)

Proof. Proceed by induction on $|G|$. If $|G| = 1$, nothing to prove.

Assume that Sylow p -subgroups exist for all of order smaller than $|G|$.

- If $p \mid |Z(G)|$ then by the lemma $Z(G)$ has a subgroup of order p , call it N . Let $\bar{G} = G/N$, $|N| = p$ so $|G/N| = p^{\alpha-1}m$ so by IH \bar{G} has a Sylow p -subgroup (\bar{P} of order $p^{\alpha-1}$). Let P be the subgroup of G containing N such that $P/N = \bar{P}$ (correspondence isomorphism theorem.) $|P| = |P/N||N| = p^{\alpha-1}p = p^\alpha$ so P is a Sylow p -subgroup of G .
- Suppose $p \nmid |Z(G)|$. Let g_1, \dots, g_r be the representatives of the non central conjugacy classes in G . The class equation $|G| = |Z(G)| + \sum_{i=1}^r [G : C_G(g_i)]$. If $p \mid [G : C_G(g_i)] \forall i$ then $p \mid |Z(G)|$ contradicting our assumption. So $p \nmid [G : C_G(g_i)]$ for some i . Let $H = C_G(g_i)$, $|H| = p^\alpha k$, $p \nmid k$. Also $|H| < |G|$ since g_i not in $Z(G)$ so $C_G(g_i) \neq G$. By IH, H has a Sylow p -subgroup P , $|P| = p^\alpha$ so P is a Sylow p -subgroup of G .

Theorem 2.14.4 (Sylow 2). If P is a Sylow p -subgroup of G and Q is a Sylow p -subgroup in G $\exists g$ such that $Q \leq gPg^{-1}$. (Any two Sylow p -subgroups are conjugate in G)

Theorem 2.14.5 (Sylow 3). The number of Sylow p -subgroups of G is of the form $1 + kp$ ie. $n_p(G) \equiv 1 \pmod p$, $n_p = [G : N_G(P)]$ for P , any Sylow p -subgroup $n_p(G) \mid m$.

Example 2.14.6. $G = S_3$. $|S_3| = 2^1 \cdot 3^1$ so \exists a Sylow 2-subgroup and a Sylow 3-subgroup. The Sylow 2-subgroups have order 2 and the Sylow 3-subgroups have order 3.

$$n_2 \equiv 1 \pmod 2, n_2 \mid 3 \text{ so } n_2 = 1 \text{ or } 3. \quad Syl_2(S_3) = \{\langle (12) \rangle, \langle (23) \rangle, \langle (13) \rangle\}$$

$$n_3 \equiv 1 \pmod 3, n_3 \mid 2 \text{ so } n_3 = 1. \quad Syl_3(S_3) = \{\langle (123) \rangle\}$$

2.15 March 17

To Do

2.16 March 29

2.16.1 Finitely Generated Abelian Groups

Example 2.16.1. Suppose $n = 180 = 2^2 \cdot 3^2 \cdot 5$

Possible n_1 values: $n_1 = 2^2 \cdot 3^2 \cdot 5$, $n_1 = 2 \cdot 3^2 \cdot 5$, $n_1 = 2^2 \cdot 3 \cdot 5$, $n_1 = 2 \cdot 3 \cdot 5$

$$(1) \ n_1 = 2^2 \cdot 3^2 \cdot 5 \quad G \cong \mathbb{Z}/180\mathbb{Z}$$

$$(2) \ n_1 = 2 \cdot 3^2 \cdot 5 \quad G \cong \mathbb{Z}/90\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_s\mathbb{Z}$$

$$180 = 90n_2 \cdots n_s \text{ so } 2 = n_2 \cdots n_r \text{ so } n_2 = 2$$

$$G \cong \mathbb{Z}/90\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

$$(3) \quad n_1 = 2^2 \cdot 3 \cdot 5 \quad G \cong \mathbb{Z}/60\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$$

$$180 = 60n_2 \cdots n_r \text{ so } 3 = n_2 \cdots n_r \text{ so } n_2 = 3$$

$$G \cong \mathbb{Z}/60\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

$$(4) \quad n_1 = 2 \cdot 3 \cdot 5 \quad G \cong \mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_w\mathbb{Z}$$

$$180 = 30n_2 \cdots n_w \text{ so } 6 = n_2 \cdots n_w. \text{ Suppose } n_2 = 2 \text{ (or } n_2 = 3). \text{ Then } n_3 | n_2 \text{ so } n_3 = 2 \text{ (or } n_3 = 3) \text{ but } n_1 n_2 n_3 \text{ will be divisible by } 2^3 \text{ (or } 3^3) \text{ but } 180 \text{ is not so } G \cong \mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}.$$

