MATH 113: Abstract Algebra

Jad Damaj

Spring 2022

Contents

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 $\mathbb{N} := \{1, 2, 3, \ldots\}$ with $+, \times$
- the integers $\mathbb{Z} := \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ 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

- $P \to Q$ 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:

- $S = \{$Notation for elements in $S|$ properties specifying being in $S\}$
  Ex: $\{x \in \mathbb{Z} | 2 \text{ divides } x\}$, $\{1, 2, 3, \dots, \}$, $\{1, 2, 3\}$
- 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 $S \sqcup T$)
- $S \times T = \{(a, b) | a \in S, b \in T\}$ - Cartesian product of S and T
- The set that contains no objects is called the empty set, $\emptyset$

1.1.3 Maps/Functions

- $f : A \to B$ 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: $S = \mathbb{N}, T = \mathbb{N} \quad f : \mathbb{N} \to \mathbb{N} \quad a \mapsto a^2$
- We say f is well defined if $a_1 = a_2 \to f(a_1) = f(a_2)$ $\forall a_1, a_2 \in A$
- The set $f(A) = \{b \in B | b = f(a) \text{ for some } a \in A\}$ is a subset of B called the range or image of f
- The set $f^{-1}(C) = \{a \in A | f(a) \in C\}$ is called the preimage of C under f $(C \subset B)$
- We say f is injective if $f(x) = f(y) \to x = y$ $\forall x, y \in A$
- We say f is surjective if given $b \in B$ $\exists a \in A$ 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 $f(a) = a$ $\forall a \in A$. In this case we write $f = \text{Id}_A$
- if $f : A \to B$ and $g : B \to C$, the composite map $f\dot{g} : A \to C$ is defined by $(g\dot{f})(a) = g(f(a))$

1.1.4 Equivalence Relations

Let A be a nonempty set. A binary relation on as 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: $a \sim b \to b \sim a \ \forall a, b \in A$
- transitive: $a \sim b$ and $b \sim c \to a \sim c \ \forall a, b, c \in A$

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

Example 1.1.2. Consider the binary relation on $\mathbb{Z} \times \mathbb{Z}$ given by $(x, y) \in R$ if $2|x - y$. We will show $\sim$ is an equivalence relation:
reflexiveness: $x - x = 0$ so $2|0 = x - x$ for all $x \in \mathbb{Z}$
symmetricness: Suppose $2|x - y$. Since $(x - y) = -(y - x)$, $2|y - x$ for all $x, y \in \mathbb{Z}$
transitivity: If $2|x - y$ and $2|y - z$ then $2|x - y + y - z$ so $2|x - z$
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 $2|x - y$"

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

- If x is even, $x = 2n$ for some $n \in \mathbb{Z}$ then $2|y - 2n \to y$ 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 $2|y - 2n - 1 \to y$ 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 $a|b$ (if a does not divide b, write $a \not| b$)
- 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. $d|a$ and $d|b$
  2. If $e|a$ and $e|b$, then $e|d$
- If $a, b \in \mathbb{Z} \setminus \{0\}$ there is a unique positive integer l, called the least common divisor satisfying:
  1. $a|l$ and $b|l$
  2. If $a|m$ and $b|m$, then $l|m$

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 $a = q_0 b + r_0$, $b = q_1 r_0 + r_1$, $r_0 = q_2 r_1 + r_2$, ..., $r_{n-2} = q_n r_{n-1} + r_n$, $r_{n-1} = q_{n+1} r_n$ where r_n is the last nonzero remainder, $r_n = \gcd(a, b)$

Because of division algorithm, $|b| > |r_0| > |r_1| > \cdots > |r_n|$ is a deceasing 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. $r_0 = a - q_0 b$ so if $d|b$ and $d|a$, $d|a - q_0 b = r_0$
Also $r_0 + q_0 b = a$ so if $d|b$ and $d|r_0$, $d|r_0 + q_0 b = a$ □

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

Example 1.2.2. Calculate $\gcd(35, 20)$
$25 = 20 \cdot 1 + 5$, $20 = 15 \cdot 1 + 5$, $15 = 5 \cdot 3 + 0$ so $\gcd(35, 20)$ =$\gcd(15, 5) = 3$

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 $15 \not| 3, 15 \not| 5$

Proof. If $p \not| a$ 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 $p|bau + pbv$ 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 $p_1, \ldots, p_s$ and positive integers $d_1, \ldots, d_s$ 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, $p_1, \ldots, p_n$. Consider $p_1 \cdots p_n + 1$ by FTA there is a prime factorization so at least one prime divides it. Can't be $p_1, \ldots, p_r$ 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 $a \equiv b \mod m$.

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 clasess: $\mathbb{Z}/m\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}$

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

Definition 1.2.11. We define addition and multiplication on $\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ 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 $a_1 \equiv b_1 \mod m$, then $m|a1 - b - 1$ so $a_1 = b_1 + sm$ for $s \in \mathbb{Z}$
  Also $a_2 \equiv b_2 \mod m$ so $a_2 = b_2 + tm$ for $t \in \mathbb{Z}$
  $(a_1 + a_2) = b_1 + b_2 + (s+t)m$ so $a_1 + a_2 \equiv b_1 + b_2 \mod m$ also $a_1 a_2 = (b_1 + sm)(b_2 + tm) = b_1 b_2 + (b_1 t + b_2 s + stm)m$ so $a_1 a_2 \equiv b_1 b_2 \mod m$ □

- $[0] \in \mathbb{Z}/m\mathbb{Z}$ 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 $ax \equiv 1 \mod m$ 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 $au \equiv 1 \mod m$

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 $* : G \times G \to G$. 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 from 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 moniod 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 $= GL_n(\mathbb{R}) := \{M \in M_n(\mathbb{R}) | \det(M) \neq 0\}$.
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 $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ 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 $*$ them,

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 associatvity 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 $|x| = \infty$.

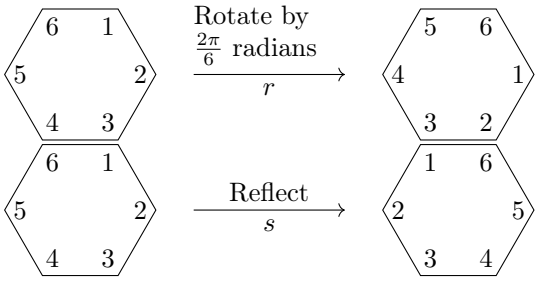
Example 2.2.12.

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

2.2.2 Dihedral Groups

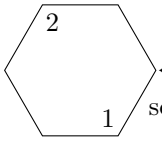
- The elements are symmetries of geometric objects
- Consider regular $n - gons$ for $n \geq 3$

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 $\{1, \ldots, 6\} \to \{1, \ldots, 6\}$. 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



← No way to do this without breaking the hexagon
so $\sigma(1) = 3, \sigma(2) = 6$ is not one of the symmetries

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 $2n$.

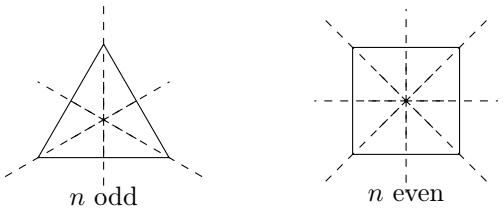
Why is $|D_{2n}| = 2n$?
For any vertex i, there is a symmetry that sends 1 to the vertex i. The vertex 2 (next to 1) must go either to the vertex $i+1$ or $i-1$. So you have n choices for where to send the vertex "1" and 2 choices for where to send to vertex "2". So there are $n \cdot 2$ choices for 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) $1, r(\frac{2\pi}{6}), r^2(\frac{4\pi}{6}), r^3(\pi), r^4(\frac{8\pi}{6}), r^5(\frac{10\pi}{6}), r^6(2\pi) = 1$
$1, r, \ldots, r^5$ all distinct so $|r| = 6$

(ii) $s^2 = 1$ so $|s| = 2$

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

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

(v) $r^i \neq sr^j$ 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.
$D_{12} = \{r^i s^j | i = 0, \ldots, n-1\, j = 0, 1\}$ 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, $\sigma : \Omega \to \Omega$, $\tau : \Omega \to \Omega$, then $\sigma \circ \tau$ is a bijection $\Omega \to \Omega$.
- The identity of S_Ω is the permutation 1 defined by $1(a) = a \, \forall a \in \Omega$.
- Every permutation has an inverse $\sigma^{-1} : \Omega \to \Omega$ such that $\sigma^{-1} \circ \sigma = \sigma \circ \sigma^{-1} = 1$.
- Composition of functions is associative so $\circ$ is associative.
- Thus, $(S_\Omega, \circ)$ is a group called the symmetric group of S_Ω
- Often we will use $\Omega = \{1, \ldots, n\}$- will write S_n instead of S_Ω

Example 2.3.2. $\Omega = \{1, 2, 3\}$
Let σ be in S_Ω sending $\sigma(1) = 2$, $\sigma(2) = 3$, $\sigma(3) = 1$.
$\begin{pmatrix} \sigma : & 1 \to 2 \\ & 2 \to 3 \\ & 3 \to 1 \end{pmatrix}$ We write $(1\,2\,3)$ to represent σ.
$\tau \in S_\Omega$ by $\tau(1) = 2$, $\tau(2) = 1$, $\tau(3) = 3$
$\begin{pmatrix} \tau : & 1 \to 2 \\ & 2 \to 1 \\ & 3 \to 3 \end{pmatrix} = (1\,2)(3)$. 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 numbers in 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. $(1\,2\,3) \circ (1\,2)(3\,4)$
$\tau : 1 \to 2 \quad \sigma : 2 \to 1$ so $\sigma \circ \tau : 1 \to 3$
$\tau : 3 \to 4 \quad \sigma : 4 \to 4$ so $\sigma \circ \tau : 4 \to 4$
$\tau : 4 \to 4 \quad \sigma : 3 \to 1$ so $\sigma \circ \tau : 4 \to 1$
$\tau : 2 \to 1 \quad \sigma : 1 \to 2$ so $\sigma \circ \tau : 2 \to 2$
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 $\varphi : G \to H$ 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 $\varphi : G \to H$ is called an isomorphism (G, H are isomomorphic, 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 if an endomorphism is an isomorphism then it is called an automorphism.