Classification of Groups of Order 180

| Invariant Factors | Groups | Largest Order of Element |
|-------------------|---|--------------------------|
| (180) | $\mathbb{Z}/180\mathbb{Z}$ | 180 |
| (90, 2) | $\mathbb{Z}/90\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ | 90 |
| (60, 3) | $\mathbb{Z}/60\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ | 60 |
| (30, 6) | $\mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ | 30 |

Another way is Elementary Divisors:

Theorem 2.16.2. If G is an abelian group of order $n > 1$, where $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, then

- (1) $G \cong A_1 \times \cdots \times A_k \quad |A_i| = p_i^{\alpha_i}$
- (2) For each A_i , $A_i \cong \mathbb{Z}/p_i^{\beta_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_i^{\beta_t}\mathbb{Z}$
 $\beta_1 \geq \beta_2 \geq \cdots \geq 1$ and $\beta_1 + \cdots + \beta_t = \alpha_i$.

Remark 2.16.3.

- If G is abelian it is isomorphic to the product of its Sylow Subgroups.
- In general, the elementary divisors are not the invariant factors of G . They correspond to invariant factors of subgroups of G .

Example 2.16.4. $|G| = 180 = 2^2 \cdot 3^2 \cdot 5$

$$G = A_1 \times A_2 \times A_3 \quad |A_1| = 2^2, |A_2| = 3^2, |A_3| = 5$$

$$A_1 \cong \mathbb{Z}/4\mathbb{Z} \text{ or } A_1 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

$$A_2 \cong \mathbb{Z}/9\mathbb{Z} \text{ or } A_2 \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

$$A_3 \cong \mathbb{Z}/5\mathbb{Z}$$

$$G \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/180\mathbb{Z}$$

$$G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/90\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

$$G \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/60\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

$$G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$$

Chapter 3

Rings

3.1 March 29

3.1.1 Rings

Before: Groups \rightarrow set with one binary operation

Now: Rings \rightarrow set with two binary operations. One gives rise to an abelian group and the other is associative with identity. Want the two operations to be compatible

Rings(1870-1920's):

- Dedekind, Hilbert: Used without definition
- Fraenkel: Definition too strict
- Noether: Modern Definition

Definition 3.1.1. A ring R is a set with two binary operations $+$ and \times such that

- (1) $(R, +)$ is an (abelian) group
- (2) \times is associative
 $(a \times b) \times c = a \times (b \times c) \quad \forall a, b, c \in R$
- (3) The distributive law holds $\forall a, b, c \in R$
 $(a + b) \times c = (a \times c) + (b \times c) \quad a \times (b + c) = (a \times b) + (a \times c)$
- (4) There is a multiplicative identity 1 such that $a \times 1 = 1 \times a = a \quad \forall a \in R$

Definition 3.1.2. A ring is called commutative if multiplication is commutative.

Remark 3.1.3. There is debate as to whether rings have identity or not

- 1921: Def didn't include 1
- 1960's: People started using 1

Some people call it "ring with unit"

Note: $1 \in R \rightarrow (R, +)$ is abelian.

$$(1+1) \times (a+b) = 1 \times (a+b) + 1 \times (a+b) = a+b+a+b$$

$$\text{or} \quad = (1+1) \times a + (1+1) \times b = a+a+b+b$$

Definition 3.1.4. A ring R is called a division ring if every nonzero $a \in R$ has a multiplicative inverse. (ie. $\exists b \in R$ such that $ab = ba = 1$)

Definition 3.1.5. A commutative division ring is called a field.

Example 3.1.6.

- (0) The zero ring $R = \{0\}$, $0 = 1$, commutative
- (1) $(\mathbb{Z}, +, \times)$ is a ring, commutative
- (2) $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$, commutative
- (3) $(\mathbb{Z}/n\mathbb{Z}, +, \times)$, commutative ring.

3.2 March 31

3.2.1 Rings

Example 3.2.1. $M_n(R)$ with usual addition and multiplication, elements in R is a ring.

Example 3.2.2 (Non-Example).

- $(2\mathbb{Z}, +, \times)$: Doesn't have multiplicative identities
- $(\mathbb{Q} \setminus \{0\}, +, \times)$: No additive identity

Example 3.2.3.

- (1) $(\mathbb{Z}, +, \times)$ ring, not a field since no multiplicative inverses
- (2) $(\mathbb{Q}, +, \times)$ ring, field iff n is prime
 $[0] \neq [a]$, n prime. $\gcd(a, n) = 1$ so $\exists u, v \in \mathbb{Z}$ such that $ua + vn = 1$.
 $[u][a] + [0] = [1] \rightarrow [u][a] = [1] \quad (ua \equiv 1 \pmod{n})$

More Complex Examples: Let X be a nonempty set, A a ring. The set of functions $f : X \rightarrow A$ is a ring with operations $(f+g)(x) = f(x) + g(x)$, $(fg)(x) = f(x)g(x)$.

Ring axioms holds since they hold for A . $1 \in R$ is given by $f(x) = 1 \forall x \in X$.

R is commutative iff A is commutative.

Lemma 3.2.4. Let R be a ring.

- (1) $0a = a0 = 0 \forall a \in R$
- (2) $(-a)(b) = (a)(-b) = -(ab) \forall \in R$
- (3) $(-a)(-b) = ab$

$$(4) -a = (-1)a$$

Proof.

- (1) $0a = (0 + 0)a = 0a + 0a$ so $0 = 0a$
- (2) $ab + (-a)b = (a - a)b = 0b = 0$ so $(-a)b = -(ab)$
- (3) $(-a)(-b) + a(-b) = (-a + a)(-b) = 0$ so $(-a)b = -(ab)$
- (4) $(-a)(-b) + a(-b) = (-a + a)(-b) = 0$ so $(-a)(-b) = -(a(-b)) = ab$
- (5) $(-1)(a) + (1)(a) = (-1 + 1)a = 0$ so $(-1)(a) = -a$

Definition 3.2.5. Let R be a ring.

1. A nonzero element a of R is called a 0-divisor (zero-divisor) if there is an element $b \in R$ such that $ab = 0$ or $ba = 0$
2. A nonzero element of R is called a unit in R if there is some v in R such that $uv = vu = 1$. The set of units of R is denoted R^\times

Remark 3.2.6. For a ring R , R^\times forms a group under multiplication.

Remark 3.2.7. We can change the definition of a field to say F is a commutative ring with $1 \neq 0$ such that every nonzero element is a unit. $F^\times = F \setminus \{0\}$.

Lemma 3.2.8. A unit cannot be a zero divisor.

Proof. Assume that $a \in R$, $a \in R^\times$ and $\exists b \neq 0$ such that $ab = 0$ and $va = 1$ for some $v \in R$. $0 = v(0) = v(ab) = (va)b = 1b = b$, contradicting our assumption.

Example 3.2.9.

- (1) In \mathbb{Z} there are no 0-divisors the units are ± 1 , $\mathbb{Z}^\times = \{\pm 1\}$
- (2) In $\mathbb{Z}/n\mathbb{Z}$ every nonzero element is either a unit or a zero divisor.
 $[0] \neq [1] \in \mathbb{Z}/n\mathbb{Z}$ if $\gcd(a, n) = 1$ then $[a]$ is a unit. If $\gcd(a, n) \neq 1$ then let $b = \frac{n}{\gcd(n, a)}$ and set $\gcd(n, a) > 1$, $b < n \rightarrow [b] \neq [0]$ since $[a][b] = [0]$, $[a]$ is a zero divisor.

Definition 3.2.10. A commutative ring ($1 \neq 0$) is called an integral domain if it has no zero divisors. (ex. \mathbb{Z})

Proposition 3.2.11. Let R be a ring with no zero divisors. Let $a, b, c \in R$, then if $ab = ac$ then $a = 0$ or $b = c$.