Example 2.4.5.

(1) $\varphi : (\mathbb{Z}, +) \to (\mathbb{Q}, +)$ 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) $\varphi : (\mathbb{Z}, +) \to (\mathbb{Z}/m\mathbb{Z}, +)$ 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 $\varphi : G \to G$ by $x \mapsto x$ is an isomorphism (also an automorphism.)

(4) Let $\mathbb{R} := \{x \in \mathbb{R} | x > 0\}$. The exponential map, exp: $(\mathbb{R}, +) \to (\mathbb{R}^+, \times)$ 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 $\varphi : G \to H$ 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 $f : G \to H$ and $g : H \to M$ be homomorphisms. Then $g \circ f : G \to M$ 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 $\varphi : G \to H$ 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 ableian.
$\leftarrow$) Assume H is abelian. Let x, y in G be arbitrary. Consider $\varphi(xy) = \varphi(x)\varphi(y)$. Since H is ableian, $\varphi(xy) = \varphi(y)\varphi(x) = \varphi(yx)$. Since φ is an isomorphism, it is injective so it follows that $xy = yx$. Thus, G is abelian.

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

Proof. To show this for all nonegative 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 $\varphi : G \to H$ 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 $\varphi(e_G) = e_H$. □

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 $x, y \in H \cap K$, 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 $H \neq 0$ 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. $C_G(A) = \{g \in G | gag^{-1} = a \, \forall a \in A\}$. $C_G(A)$ is called the centralizer of A. It consists of the set of elements in G that comute 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, $xya(xy)^{-1} = xyax^{-1}x^{-1} = x(yay^{-1})x^{-1} =$

$xax^{-1} = a$ 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. □

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 $N_{D_8}(A) = D_8$. □

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 $r^3 s = sr^{-3} \neq sr^3$. $r^2 s = sr^{-2} = sr^2$ so r^2 and s commutes. Also $r^2 sr^i = sr^2 r^i = sr^i r^2$ so r^2 commutes with D_8. Thus $Z(D_8) = \{1, r^2\}$. □

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) $(\mathbb{Z}/m\mathbb{Z}, +) = \langle [1] \rangle = \{[1], [2], \ldots, [m-1], [0]\}$

Remark 2.6.3. Generators need not be unique.

Cyclic groups are abelian.

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

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 $|x| = n$, $\{1, x, \ldots, x^{n-1}\}$ 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 $x^t = x^{nq+r} = (x^n)^q x^r = 1^q x^r = x^r \in \{1, x, \ldots, x^{n=1}\}$. 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 $n \not| a$, 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 infinte, $G \cong (\mathbb{Z}, +)$
2. If G if finite and $|G| = m$, $G \cong (\mathbb{Z}/m\mathbb{Z}, +)$

Proof.

(1) Let $G = \langle x \rangle$, $\varphi : G \to \mathbb{Z}$ by $x^n \mapsto n$
Well defined: $x^a = x^b \to a = b$ by previous proposition
Injective: $a = b \to x^a = x^b$
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 $|G| = m$, $G = \langle x \rangle$, $\varphi : G \to \mathbb{Z}/m\mathbb{Z}$ 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 $x^r = x^s \to \varphi(x^s) = \varphi(x^r)$ 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 $\{1, x, \ldots, x^{m-1}\}$ are all distinct so $G = \{1, x, \ldots, x^{m-1}\}$ and $\mathbb{Z}/m\mathbb{Z} = \{[0], [1], \ldots, [m-1]\}$. So each element in $\mathbb{Z}/m\mathbb{Z}$ has a preimage.
Injective: WTS $[a] = [b] \to x^a = x^b$. Suppose $x^a \neq x^b$, then $x^{a-b} \neq 1$ so $m \not| a - b$ so $a \not\equiv b \mod m$ 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 $|y||b$.
Let $k = |y|$, we have $k|b$, WTS $b|k$. $x^{ak} = y^k = 1$ so $n|ak$ so $db|dck$ so $b|ck$. Since $\gcd(b,c) = 1$, $b|k$.

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

Consider D_{16}. Let $R = \{1, r, \ldots, r^7\}$. 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. $\mathbb{Z}/12\mathbb{Z} = \{[0],[1],\ldots,[11]\}$.
[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

(a) Every subgroup of H is cyclic.

(b) If $|H| = n < \infty$, for each positive integer a dividing n, there is a unique subgroup of H of order a.

Proof.

(a) Let $K = \langle x\rangle$. If $K = \{1\}$ we are done.
Otherwise, let $a = \min\{k > 0$ such that $x^k \in H\}$. Claim: $K = \langle x^a\rangle$
Suppose not (suppose $\exists\ x^b \in K$ with $a \not| b$). 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 $a|b$ $\forall b$ with $x^b \in K$.

(b) $|H| = n < \infty$, $a|n$. $x^{n/a}$ 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 $x^{ku} = x^{ku+nv} = x^{a/n} \in \langle x^k\rangle$. 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 $\gcd(b,12)|\gcd(a,12)$.

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,

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

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.

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

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

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

Proof. Using the subgroup criterion we will show $\overline{A}$ is a subgroup.
$\overline{A}\neg\emptyset$ since $A = \emptyset \to \overline{A} = \{1\}$. If $a, b\in\overline{A}$. $a_1^{\varepsilon_1}a_2^{\varepsilon_2}\cdots a_n^{\varepsilon_n}, b = b_1^{\delta_1}b_2^{\delta_2}\cdots b_m^{\delta_m}$ 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. $\langle(1\,2),(1\,3)(2\,4)\rangle\leq S_4$ is isomorphic to D_8.

2.7.3 Quotient Groups

Definition 2.7.9. If $\varphi: G\to H$ 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 $\mathrm{im}(\varphi) = \{\varphi(x)|x\in G\}$

Proposition 2.7.10. Let H, G be groups, $\varphi: G\to H$ a homomorphism, the kernel of φ is a subgroup of G and $\mathrm{im}\varphi$ 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 $\varphi(xy^{-1}) = \varphi(x)\varphi(y^{-1}) = \varphi(x)\varphi(y^{-1}) = \varphi(x)\varphi(y)^{-1} = e_H e_H^{-1}$ so $xy^{-1} \in \ker\varphi$ so $\ker\varphi \leq G$.

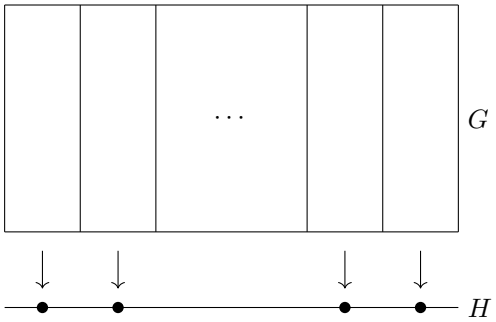
Proof ((Image)). $\varphi(e_G) = e_H \in \text{im}\varphi$ so $\text{im}\varphi \neq \emptyset$.
If $x, y \in \text{im}\varphi$, say $x = \varphi(a)$, $y = \varphi(b)$ $a, b \in G$ then $y^{-1} = (\varphi(b))^{-1} = \varphi(b^{-1})$, so $xy^{-1} = \varphi(a)\varphi(b^{-1}) = \varphi(ab^{-1})$ so $xy^{-1}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

2.8 February 15

2.8.1 Quotient Groups

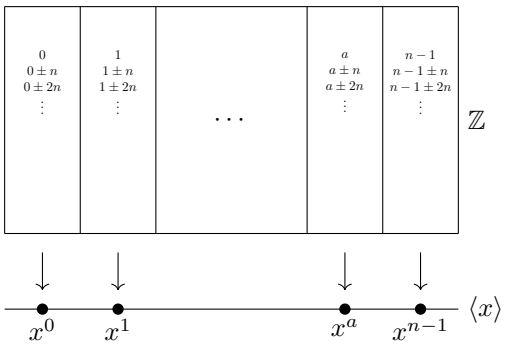
Another way to make a (smaller) group out of a given group.