Proof. If $ab = ac$, $ab - ac = 0$ so $a(b - c) = 0$ so $a = 0$ or $b - c = 0 \rightarrow b = c$.

Corollary 3.2.12. Any finite integral domain is a field.

Proof. Let $a \neq 0$, $a \in R$. Consider $R \rightarrow R$ by $x \mapsto ax$. The map is injective since $ax_1 = ax_2 \rightarrow x_1 = x_2$. Since R is finite, it is also surjective so $\exists b$ such that $ab = 1$ so a is a unit. Since a was an arbitrary non zero element, R is a field.

Definition 3.2.13. A subset of a ring is an additive subgroup of R that is closed under multiplication and contains the multiplicative identity of R .

Example 3.2.14.

$$(1) \quad \mathbb{Z} \underset{\text{subring}}{\subset} \mathbb{Q} \underset{\text{subring}}{\subset} \mathbb{R}$$

(2) If R is a subring of a field F then R is an integral domain

Proof. $a, b \in R$, $a, b \in F$ so $ab = ba$ so R is commutative

to show R is an integral domain, if $a \neq 0$, $a \in R \subset F$, a is a unit so a is non a zero divisor. \square

3.2.2 Polynomial Rings

Definition 3.2.15. Let R be a commutative ring with $1 \neq 0$, then $R[x]$ “ R adjoin x ” is the set of polynomials with coefficients with in R ,

$$R[x] = \{a_0 + a_1x + \cdots + a_nx^n \mid a^i \in R\}$$

Let $f(x) = a_0 + a_1x + \cdots + a_nx^n$, $a_n \neq 0$ (largest such n)

- We say $\text{degree}(f) = n$
- $a_n = 1 \rightarrow f$ is monic
- operations:

$$(a_0 + a_1x + \cdots + a_nx^n) + (b_0 + b_1x + \cdots + b_nx^n) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n$$

$$(a_0 + a_1x + \cdots + a_nx^n)(b_0 + b_1x + \cdots + b_nx^n) =$$

$$(a_0b_0) + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \cdots + a_nb_nx^{2n}$$

Coefficient of x^k is $\sum_{i=1}^k a_ib_{k-i}$.

$R[x]$ is a commutative ring, R is a subring

3.3 April 5

3.3.1 Polynomial Rings

Example 3.3.1. $\mathbb{Z}/3\mathbb{Z}[x]$, coefficients 0, 1, 2.

$$p(x) = x^2 + 2x + 1, q(x) = x^3 + x + 2$$

$$p(x) + q(x) = x^3 + x^2 + 3x + 3 = x^3 + x^2$$

$$p(x)q(x) = x^5 + 2x^4 + 2x^3 + x^2 + 2x + 2$$

The coefficients in a ring make a difference

Example 3.3.2. $x^2 + 1$ in $\mathbb{Z}[x]$ cannot be factored.

in $\mathbb{C}[x]$ can be factored: $(x - i)(x + i) = x^2 + 1$

in $\mathbb{Z}/2\mathbb{Z}[x]$ forms a perfect square: $(x + 1)^2 = (x + 1)(x + 1) = x^2 + 1$

$R[x]$ inherits properties from R

Proposition 3.3.3. Let R be an integral domain. Let $p(x), q(x)$ be nonzero elements of $R[x]$.

- 1) $\deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x))$
- 2) $(R[x])^\times = R^\times$
- 3) $R[x]$ is an integral domain.

Proof.

- (1) $p(x) = a_n x^n + \cdots + a_0$, $q(x) = b_m x^m + \cdots + b_0$, $a_n, b_m \neq 0$, $\deg(p(x)) = n$, $\deg(q(x)) = m$. $p(x)q(x) = a_n b_m x^{m+n} + \cdots + a_0 b_0$, since $a_n, b_m \neq 0$ $a_n b_m \neq 0$ so $\deg(p(x)q(x)) = m + n = \deg(p(x)) + \deg(q(x))$.
- (3) $p(x), q(x) \neq 0$, $p(x)q(x) \neq 0$ (degrees are additive) so R is an integral domain.
- (2) if $p(x)$ is a unit, $p(x)q(x) = 1$ for some $q(x) \in R[x]$, $\deg(1) = 0$, $\deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x)) = \deg(1) = 0$ so $\deg(p(x)) = \deg(q(x)) = 0$ so $p(x), q(x) \in R$, $p(x)q(x) = 1$ so $p(x), q(x) \in R^\times$.