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



$\varphi : G \to H$ is surjective
Regions in G are fibers of the points in H

Example 2.8.1. $G = \mathbb{Z}$, $H = \langle x \rangle$, $|x| = m$. $\varphi : \mathbb{Z} \to \langle x \rangle$ 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 $\{n, 1, \ldots, n-1\} \to \{1, x^1, \ldots, x^{n-1}\}$
The fiber of φ over x^a: $\varphi^{-1}(a) = \{m \in \mathbb{Z} | x^m = a\} = \{m \in \mathbb{Z} | x^{m-a} = 1\} = \{m \in \mathbb{Z} | n | m - a\} = \{m \in \mathbb{Z} | m \equiv a \mod n\} = [a]$



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 $\varphi : G \to H$ be a homomorphism with kernel K. Then the quotient group "G mod 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 $\varphi : G \to H$ 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. $X \in G/K \to X = gK$.
We can define multiplication by choosing coset representatives.

Theorem 2.8.6. $\varphi : G \to H$ 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 $uv \in Z$, $Z = uvK$. □

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 $\varphi : G \to H$ uK, vK with $uKvK = uvK$

Can we generalize quotient groups to any subgroup N?

Claim: If $\varphi : G \to H$ 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 $\varphi(gKg^{-1}) = \varphi(g)e\varphi(g^{-1}) = \varphi(g)e\varphi(g)^{-1} = e$ □

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 $x_1N = x_2, y_1N = y_2N$, 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 $x_1y_1N = x_2y_2N$. □

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. □

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 $\varphi : G \to H$, $\ker(\varphi) \trianglelefteq G$.

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

Proposition 2.9.3. For $H \trianglelefteq G$, the map $\varphi : G \to G/H$ 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 $|H| \,|\, |G|$ 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 $H \to gH$ by $h \mapsto gh$ is a bijection so $|H| = |gH| = n$. Thus, $|G| = nk$ so $|H| \,|\, |G|$ and $k = \frac{|G|}{n} = \frac{|G|}{|H|}$.

Definition 2.9.6. The number of cosets if 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 $|x| \,|\, |G|$ and $x^{|G|} = 1$.

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

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 $|\langle x \rangle| \,|\, |G|$ so $|\langle x \rangle| = p = |G|$ so $G = \langle x \rangle$ so G is cylic.

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, $n| \, |G|$ then G need not have a subgroup of order n.

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

Slyow's Thm: If $|G| = p^\alpha m$, $p \not| m$ 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 $\varphi : G \to H$ be a homomorphism, $\ker \varphi \trianglelefteq G$. It makes sense to form $G/\ker \varphi \ \{g \ker \varphi | g \in G\}$, 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, $\varphi : G \to H$ a homomorphism, then $G/\ker(\varphi) \cong \text{im}\varphi$.

Proof. Consider $\psi : G/\ker \varphi \to \text{im}\varphi$ by $x \ker \varphi \mapsto \varphi(x)$. WTS ψ is an isomorphism. By def of imφ, 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 φ 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) $(\mathbb{Z},+) \hookrightarrow (\mathbb{Q},+)$, $\varphi : \mathbb{Z} \to \mathbb{Q}$ 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) $(\mathbb{Z},+) \twoheadrightarrow (\mathbb{Z}/m\mathbb{Z},+)$, $\varphi : \mathbb{Z} \to \mathbb{Z}/m/mZ$ 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) $\varphi : G \to H$ by $g \mapsto e_H$. $\ker\varphi = G$, $\text{im}\varphi = e_H$ so $G/G \cong e_H$.

Corollary 2.10.3. If $\varphi : G \to H$ 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)**.** $\to$) 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 $\varphi(g_1) = \varphi(g_2) \leftrightarrow \varphi(g_1)\varphi(g_2)^{-1} = e \leftrightarrow \varphi(g_1)\varphi(g_2^{-1}) = e \leftrightarrow e(g_1g_2^{-1}) = e \leftrightarrow g_1g_2^{-1} \in \ker\varphi$ 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 $\varphi : G/H \to G/K$ 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 $\text{im}\varphi = G/K$.
$\ker\varphi = \{gH \in G/H | \varphi(gH) = eK\} = \{gH \in G/H | gK = eK\} = \{gH \in G/H | g \in K\} = K/H$. So by the first isomorphism theorem, $G/H \,/\, G/H \cong G/H$.

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

2.11.1 Group Actions

We'll let groups act on sets (and on themselves later)

Applications:

Cayley's Thm: Every group of order n is isomorphic to a subgroup of S_n.

Sylow's Thm: existence? Number of subgroups of a certain order.

Definition 2.11.1. A group of order G on a set A is a map $G \times A \to A$ (we write $g \cdot a$ for $g \in G$, $a \in A$) satsifying:

(1) $g_1 \cdot (g_2 \cdot a) = g_1 g_2 \cdot a \ \forall g_1, g_2 \in G,\ a \in A$

(2) $1 \cdot a = a \ \forall a \in A$

For each g we can define the map $\sigma_g : A \to A$ by $a \mapsto g \cdot a$.

Lemma 2.11.2. For each element $g \in G$, σ_g is a permutation and $\varphi : G \to S_A$ by $g \mapsto \sigma_g$ is a homomorphism.

Proof. σ_g is a permutation from $A \to A$. We can show it is a bijection since there is an inverse for $g \in G$ given by $g^{-1} \in G$.
$\sigma_g \circ \sigma_{g^{-1}} = g \cdot (g^{-1} \cdot a) = (gg^{-1})(a) = 1 \cdot a = a$, and
$\sigma_{g^{-1}} \circ \sigma_g = g^{-1} \cdot (g \cdot a) = (g^{-1}g)(a) = 1 \cdot a = a$.
To show φ is a homomorphism, WTS $\varphi(g_1 g_2) = \varphi(g_1) \circ \varphi(g_2)$.
$\varphi(g_1 g_2)(a) = \sigma_{g_1 g_2}(a) = g_1 g_2 \cdot a = g_1 \cdot (g_2 \cdot a) = \sigma_{g_1}(\sigma_{g_2}(a)) = (\varphi(g_1) \circ \varphi(g_2))(a)$

Definition 2.11.3. φ is called the permutation representation.

We know {actions of G on A} $\leftrightarrow$ { homomorphism $G \to S_A$}.
We just showed "$\to$", the other direction works too.
Given $\psi : G \to S_A$, consider $G \times A \to A$ by $g \cdot a = \psi(g)(a)$.

Definition 2.11.4. The stabilizer of a in G is the set $G_a = \{g \in G | g \cdot a = a\}$ ($G_a \leq G$)

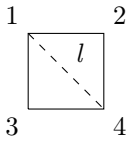
Definition 2.11.5. The kernel of the action of G on A is $\{g \in G | g \cdot a = a \forall a \in A\}$.

Remark 2.11.6. $\ker \varphi$ is the same as "the kernel of the action of G on A"

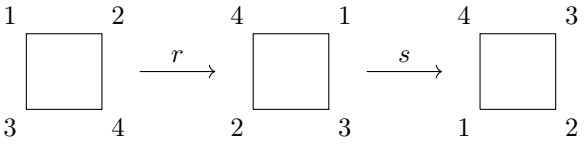
Example 2.11.7.

1. let $g \cdot a = a \ \forall g \in G \ \forall a in A$. $\sigma_g : A \to A$ is $a \mapsto a$ so $\varphi : G \to S_A$ is $g \mapsto$id.
2. For any nonempty set A, S_A acts on A by $\sigma \cdot a = \sigma(a)$ for all $\sigma \in S_A$, $a \in A$. $\varphi : S_A \to S_A$ by $\sigma \mapsto \sigma$.

Example 2.11.8. $G = D_8$ $A = \{1\,2\,3\,4\}$
r =rotation, s = reflection across l.



$\varphi : D_8 \to S_4$ by $r \mapsto (1\,2\,3\,4) = \sigma_r$, $s \mapsto (2\,4) = \sigma_s$.
$\varphi(sr) = \sigma_{sr} = \sigma_s \circ \sigma_r = (2\,4)(1\,2\,3\,4) = (1\,4)(2\,3)$.



Stabilizer of vertices 1,3: $\{s, 1\} = \langle r \rangle$
Stabilizer of vertices 2,4: $\{sr^2, 1\} = \langle sr^2 \rangle$
Kernel of action: $\{1\}$

Proposition 2.11.9. Let G be a group acting on a nonempty set A, then the relation defined by $a \sim b$ iff $a = g \cdot b$ for some $g \in G$ is an equivalence relation. For $a \in A$ the number of elements in the equivalence class of a is equal to $[G : G_a]$.

Proof. Since $1 \cdot a = a$, $a \sim a$.
If $a \sim b$, $a = g \cdot b$ for some $g \in G$ so $g^{-1} \cdot a = g^{-1} \cdot g \cdot b = g^{-1}g \cdot b = 1 \cdot b = b$ so $b = g^{-1} \cdot a$, $g^{-1} \in G$ so $b \sim a$.
Finally, if $a \sim b$, $b \sim c$, $a = g \cdot b$, $b = h \cdot c$ for $g, h \in C$. $a = g \cdot b = g \cdot h \cdot c = gh \cdot c$ so $a = gh \cdot c$ for $gh \in G$ so $a \sim c$.
Now, let $C_a = \{g \cdot a | g \in G\}$ the equivalence class of a. We'll set up a bijection between the elements of C_a and the cosets of G_a.
Suppose $b = g \cdot a \in C_a$. Then gG_a is a coset of G_a in G. Define the map $C_a \to \{$ left cosets of G_a in $G\}$ by $b = g \cdot a \mapsto gG_a$. The map is surjective because for $g \in G$, $g \cdot a \in C_a$. Also injective because $g \cdot a = h \cdot a \leftrightarrow hg^{-1} \cdot a = a \leftrightarrow h^{-1}g \in G_a \leftrightarrow hG_a = gG_a$.