We have shown $(R[x])^\times \subset R^\times$. Suppose $a, b \in R^\times$, $ab = 1$. Viewing them as constant polynomials we see that $a, b \in (R[x])^\times$.

Remark 3.3.4.

- if R has 0 divisors, so does $R[x]$
- If S is a subring of R then $S[x]$ is a subring of $R[x]$

3.3.2 Ring Homomorphisms

Definition 3.3.5. Let R and S be rings, a ring homomorphism is a map $\varphi : R \rightarrow S$ such that

- (i) $\varphi(a + b) = \varphi(a) + \varphi(b)$
- (ii) $\varphi(ab) = \varphi(a)\varphi(b)$

Definition 3.3.6. The kernel of φ is $\ker \varphi = \{r \in R \mid \varphi(r) = 0\}$
(The kernel of the additive group homomorphism)

Definition 3.3.7. A bijective ring homomorphism is called a ring isomorphism.

Example 3.3.8.

- (1) $\pi : \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ by $a \mapsto [a]$

$$\begin{aligned}\pi(a+b) &= [a+b] = [a] + [b] = \pi(a) + \pi(b) \\ \pi(ab) &= [ab] = [a][b] = \pi(a)\pi(b)\end{aligned}$$

- (2) $\varphi : \mathbb{Q}[x] \rightarrow \mathbb{Q}$ by $p(x) \mapsto p(0)$ (constant term)
 $\varphi(p(x) + q(x)) = p(0) + q(0) = \varphi(p(x)) + \varphi(q(x))$
 $\varphi(p(x)q(x)) = p(0)q(0) = \varphi(p(x))\varphi(q(x))$
 $\ker \varphi = \{p(x) \mid p(0) = 0\} = \text{polynomials with constant term } 0$

$\ker \varphi$ is not necessarily a subring as it may not have identity.

Example 3.3.9 (Non-Example). Let $n \in \mathbb{Z}$, $M_n; \mathbb{Z} \rightarrow \mathbb{Z}$ by $x \mapsto nx$

Group homomorphism: $M_n(x+y) = n(x+y) = nx + ny = M_n(x) + M_n(y)$

$M_n(xy) = nxy$ by $M_n(x)M_n(y) = nxny = n^2xy$. Not a ring homomorphism unless $n = 0, 1$

Facts About Kernels

1. $\ker \varphi$ is an additive subgroup of R
2. If $\alpha \in \ker \varphi$ then αr and $r\alpha$ are in $\ker \varphi \forall r \in R$

Proof.

$$\varphi(\alpha r) = \varphi(\alpha)\varphi(r) = 0\varphi(r) = 0 \text{ so } \alpha r \in \ker \varphi$$

$$\varphi(r\alpha) = \varphi(r)\varphi(\alpha) = \varphi(r)0 = 0 \text{ so } r\alpha \in \ker \varphi$$

□

Recall Quotient Groups:

$\varphi : R \rightarrow S$ is a ring homomorphism with $\ker \varphi = I$ $R/I \cong \text{im}(\varphi)$ by $r + I \mapsto \varphi(r)$

Definition 3.3.10. Define operations on R/I by:

$$(r_1 + I) + (r_2 + I) = (r_1 + r_2) + I$$

$$(r_1 + I)(r_2 + I) = (r_1 r_2) + I$$

These operations turn R/I into a ring

$$\left. \begin{array}{ccc} (r_1 + I) + (r_2 + I) & \mapsto & \varphi(r_1) + \varphi(r_2) \\ \parallel & & \parallel \\ (r_1 + r_2) + I & \mapsto & \varphi(r_1 + r_2) \end{array} \right\} +$$

$$\left. \begin{array}{ccc} (r_1 + I)(r_2 + I) & \mapsto & \varphi(r_1)\varphi(r_2) \\ \parallel & & \parallel \\ (r_1 r_2) + I & \mapsto & \varphi(r_1 r_2) \end{array} \right\} \times$$

Definition 3.3.11. Let R be a ring, a subset $I \subset R$ is called an ideal of R if

- (1) $(I, +) \leq (R, +)$ (additive subgroup)
- (2) $r \in R, i \in I \quad ri \in I$ (left ideal) $ir \in I$ (right ideal)

Remark 3.3.12. If R is commutative left and right ideals coincide.

Corollary 3.3.13. A subset $I \subset R$ is an ideal iff it is the kernel of some ring homomorphism.

Given an ideal we can form a quotient ring R/I .

As with groups we have isomorphism theorems.

Theorem 3.3.14 (1st Ring Isomorphism Theorem). If $\varphi : R \rightarrow S$ is an isomorphism, then $R/\ker \varphi \cong \text{im}(\varphi)$.

Example 3.3.15.

- (1) We saw $n\mathbb{Z}$ was an ideal of \mathbb{Z}
- (2) $I = \{\sum_{i=0}^n a_i x^i \mid a_0 = a_1 = 0\}$.
 For two elements in I , their sum also has $a_0 = a_1 = 0$, in I . If $f \in I$, $-f \in I$, $0 \in I$ so I is an additive subgroup.
 If $f(x) \in \mathbb{Z}[x]$, $f(x)I \subset I$, $If(x) \subset I$ since degrees are additive under multiplication. (ex: $(x^2)(x+1) = x^3 + x^2$)
 Two polynomials are in the same coset of I if their difference is a polynomial with $a_0 = a_1 = 0$. $p(x) + I = q(x) + I$ iff $p(x) - q(x) \in I$.
 The complete set of representative of R/I is $(ax + b) + I = \overline{(a + b)}$.
 $\bar{x} \cdot \bar{x} = \overline{x^2} = 0$ so R/I can have zero divisors even though $\mathbb{Z}[x]$ does not.

3.4 April 14

3.4.1 Operations with Ideals

Definition 3.4.1. Let I and J be ideals of R .

- (1) The sum of I and J is $I + J = \{a + b \mid a \in I, b \in J\}$
- (2) The product of I and J is $IJ = \{\sum_{i=1}^n a_i b_i \mid a_i \in I, b_i \in J, n \geq 0\}$
- (3) For $n \geq 1$, define the n th power of I as finite terms of the form $a_1 \cdots a_n$.

Remark 3.4.2.

- 1) $I + J$, IJ are ideals. In fact, $I + J$ is the smallest ideal containing I and J and $IJ \subset I \cap J$.
- 2) $\{ab \mid a \in I, b \in J\}$ may not be closed under addition.

Example 3.4.3.

- 1) In \mathbb{Z} , let $I = 6\mathbb{Z}$ and $J = 10\mathbb{Z}$.
 $I + J = \{6x + 10y \mid x, y \in \mathbb{Z}\}$. Everything in $I + J$ is a multiple of 2 so $I + J \subset 2\mathbb{Z}$ ($\gcd(6, 10) = 2$). WTS $I + J = 2\mathbb{Z}$ so enough to show $2\mathbb{Z} \subset I + J$. $2 = 2 \cdot 6 + (-1) \cdot 10$ so $2 \in I + J$ so $2\mathbb{Z} \subset I + J$. Thus, $6\mathbb{Z} + 10\mathbb{Z} = 2\mathbb{Z}$. $IJ =$ sums of $\sum 6x_i 10y_i = 60(\sum x_i y_i) = 60\mathbb{Z}$.

Remark 3.4.4. $m\mathbb{Z} + n\mathbb{Z} = \gcd(m, n)\mathbb{Z}$, in general

- 2) Let $I = \{\text{polynomials with even constant term}\} \subset \mathbb{Z}[x]$. 2 and $x \in I$, so $2 \cdot 2 = 4 \in I^2$ and $x \cdot x = x^2 \in I$ so $x^2 + 4 \in I^2$ but $x^2 + 4$ can't be written as the product of two terms in I .

3.4.2 Properties of Ideals

- Let R be commutative

Definition 3.4.5. Let $A \subset R$ be a subset

- 1) (A) is the ideal given by $(A) = \bigcap_{I \supseteq A} I$ (smallest ideal containing A)
- 2) Ideals generated by a single element are called principal ideals.
- 3) An ideal generated by a finite set is called finitely generated. For $A = \{a\}$ or $A = \{a_1, \dots, a_r\}$ write $(A) = (a)$ or $(A) = (a_1, \dots, a_r)$. Another way to interpret this:

$$(A) = \{r_1 a_1 + \dots + r_n a_n \mid r_i \in R, a_i \in A, n \in \mathbb{Z} > 0\}$$

Example 3.4.6.