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 $\{g \cdot a | g \in G\}$ =orb a is called the orbit of a (orbit containing a in G)

(2) The action of G on A is called transitive if ther 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 $\underset{1}{a_1 H_1}, \ldots, \underset{n}{a_n H_n}$ (labels)
Can define σ_g as $\sigma_g(i) = j$ iff $g \cdot a_i H = a_j H$.

Example 2.12.3. $G = D_8$, $H = \langle s \rangle = \{1, s\}$, $A = \{\underset{4}{1H}, \underset{1}{rH}, \underset{2}{r^2 H}, \underset{3}{r^3 H}\}$ $\leftarrow$labels
Computing σ_s:
$s \cdot 1H = s1H = H = 1H \qquad \sigma_s(4) = 4$
$s \cdot rH = srH = r^{-1}sH = r^{-1}H = r^3 H \qquad \sigma_s(1) = 3$
$s \cdot r^2 H = sr^2 H = r^{-2}sH = r^{-2}H = r^2 H \qquad \sigma_s(2) = 2$
$s \cdot r^3 G = sr^H = r^{-3}sH = r^{-3}H = r^1 H \qquad \sigma_2(3) = 1$
so $\sigma_s = (1\,3)$. Similarly, $\sigma_r = (1\,2\,3\,4)$.

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 ation is 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 $\varphi : G \to S_n$. $\ker \varphi \leq H$, 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 $\{gH\}$. $\varphi : G \to S_p$. Let $K = \ker\varphi$ $[H:K] = k$, $[G:H][H:K]$. H has p cosets so $G/K \cong$subgroup S_p so $|G/k| \,|\, p!$. $|G/K| = pk$ so $pk|p!$ so $k|(p-1)!$. Since $|G|$ has no prime divisors less than p, $|G/K|$ has no prime divisors less than p. $(p-1)!$ has no primes 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 $G_S = \{g \in G | gSg^{-1}\} = N_G(s)$.

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. $g_1, \ldots, g_r$ 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 $Z(G) = \{1, z_2, \ldots, z_m\}$, let g_i be a representative of K_i with $K_1, \ldots, K_r$ list of all noncentral conjugacy classes (more than 1 element).
$\{1\}, \{z_2\}, \ldots, \{z_m\}, K_1, \ldots, K_r$ 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 $|D_8| = |Z(D_8)| + \sum_{\substack{i=r,\\ s,sr}}[G : C_G(x)]$ 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 $p|[G : C_G(g_i)]$ $\forall i$ so $p|\sum_{i=1}^{r}[C : C_G(g_i)]$ and $p \,|\, |G|$ so $p \,|\, |Z(G)|$ so $Z(G)$ is nontrivial.

Corollary 2.13.8. If $|G| = p^2$ (p prime) then G is abelain. ($G \cong \mathbb{Z}/p^2\mathbb{Z}$ 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 cylcic 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:

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

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.

(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 2.13.11. 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 $G_S = \{g \in G | gSg^{-1}\} = N_G(s)$.

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. $g_1, \ldots, g_r$ 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 $Z(G) = \{1, z_2, \ldots, z_m\}$, let g_i be a representative of K_i with $K_1, \ldots, K_r$ list of all noncentral conjugacy classes (more than 1 element).
$\{1\}, \{z_2\}, \ldots, \{z_m\}, K_1, \ldots, K_r$ 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.

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

(1) $D_8 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$.
$\text{orb}(r) = \text{orb}(r^3) = \{r, r^3\}$ $\quad \text{orb}(sr) = \text{orb}(sr^3) = \{sr, sr^3\}$
$\text{orb}(s) = \text{orb}(sr^2) = \{s, sr^2\}$ $\quad Z(D_8) = \{1, r^2\}$
so $|D_8| = |Z(D_8)| + \sum_{\substack{i=r, \\ s, sr}} [G : C_G(x)]$ 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 $p | [G : C_G(g_i)]$ $\forall i$ so $p | \sum_{i=1}^{r} [C : C_G(g_i)]$ and $p \,|\, |G|$ so $p \,|\, |Z(G)|$ so $Z(G)$ is nontrivial.

Corollary 2.13.16. If $|G| = p^2$ (p prime) then G is abelain. ($G \cong \mathbb{Z}/p^2\mathbb{Z}$ 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 cylcic 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, $|G| = n$, $d|n \not\Rightarrow \exists$ 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 $p \,|\, |G|$ 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 $p \,|\, |x|$, 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 $p \not| |x|$. Let $N = \langle x \rangle x$. 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 $p \not| |N|$, $p \,|\, |G/N|$. By IH, G/N (smaller than G) contains an element of order p, $\overline{y} = yN$. $\overline{y} \neq \overline{1}$ so $\overline{y} \notin N$. Also, $\overline{y}^p = \overline{1}$ so $\overline{y}^p \in N$ 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 $p \,|\, |y|$. 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. Subgroups of G that are also p-groups are called p-subgroups.

(2) If G is a subgroup of order $p^\alpha m$ where $p \not| m$ 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 Slyow 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 $p \,|\, |Z(G)|$ then by the lemma $Z(G)$ has a subgroup of order p, call it N. Let $\overline{G} = G/N$, $|N| = p$ so $|G/N| = p^{\alpha-1}m$ so by IH $\overline{G}$ has a Sylow p-subgroup ($\overline{P}$ of order $p^{\alpha-1}$). Let P be the the subgroup of G containing N such that $P/N = \overline{P}$ (correspondence isomorphism theorem.) $|P| = |P/N||P| = p^{\alpha-1}p = p^\alpha$ so P is a Sylow p-subgroup of G.
- Suppose $p \not| |Z(G)|$. Let $g_1, \ldots, g_r$ 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 $p|[G : C_G(g_i)]$ $\forall i$ then $p \,|\, |Z(G)|$ contradicting

our assumption. So $p \not| [G : C_G(g_i)]$ for some i. Let $H = C_G(g_i)$, $|H| = p^\alpha k$, $p \not| k$. 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 if 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. $n_p(G) \equiv 1 \mod p$, $n_p = [G : N_G(p)]$ for P, any sylow p-subgroup $n_p(G)|m$.

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.
$n_2 \equiv 1 \mod 2$, $n_2|3$ so $n_2 = 1$ or 3. $Syl_2(S_3) = \{\langle(1\,2)\rangle, \langle(2\,3)\rangle, \langle(1\,3)\rangle\}$
$n_3 \equiv 1 \mod 3$, $n_3|2$ so $n_3 = 1$. $Syl_3(S_3) = \{\langle(1\,2\,3)\rangle\}$

2.15 March 17

2.15.1 Direct Products

$(G_1, *_1), \ldots, (G_n, *_n)$ groups

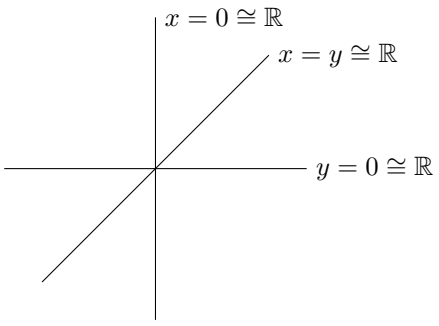
Definition 2.15.1. The direct product $G_1 \times \cdots \times G_n$ is the set of n-tuples $(g_1, \ldots, g_n)$, $g_i \in G$ and the group operation is defined componentwise.

$$(g_1, \ldots, g_n) * (h_1, \ldots, h_n) = (g_1 *_1 h_1, \ldots, g_n *_n h_n)$$

Example 2.15.2. $G_1 = \mathbb{Z}$, $G_2 = S_3$, $G_3 = \mathbb{Q} \setminus \{0\}$
$G = G_1 \times G_2 \times G_3$, $(m, \sigma, w) * (n, \tau, v) = (m + n, \sigma \circ \tau, wv)$

Proposition 2.15.3. If $G_1, \ldots, G_n$ are groups, their direct product is a group of order $|G_1| \times \cdots \times |G_n|$.

Example 2.15.4. $\mathbb{R} \times \mathbb{R}$



Any line through the origin is a copy of $\mathbb{R}$.

Proposition 2.15.5. Let $G_1, \ldots, G_n$ be groups, $G_1 \times \cdots \times G_n$ their direct product

(1) For each fixed i, $G_i \cong \{(1, \ldots, 1, g_1, 1, \ldots, 1) | g_i \in G_i\}$. Identify G_i with this subgroup. Then $G_i \trianglelefteq G$, $G/G_i \cong G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times G_n$.

(2) For each i, $\pi_i : G \to G_i$ is defined by $(g_1, \ldots, g_n) \mapsto g_i$.
$\ker \pi_j = \{(g_1, \ldots, g_{i-1}, 1, g_{i+1}, \ldots, g_n) | g_j \in G\} \cong G_1 \times \cdots G_{i-1} \times G_{i+1} \times \cdots \times G_n$.

(3) If $x \in G_i$, $x \in G_j$, $i \neq j$ $xy = yx$.

Proof.