- 1) $(0) = 0$ (0 ideal), $R = (1)$ (whole ring)
- 2) in \mathbb{Z} , $n\mathbb{Z} = (n)$ and every ideal in \mathbb{Z} is principal: $(n, m) = (\gcd(n, m))$. Also, $m\mathbb{Z} \subset n\mathbb{Z}$ iff $n \mid m$.
- 3) in $\mathbb{Z}[x]$, the ideal $(2, x)$ is not principal.
 $(2, x) = \{2p(x) + xq(x) \mid p(x), q(x) \in \mathbb{Z}[x]\}$. Note: $(2, x) \neq \mathbb{Z}[x]$
 Suppose $(2, x) = (\alpha(x))$, $2 \in (\alpha(x))$ so $2 = \alpha(x)p(x)$ for some $p(x)$ so $\alpha(x), p(x)$ are both constants and $\alpha(x), p(x) = \{\pm 1, \pm 2\}$. Since $(\alpha(x)) \neq \mathbb{Z}[x]$, $\alpha(x) \neq \pm 1$. If $\alpha(x) = \pm 2$, $x \in (2, x)$ so $x = \pm 2q(x)$, not possible since $q(x)$ has integral coefficients.

Proposition 3.4.7. I an ideal of R .

- (1) $I = R \leftrightarrow I$ contains a unit.
- (2) (R commutative) R is an ideal \leftrightarrow the only ideals of R are (0) and R .

Proof.

- (1) \rightarrow $I = R$, R contains 1 which is a unit
 \leftarrow If u is a unit in I with inverse v , for $r \in R$, $r = r \cdot 1 = r(vu) = (rv)u \in I$.
- (2) \rightarrow If R is a field, every element is a unit so follows from (1).
 \leftarrow If (0) and (R) are the only ideals of R . If $u \neq 0$, $u \in R$ $(u) = R$ so $1 \in (u)$ so $\exists v \in R$ such that $uv = 1$ so u is a unit. Hence, R is a field.

Corollary 3.4.8. IF R is a field, any nonzero homomorphism from R to another ring is injective.

Proof. R has ideals $(0), R$. If $\varphi : R \rightarrow S$ is homomorphism, since $\ker \varphi$ is an ideal, if $\ker \varphi \neq R$ then $\ker \varphi = 0$ so φ is injective.

An important class of Ideals: Those that are not contained in any other proper ideal.

Definition 3.4.9. An ideal M of R is maximal if $M \neq R$ and the only ideals containing M are M and R . (ie. if $M \subseteq I \subseteq R$, and I is an ideal, $I = M$ or $M = R$)

Zorn's Lemma: Let (A, \leq) be a partially ordered set. Then if every chain $x_1 \leq x_2 \leq \dots$ has an upper bound in A , then A has a maximal element. (Equivalent to axiom of choice)

Proposition 3.4.10. Let R be a ring. Then every ideal $I \neq R$ is contained in a maximal ideal of R .

Proof. Let R be a ring, I an proper ideal. Let $S = \{K \mid K \text{ ideal}, I \subset K \subsetneq R\}$ ordered by inclusion \subseteq . Construct a chain $C : J_1 \subset J_2 \subset J_3 \subset \dots$ in S . Let $J = \bigcup_{J_i \in S} J_i$, we see that J is an ideal, J contains I , $J \neq R$ otherwise J contains a unit so some J_i contains a unit so $J_i = R$ (not possible) so J is an upper bound of the chain so by Zorn's Lemma, S has a maximal element which is the maximal ideal M .

Proposition 3.4.11. (R commutative) M is a maximal ideal of $R \leftrightarrow R/M$ is a field.

Proof. M is a maximal ideal \leftrightarrow there is no ideal in R such that $M \subsetneq I \subsetneq R$. Also, the ideals of R containing M correspond to the ideals of R/M so M is maximal \leftrightarrow only ideals of R/M are (0) and $R/M \leftrightarrow R/M$ is a field.