(1) $H = \{(1, \ldots, 1, g_i, 1, \ldots, 1) | g_i \in G_i\}$ can show its a subgroup.
Let $\psi : G_i \to H$ by $g_i \mapsto (1, \ldots, 1, g_i, 1, \ldots, 1)$ can be shown to be an isomorphism. Identify G_i with H.
$\varphi : G \to G_1 \times \cdots G_{i-1} \times G_{i+1} \times \cdots \times G_n$ by $(g_1, \ldots, g_n) \mapsto (g_1, \ldots, g_{i-1}, g_{i+1}, \ldots, g_n)$ can show φ is a homomorphism, φ is surjective so $\text{im}\varphi = G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n$. $\ker \varphi = \{(g_1, \ldots, g_n) | g_i = 1 \, \forall i \neg j\} = \{(1, \ldots, 1, g_i, 1, \ldots, 1)\} = G_i$ so $G_i \trianglelefteq G$, by 1rst isomorphism theorem $G/G_i \cong G_1 \times \cdots G_{i-1} \times G_{i+1} \times \cdots \times G_n$.

Example 2.15.6. $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, p primes $\to G$ has exactly $p + 1$ subgroups of order p.
$|G| = p^2$, elements have order 1 or p so each nonidentity element has order p, $p^2 - 1$ of them. By Lagrange's theorem, distinct subgroups of order p have nontrivial intersection. Each subgroup has $p = 1$ nonidentity elements so $\frac{p^2-1}{p+1} = p + 1$ subgroups.

2.15.2 Finitely Generated Abelian Groups

Definition 2.15.7. A group G is finitely generated if there is a finite subset A of G such that $G = \langle A \rangle$.

If G is finitely generated and abelian, $A = \{a_1, \ldots, a_n\} \in G$ such that $x \in G$ can be written as $x = a_1^{\lambda_1} * \cdots * a_n^{\lambda_n}$, $\lambda_i \in \mathbb{Z}$.

Remark 2.15.8. If the a_i all have infinite order, the representation is unique. We call G a free abelian group.

Example 2.15.9. $\mathbb{Z}^R = \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{r \text{ terms}}$

Definition 2.15.10. $x \in G$ is called torsion if it is of finite order. Denote elements $TG \leq G$.
If $TG = \{\text{id}\}$, G is torsion free.
If $TG = G$, we say G is torsion.

Proposition 2.15.11. Let G be a finitely generated abelian group, G/TG is torsion free.

Proof. WTS if xTG is torsion, $x \in TG$. $TG \trianglelefteq G$ since G is abelian. Suppose xTG is torsion, $(xTG)^n = TG$ so $x^nTG = TG$ so $x^n \in TG$ so $\exists m$ such that $(x^n)^m = \text{id}$. So $x^{nm} = TG$ so $x \in TG$ and $xTG = TG$.

Theorem 2.15.12 (Fundamental Theorem of Finitely Generated Abelian Groups)**.** Let G be a finitely generated abelian group

(1) $G \cong \mathbb{Z}^r \times Z_{n_1} \times \cdots \times Z_{n_s}$ such that

- $r, n_i \in \mathbb{Z}$, $r \geq 0$, $n_i \geq 2$ $\forall i$
- $n_{i+1} | n_i$ for $1 \leq i \leq s-1$

(2) The expression is unique.

Definition 2.15.13. r is called the rank, n_i called the invariant factors of G.

Remark 2.15.14. Two finitely generated abelian groups, are isomorphic iff they have the same rank and list of invariant factors.

- A finitely generated abelian group is finite if $r = 0$
- theorem gives us an effective way to list all finite abelian groups of a certain order.

Enumerate positive $n_1, \ldots, n_s$ such that

(1) $n_j \geq 2$ $\forall j \in \{1, \ldots, s$

(2) $n_{i+1} | n_i$ $\forall i \in \{1, \ldots s-1\}$

(3) $n_1 \ldots n_s = n$

Note that n_1 is the largest invariant factor, also $n_i | n$.

- If $p | n$ then $p | n_1$ since $p | n_1 \cdots n_s$ so $p | n_i$ for some i si $p | n_1$
- In particular if n is the product of distinct primes $n = n_1$

Corollary 2.15.15. IF n is the product of distinct primes, up to isomorphism, the only abelian group of order n is $\mathbb{Z}/n\mathbb{Z}$.r

2.16 March 29

2.16.1 Finitely Generated Abelain 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) $n_1 = 2 \cdot 3^2 \cdot 5$ $\quad G \cong \mathbb{Z}/90\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_s\mathbb{Z}$
$180 = 90 n_2 \cdots n_s$ so $2 = n_2 \cdots n_r$ so $n_2 = 2$
$G \cong \mathbb{Z}/90\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

(3) $n_1 = 2^2 \cdot 3 \cdot 5$ $\quad G \cong \mathbb{Z}/60\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$
$180 = 60 n_2 \cdots n_r$ so $3 = n_2 \cdots n_r$ so $n_2 = 3$
$G \cong \mathbb{Z}/60\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

(4) $n_1 = 2 \cdot 3 \cdot 5 \quad G \cong \mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_w\mathbb{Z}$
$180 = 30n_2 \cdots n_w$ so $6 = n_2 \cdots n_w$. Suppose $n_2 = 2$ (or $n_2 = 3$). Then $n_3 | n_2$ so $n_3 = 2$ (or $n_3 = 3$) but $n_1 n_2 n_3$ will be divisible by 2^3 (or 3^3) but 180 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 or 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, $A_i \cong \mathbb{Z}/p_i^{\beta_1}\mathbb{Z} \times \cdots \mathbb{Z}/p_i^{\beta_t}\mathbb{Z}$
$\beta_1 \geq \beta_2 \geq \cdots \geq 1$ 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. The correspond to invariant factors of subgroups of G.

Example 2.16.4. $|G| = 180 = 2^2 \cdot 3^2 \cdot 5$
$G = A_1 \times A_2 \times A_3 \quad |A_1| = 2^2$, $|A_2| = 3^2$, $|A_3| = 5$
$A_1 \cong \mathbb{Z}/4\mathbb{Z}$ or $A_1 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
$A_2 \cong \mathbb{Z}/9\mathbb{Z}$ 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 → set set with one binary operation
Now: Rings → 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
$(a \times b) \times c = a \times (b \times c)$ $\forall a, b, c \in R$

(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 $a \times 1 = 1 \times a = a$ $\forall a \in R$

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: $1 \in R \to (R, +)$ is abelian.
$(1+1) \times (a+b) = 1 \times (a+b) + 1 \times (a+b) = a+b+a+b$
or $= (1+1) \times a + (1+1) \times b = a+a+b+b$

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 $ua + vn = 1$.
$[u][a] + [0] = [1] \to [u][a] = [1] \quad (ua \equiv 1 \mod n)$

More Complex Examples: Let X be a nonempty set, A a ring. The set of functions $f : X \to A$ 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 $\gcd(n,a) > 1$, $b < n \to [b] \neq [0]$ 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 $b - c = 0 \to b = c$.

Corollary 3.2.12. Any finite integral domain is a field.

Proof. Let $a \neq 0$, $a \in R$. Consider $R \to R$ by $x \mapsto ax$. The map is injective since $ax_1 = ax_2 \to x_1 \to x_2$. 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 us an additive subgroup of R that is closed under multiplication and contains the multiplicative identity of R.

Example 3.2.14.

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

(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. □

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 $f(x) = a_0 + a_1x^1 + \cdots + a_nx^n$, $a_n \neq 0$ (largest such n)

- We say degree$(f) = n$
- $a_n = 1 \to f$ is monic
- operations:

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

$$(a_0 + a_1x + \cdots + a_nx^n)(b_0 + b_1x + \cdots + b_nx^n) =$$
$$(a_0b_0) + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \cdots + a_nb_nx^{2n}$$

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 doman.

(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 $(R[x])^\times \subset R^x$. 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 $\varphi : R \to S$ 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) $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ by $a \mapsto [a]$

$\pi(a+b) = [a+b] = [a] + [b] = \pi(a) + \pi(b)$
$\pi(ab) = [ab] = [a][b] = \pi(a)\pi(b)$

(2) $\varphi : \mathbb{Q}[x] \to \mathbb{Q}$ by $p(x) \mapsto p(0)$ (constant term)
$\varphi(p(x) + q(x)) = p(0) + q(0) = \varphi(p(x)) + \varphi(q(x))$
$\varphi(p(x)q(x)) = p(0)q(0) = \varphi(p(x))\varphi(q(x))$
$\ker\varphi = \{p(x) \mid p(0) = 0\}$ = 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 $n \in \mathbb{Z}$, $M_n; \mathbb{Z} \to \mathbb{Z}$ 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.
$\varphi(\alpha r) = \varphi(\alpha)\varphi(r) = 0\varphi(r) = 0$ so $\alpha r \in \ker\varphi$
$\varphi(r\alpha) = \varphi(r)\varphi(\alpha) = \varphi(r)0 = 0$ so $r\alpha \in \ker\varphi$ □

Recall Quotient Groups:
$\varphi : R \to S$ is a ring homomorphism with $\ker\varphi = I$ $R/I \cong \text{im}(vp)$ 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

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

$$\left.\begin{array}{ccc} (r_1+I)(r_2+I) & \mapsto & \varphi(r_1)\varphi(r_2) \\ \vdots\| & & \| \\ (r_1r_2)+I & \mapsto & \varphi(r_1r_2) \end{array}\right\} \times$$

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) $r \in R$, $i \in I$ $ri \in I$ (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 (1rst Ring Isomorphism Theorem)**.** If $\varphi : R \to S$ 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) $I = \{\sum_{i=0}^{n} a_i n_i \,|\, a_0 = a_1 = 0\}$.
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 $(ax+b) + I = \overline{(a+b)}$.
$\overline{x} \cdot \overline{x} = \overline{x^2} = 0$ 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 $I + J = \{a + b | a \in I, b \in J\}$

(2) The product of I and J is $IJ = \{\sum_{i=1}^{n} a_i b_i | a_i \in I, b_i \in J, n \geq 0\}$

(3) For $n \geq 1$, define the nth 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) $\{ab | a \in I, b \in J\}$ may not be closed under addition.

Example 3.4.3.

1) In $\mathbb{Z}$, let $I = 6\mathbb{Z}$ and $J = 10\mathbb{Z}$.
$I + J = \{6x + 10y | x, y \in \mathbb{Z}\}$. 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) =smallest ideal containing $A = \bigcap_{\substack{I \text{ ideal of } R \\ I \supseteq A}} I$

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 $A = \{a_1, \ldots, a_r\}$ write $(A) = (a)$ or $(A) = (a_1, \ldots, a_r)$. Another way to interpret this:

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

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 $n|m$.

3) in $\mathbb{Z}[x]$, the ideal $(2, x)$ is not principal.
$(2, x) = \{2p(x) + xq(x) | p(x), q(x) \in \mathbb{Z}[x]\}$. Note: $(2, x) \neq \mathbb{Z}[x]$
Suppose $(3, x) = \alpha(x)$, $2 \in (\alpha(x))$ 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 $\varphi : R \to S$ is homomorphsim, 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 $x_1 \leq x_2 \leq \cdots$ 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 $S = \{K | K \text{ ideal}, I \subset K \subsetneq R\}$ ordered by inclusion $\subseteq$. Construct a chain $C : J_1 \subset J_2 \subset J_3 \subset \cdots$ 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 I 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.

3.5 April 19

3.5.1 Maximal Ideals

Example 3.5.1.

1) $n\mathbb{Z}$ in $\mathbb{Z}$, $n\mathbb{Z}$ maximal $\leftrightarrow \mathbb{Z}/n\mathbb{Z}$ is a field $\leftrightarrow n$ is prime

2) $(2, x)$ in $\mathbb{Z}[x]$ maximal
$\mathbb{Z}[x] \to \mathbb{Z}[x]/(2, x) \cong \mathbb{Z}/2\mathbb{Z}$ by $p(x) \mapsto p(0) \mod 2$

3) (x) in $\mathbb{Z}[x]$ is not maximal, $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$

Definition 3.5.2. Assume R is commutative an ideal P is called prime if $ab \in P$ for $a, b \in R$, then $a \in P$ or $b \in P$.

Remark 3.5.3. In $\mathbb{Z}$, the prime ideals are $p\mathbb{Z} = (p)$ for p prime, and the zero ideal.

Proposition 3.5.4. P prime $\leftrightarrow R/P$ is an integral domain.

Proof. P is a prime ideal, $P \neq R$ and if $ab \in P$, then $a \in P$ or $b \in P$. Let $\overline{a} = a + P$, $\overline{b} = b + P$, $a \in P \to \overline{a} = 0$ in R/P. Then P is a prime ideal iff $\overline{a}\overline{b} = 0 \to \overline{a} = 0$ or $\overline{b} = 0$, ie, iff R/P is an integral domain.

Corollary 3.5.5. Every maximal ideal is prime.

Example 3.5.6.

1) Ideals (p), for p prime, in $\mathbb{Z}$ are prime (they are also maximal)
2) The zero ideal in $\mathbb{Z}$ is prime but not maximal
3) (x) in $\mathbb{Z}[x]$ is prime, $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$ (not maximal)
4) The zero ideal in $\mathbb{Z}[x]$ is prime (not maximal)

3.5.2 Euclidean Domains

Q: In which rings can we do the division algorithm?

Definition 3.5.7. Let R be an integral domain. Any function $N : R \to \mathbb{Z}^+ \cup \{0\}$ where $N(0) = 0$ is called a norm. "measures of size in R"

Definition 3.5.8. R is a euclidean domain if $\exists$ a norm on R such that for any twwo $a, b \in R$ when $b \neq 0$ $\exists q, r \in R$ with $r = 0$ or $N(r) < N(b)$.

Think: Euclidean Domains are integral domains where you can do the division algorithm.

Example 3.5.9.

0. Fields are Euclidean Domains.
   $a, b \in F$, $b \neq 0$, $a = qb$ take $q = ab^{-1}, r = 0$ (can let $N(a) = 0 \, \forall a \in F$)
1. $\mathbb{Z}$ is a euclidean domain, $N(a) = |a|$
2. if F is a field, $F[x]$ is a euclidean domain, $N(p(x)) = \deg(p(x))$
3. $\mathbb{Z}[i]$ is a euclidean domain, $N(a + bi) = a^2 + b^2$

Proposition 3.5.10. In a Euclidean Domain every ideal is principal.

Proof. If I is the zero ideal, we are done.
So suppose I is not the zero ideal, let d be any nonzero element of minimal norm in I. Becuase $d \in I$, $(d) \subset I$. WTS $(d) = I$. Let $a \in I$, by Euclidean algorith, $a = qd + r$ so $r = a - qd$. $a \in I$, $-qd \in I$, so $r \in I$. So by the minimality of d, $r = 0$. $a = qd$ so $a \in (d)$ so $I \subseteq (d)$. Thus $I = (d)$.

Example 3.5.11. in $\mathbb{Z}[x]$ we saw $(2, x)$ was not principal so $\mathbb{Z}[x]$ is not a euclidean domain.

Definition 3.5.12. R commutative, $a, b \in R$ $b \neq 0$

1) a is a multiple of b if $\exists x$ such that $ax = b$. We say $b|a$.
   In terms of ideals: $a \in (b) \leftrightarrow (a) \subseteq (b)$
2) The gcd of (a) and (b) is a nonzero element such that
   a) $d|a$, $d|b$
   b) If $d'|a$ and $d'|b$, then $d'|d$

In terms of ideals:

a) $I = (a, b) \subseteq (d)$

b) If $(d') \supseteq I$, then $(d) \subseteq (d')$

Definition 3.5.13. A principal ideal domain (PID) is an integral domain in which very ideal is principal.

Remark 3.5.14. Every ED is a PID.

Example 3.5.15.

1. Every field is a PID.
2. $\mathbb{Z}[x]$ is not a PID.

Recall: Every maximal ideal is prime. Converse is not true but in a PID ...

Proposition 3.5.16. Every nonzero prime ideal is maximal in a PID.

Proof. Let (p) be a nonzero prime ideal, let (m) be an ideal such that $(p) \subseteq (m)$. WTS either $(p) = (m)$ or $(m) = R$. Since $p \in m$, $p = rm$ so $rm \in (p)$. Since (p) is prime, $r \in (p)$ or $m \in (p)$. If $m \in (p)$, $(m) \subseteq (p)$ so $(m) = (p)$. If $r \in (p)$, then $r = ps$ for some $s \in R$. Then $p = rm = psm$ so $p(1 - sm) = 0$. Since $p \neq 0$, integral domain, $1 = sm$ so $1 \in (m)$ so $(m) = R$.

3.5.3 Unique Factorization Domains

Definition 3.5.17. Let R be an integral domain

1. r is irreducible if it is nonzero, not a unit, and when $r = ab$, either a is a unit or b is a unit. Otherwise, r is reducible.
2. $0 \neq p \in R$, the element p is called prime if (p) is a prime ideal.
3. Two elements a and b in R are called associates if $a = bu$, $u \in R^\times$

Proposition 3.5.18. In an integral domain, en element $p \neq 0$ prime $\rightarrow$ p is irreducible.

Proof. If p is prime, (p) is a prime ideal so let $p = ab \in (p)$, then $a \in (p)$ or $b \in (p)$. If $a \in (p)$, $\exists r$ such that $a = pr$ so $p = ab = prb$ so b is a unit.

3.6 April 21

3.6.1 Unique Factorization Domains

Proposition 3.6.1. In a PID a nonzero element is prime $\leftrightarrow$ it is irreducible.

Proof. By previous proposition, prime $\to$ irreducible.
Now, we show irreducible $\to$ prime. If M is an ideal containing (p), p irreducible, and since we are in a PID, $M = (m)$ is a principal ideal. Since $p \in (m)$, $p = mr$ for some r. Since p is irreducible, one of r or m must be a unit. So either $(p) = (m)$ if r is a unit or $(m) = (1) =$ the whole ring if m is a unit. This means the only idelas continaing p are (p) and (1) so (p) is maximal so (p) is prime. Hence, p is prime.

Definition 3.6.2. A unique factorization domain (UFD) is an integral domain R in which every nonzero element $r \in R$ which is not a unit satisfies:

(1) $r = p_1 \cdots p_n$ where $p_i \in R$ is irreducible.

(2) The decomposition is unique up to associates.
(ie. if $r = q_1 \cdots q_n$ with q_i irreducible, then there is a reordering such that p_i and q_i are associates)

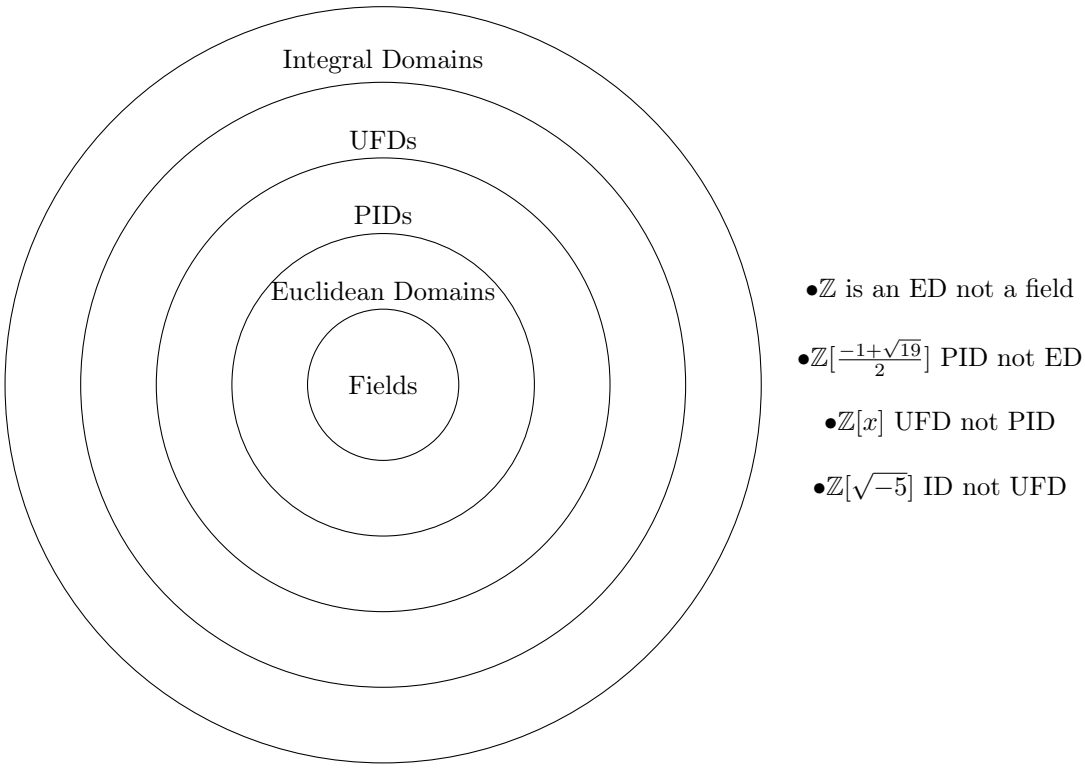
Example 3.6.3.

(1) Any field is a UFD (every nonzero element satfies 1, 2 trivially)

(2) $\mathbb{Z}$ is a UFD (Every PID is a UFD)

(3) $\mathbb{Z}[\sqrt{-5}]$ is an integral domain but not a UFD.
$6 = 2 \cdot 3 = (1 + \sqrt{-5}(1 - \sqrt{-5}))$: 2 different factorizations into irreducibles.

Proposition 3.6.4. In a UFD a nonzero element is prime iff it is irreducible.



- $\mathbb{Z}$ is an ED not a field
- $\mathbb{Z}[\frac{-1+\sqrt{19}}{2}]$ PID not ED
- $\mathbb{Z}[x]$ UFD not PID
- $\mathbb{Z}[\sqrt{-5}]$ ID not UFD

Fields $\subset$ ED $\subset$ PID $\subset$ UFD $\subset$ ID

3.6.2 Polynomial Rings

Q: What polynomial rings behave like $\mathbb{Z}$?

Theorem 3.6.5. Let F be a field. The polynomial ring $F[x]$ is a euclidean domain. Specifically, if $a(x), b(x) \in F[x]$ with $b(x) \neq 0$, then there are unique $q(x)$ and $r(x)$ in $F[x]$ such that $a(x) = q(x)b(x)+r(x)$ with $r(x) = 0$ or $\deg(r(x)) < \deg(b(x))$.

Proof. If $a(x) = 0$, then $q(x) = r(x) = 0$ so assume $a(x) \neq 0$.
We proceed by induction on $n = \deg a(x)$.
If $\deg(b(x)) > \deg(q(x))$, then $q(x) = 0$ and $r(x) = a(x)$ so assume $\deg(b(x)) < \deg(a(x))$. We can write $a(x) = \sum_{i=0}^{n} a_i x^i$, $b(x) = \sum_{i=0}^{m} b_i x^i$. Consider $a'(x) = a(x) - \frac{a_n}{b_m} x^{n-m} b(x)$. $a'(x)$ has degree less than n so by IH $\exists q'(x), r'(x)$ such that $a'(x) = q'(x)b(x) + r'(x)$ with $r(x) = 0$ or $\deg(r(x)) < \deg(b(x))$. Letting $q(x) = q'(x) + \frac{a_n}{b_m} x^{n-m}$, we have

$$\begin{aligned} b(x)q(x) + r'(x) &= b(x) * (q'(x) + \frac{a_n}{b_m} x^{n-m} + r'(x)) \\ &= b(x)q'(x) + b(x)\frac{a_n}{b_m} x^{n-m} + r'(x) \\ &= a'(x) + \frac{a_n}{b_m} x^{n-m} b(x) \\ &= a(x) \end{aligned}$$

Thus, $a(x) = b(x)q(x) + r(x)$ ($r'(x) = r(x)$ with $r(x) = 0$ or $\deg(r(x)) < \deg(b(x))$).
Uniqueness: Suppose $q_1(x), r_1(x)$ also satisfy the equation: $a(x) = q(x)b(x) + r(x) = q_1(x)b(x) + r_1(x)$. This implies $a(x) - q(x)b(x)$ and $a(x) - q_1(x)b(x)$ have degree less than $b(x)$ (they have degrees equal to $r(x)$ and $r_1(x)$). Taking the difference: $a(x) - q(x)b(x) - a(x) + q_1(x)b_1(x) = (q_1(x) - q(x))b(x)$. Degree of the product is equal to the sum of their degrees so $q_1(x) - q(x) = 0$ so $q(x) = q_1(x)$ and $r(x) = r_1(x)$.

Corollary 3.6.6. If F is a field then $F[x]$ is a PID and a UFD.

Example 3.6.7. $\mathbb{Q}[x]$ is a PID ($\mathbb{Q}$ is a field)
$(2, x)$ is not principal in $\mathbb{Z}[x]$ but 2 is a unit in $\mathbb{Q}$ so it is a unit in $\mathbb{Q}[x]$ so $\mathbb{Q}[x] = (2, x)$ so $(2, x)$ is principal in $\mathbb{Q}[x]$.

Definition 3.6.8. The polynomial ring in variables $x_1, \ldots, x_n$ with coefficients in R, denoted $R[x_1, \ldots, x_n]$ is defined inductively by $R[x_1, \ldots, x_n] = R[x_1, \ldots, x_{n-1}][x_n]$.

- A nonzero polynomial in $R[x_1, \ldots, x_n]$ is a finite sum of elements of the form $ax_1^{d_1} \cdots x_n^{d_n}$, $a \in R$, $d_i \geq 0$.
- The degree of such an element is $d = \sum_{i=1}^{n}$. The degree of a polynomial in $R[x_1, \ldots, x_n]$ is the largest among the degrees of its monomials.

Example 3.6.9. $\mathbb{Z}[x, y]$

$p(x,y) = 2x^3 + xy - y \quad \deg(p(x,y)) = 3$
$q(x,y) = 5x^4 + x^2y^3 + x \quad \deg(q(x,y)) = 5$

Example 3.6.10. $\mathbb{Q}[x]$ is a PID but $\mathbb{Q}[x,y] = \mathbb{Q}[x][y]$ is not a PID. (x,y) is not principal. This is not inconsistent with our previous thm since $Q[x]$ is not a field.

THus has been at the level of fields, but what about rings?

Theorem 3.6.11. R is a UFD $\leftrightarrow$ $R[x]$ is a UFD.

Remark 3.6.12. It follows that polynomials in any variables in a UFD is also a UFD ($R[x_1, \ldots, x_n]$)

Example 3.6.13. $\mathbb{Z}[x]$ is a UFD, $\mathbb{Z}[x,y]$ is a UFD but not a PID.

Q: how do we know which elements are irreducible?

Lemma 3.6.14 (Gauss' Lemma)**.** Let R be a UFD, let F by the smallest ring containng R in which all noznero elements are units (field of fractions of R). Let $p(x) \in R[x]$. If $p(x)$ is reducible in $F[x]$ then $p(x)$ is reducible in $R[x]$.

Corollary 3.6.15. Let R be a UFD. Suppose the gcd of the coefficients in $p(x)$ is 1. Then $p(x)$ is irreducible in $R[x]$ iff $p(x)$ is irreducible in $F[x]$.

Proof. $p(x)$ reducible in $F[x] \to p(x)$ reducible in $R[x]$ so $p(x)$ irreducible in $R[x] \to p(x)$ irreducible in $F[x]$.
So now, WTS $p(x)$ irreducible in $F[x] \to p(x)$ irreducible in $R[x]$. Since the gcd of the coefficients is 1, if $p(x)$ is reducible in $R[x]$, then $p(x) = a(x)b(x)$ where neither $a(x)$ or $b(x)$ are constant polynomials in $R[x]$. This same factorization of $p(x)$ is valid if $F[x]$, since not constant polynomials (not units). Thus, $p(x)$ is irreducible in $R[x]$ if it is irreducible in $F[x]$.

Remark 3.6.16. In particular, if $p(x)$ is monic and irreducible in $R[x]$ then $p(x)$ is irreducible in $F[x]$.

Proposition 3.6.17. Let F be a field, $p(x) \in F[x]$ has a factor of degree 1 $\iff$ $p(x)$ has a root in F.

Proof. $\to$) $p(x) = (x - \alpha)p'(x) \to p(\alpha) = 0$
$\leftarrow$) Suppose $p(\alpha) = 0$. Since $F[x]$ is an ED, apply the division algorithm to get $p(x) = q(x)(x - \alpha) + r$. Since $p(\alpha) = 0$, $r = 0$ so $p(x)$ has $(x - \alpha)$ as a factor.

Corollary 3.6.18. A polynomial of degree 2 or 3 over a field F is reducible $\iff$ it has a root in F.

Proposition 3.6.19 (Eisensteins Criterion)**.** p is a prime ideal of an integral domain R. Let $f(x) = x^n + \cdots + a_0$ bea polynomial in $R[x]$ of $deg \geq 1$. Suppose $a_{n-1}, \ldots, a_0 \in P$ and $a_0 \notin P^2$ then $f(x)$ is irreducible in $R[x]$.

Corollary 3.6.20 (Eisensteins Criterion for $\mathbb{Z}$)**.** Let p be a prime in $\mathbb{Z}$. Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ in $\mathbb{Z}[x]$. Suppose $p|a_i$ for $0 \leq i \leq n-1$ but $p^2 \not| a_0$, then $f(x)$ is irreducible in $\mathbb{Z}[x]$ so, further, $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Example 3.6.21.

(1) $x^4 + 10x + 5$, Eisensteins with $p = 5$, irreducible

(2) $x^n - p$, irreducible $\forall n$, Eisensteins with p

(3) $x^4 + 1$, $p \not| 1$ so cant apply Eisensteins directly
Consider $x \mapsto x + 1$, $x^4 + 4x^3 + 6x^2 + 4x + 2$, Eisensteins with $p = 2$, irreducible

3.7 April 26

3.7.1 Field Extensions

Q: Given any field F and a polynomial $p(x)$ in $F[x]$ does there exist a field containing F such that $p(x)$ has a root in that field.

Example 3.7.1. $F = \mathbb{R}$, $p(x) = x^2 + 1$ irreducible in $\mathbb{R}$ but contains a root in $\mathbb{C}$.

Definition 3.7.2. If K is a field containing a subfield F, then K is an extension of F , denoted K/F or $\begin{matrix} F \\ | \\ K \end{matrix}$.
The degree of K/F is the dimension of K as a vector space over F and is denoted $[K : F]$. ($\dim_F K = [K : F]$)

Think: K/F field extension, a basis of K over F is a subset $\{x_1, \ldots, x_n\} \subset K$ such that every $x \in K$ can be written as $\lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_n x_n$, $\lambda_i \in F$.

Example 3.7.3.

1) $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$
basis $= \{1, \sqrt{2}\}$, elements of the form $a + b\sqrt{2}$ for $a, b \in \mathbb{Q}$

2) $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$
basis $= \{1, \sqrt[3]{2}, \sqrt[3]{2}^2\}$, elements of the form $a + b\sqrt[3]{2} + c\sqrt[3]{2}^2$.

3) $[\mathbb{Q}(\omega) : \mathbb{Q}]$
$\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$, $\omega^3 = 1$.
$\omega \neq 1$, $\frac{\omega^3 - 1}{\omega - 1} = \omega^2 + \omega + 1$ so $\omega^2 = -\omega - 1$ so $\{1, \omega\}$ is a basis.

An important class of field extensions come from finding roots sof polynomials.

Theorem 3.7.4. let F be a field, $p \in F[x]$ irreducible polynomial. Then $\exists$ a field K containing an isomorphic copy of F in which $p(x)$ has a root. (ie. $\exists F/K$ such that $p(x)$ has a root in K)

Proof. Consider $F[x]/(p(x)) = K$. $F[x]$ is a PID, $p(x)$ is irreducible so $p(x)$ is prime. Then $(p(x))$ is a prime ideal so $(p(x))$ is maximal so $K = F[x]/(p(x))$ is a field.
Now, consider $\pi : F[x] \to F[x]/(p(x)) = K$ by $f(x) \mapsto f(x) + (p(x))$ and $\varphi = \pi|_F$, $\varphi; F \to F[x]/(p(x))$ by

$a \mapsto a + (p(x))$. $\varphi(F) \neq 0$ since φ is the identity on F so $\varphi(F) \cong F$ so K contains an isomorphic copy of F.
Now, WTS there is a root of $p(x)$ in K. We write $\overline{x}$ for image of x in K $(\pi(x))$, $p(\overline{x}) = \overline{p(x)} \equiv p(x) \mod (p(x)) = 0$, so K contains a root of $p(x)$.

Theorem 3.7.5. Let $p(x) \in F[x]$ be irreducible of degree n. Let $K = F[x]/(p(x))$. Let $\theta = x \mod (p(x)) \in K$. Then the elements $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ are a basis of K as a vector space over F.
$[K : F] = n$, $K = \{a_0 + a_1\theta + a_2\theta^2 + \cdots + a_{n-1}\theta^{n-1} \mid a_i \in F\}$

Proof. Let $a(x) \in F[x]$. $F[x]$ ED, so dividing $a(x)$ by $p(x)$, $a(x) = q(x)p(x)+r(x)$, $r(x) = 0$ or $\deg(r(x)) < \deg(p(x))$. Since $q(x)p(x) \in (p(x))$, $a(x) \equiv r(x) \mod (p(x))$ so every residue class can be represented by a polynomial of degree $< n$. So $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ spans K.
To prove independence, suppose they are linearly dependent. ie. $\exists b_0, \ldots, b_{n-1} \in F$ not all zero, such that $b_0 + b_1\theta + \cdots + b_{n-1}\theta^{n-1} \equiv 0 \mod (p(x))$ so $p(x) | b_0 + b_1\theta + \cdots b_{n-1}\theta^{n-1}$. Contradiction since $p(x)$ has degree n. Thus, $\{1, \theta, \ldots, \theta^{n-1}\}$ is a basis of K/F.

Think: Elements of $F[x]/(p(x))$ are polynomials of degree $< n$ in θ with $\theta \in K$, $p(\theta) = 0$.

Example 3.7.6.

1) $\mathbb{R}[x]/(x^2 + 1)$, polynomials of deg < 2, $a + b\theta$ where $\theta^2 + 1 = 0$, eg $\theta^2 = -1$. $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$ by $a + b\theta \mapsto a + bi$

2) $\mathbb{Q}[x]/(x^2 + 1) \cong \begin{matrix} \mathbb{Q}(i) \\ | \\ \mathbb{Q} \end{matrix}$ } deg 2. Elements $a + b\theta$, $\theta^2 + 1 = 0$, $a, b \in \mathbb{Q}$

3) $F = \mathbb{Q}$, $p(x) = x^3 - 2$ irreducible (Eisensteins)
$\mathbb{Q}[x]/(x^3 - 2) = \{a + b\theta + c\theta^2 \mid a, b, c \in \mathbb{Q}\}$, $\theta^3 = 2$

Definition 3.7.7. Let K/F be an extensions. Let $\alpha, \beta, \ldots \in K$. The smallest subfield of K containing $\alpha, \beta, \ldots$ is called the field generated by $\alpha, \beta, \ldots$ over F.

Definition 3.7.8. A field generated by a single element α over F, $F(\alpha)$, is called a simple extension.

Theorem 3.7.9. Let $p(x) \in F[x]$ be an irreducible polynomial. Let K/F bea a field extension containing α such that $p(\alpha) = 0$. Let $F(\alpha)$ denote the field generated by α. $F(\alpha) \cong F[x]/(p(x))$

Proof. Consider $\varphi; F[x] \to F(\alpha)$ by $a(x) \mapsto a(\alpha)$. $p(\alpha) = 0$ so $p(x)$ is in the kernel.
Now, we have $\pi : F[x]/(p(x)) \to F(\alpha)$. π nonzero mao since identity on F. So $F[x]/(p(x)) \cong \text{im}(\pi)$. $F(\alpha)$ smallest field containg F and α. Since $F, \alpha \in \text{im}(\pi)$, $\text{im}(\pi) = F(\alpha)$

Corollary 3.7.10. Suppose $p(x) \in F[x]$ is irreducible of def n with a root α, then

$$F(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mid a_i \in F\}$$

Example 3.7.11. $p(x) = x^3 - 2$. Roots are $\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = \sqrt[3]{2}\omega$, $\alpha_3 = \sqrt[3]{2}\omega^2$.
$\mathbb{Q}[x]/(x^3 - 2) \cong \mathbb{Q}(\alpha_2) \cong \mathbb{Q}(\alpha_2) \cong \mathbb{Q}(\alpha_3)$