MATH 113 Lecture Notes

Alec Li

Fall 2022 — Professor Lea Beneish

Contents

1 Introduction **5**
1.1 Notation . . . 5

2 Maps and Functions, Equivalence Relations **6**
2.1 Maps and Functions . . . 6
2.2 Equivalence Relations . . . 7

3 Properties of $\mathbb{Z}$ **8**
3.1 Greatest Common Divisors, Euclidean Algorithm . . . 8
3.2 Primes . . . 10

4 Congruences, Groups **11**
4.1 Congruences . . . 11
4.2 Groups . . . 12

5 Properties of Groups **14**
5.1 Properties of Groups . . . 15

6 Dihedral Groups **16**

7 Symmetric Group, Homomorphisms, Isomorphisms **18**
7.1 Symmetric Groups . . . 18
7.2 Homomorphisms and Isomorphisms . . . 21

8 Properties of Isomorphisms, Subgroups **22**
8.1 Subgroups . . . 24

9 More Subgroups **25**
9.1 Examples of Subgroups . . . 25

10 Cyclic Groups **27**

11 Cyclic Groups (cont.) **30**

12 Cyclic Groups (cont. II) **32**
12.1 Subgroups Generated by Subsets of a Group . . . 32
12.2 Quotient Groups . . . 33

13 Quotient Groups **34**
13.1 Quotient Groups . . . 34

14 Quotient Groups (cont.) **36**

15 Quotient Groups (cont. II) **38**

16 Lagrange's Theorem, Isomorphism Theorems **39**
16.1 The Isomorphism Theorems 40

17 Isomorphism Theorems **41**

18 Group Actions **42**
18.1 Group Actions 43

19 Group Actions (cont.) **45**

20 Group Actions (cont. 2) **47**
20.1 Groups acting on themselves 47

21 Conjugation Action **49**
21.1 Groups acting on themselves by conjugation 50

22 Class Equation, Sylow Theorems **51**

23 Sylow Theorems **52**

24 Sylow Theorems (cont.) **54**

25 Rings **55**

26 Direct Products, Finitely Generated Abelian Groups **57**
26.1 Fundamental Theorem of Finitely generated Abelian Groups 59

27 Subrings, Zero Divisors, Units **62**

28 Polynomial Rings—Introduction **64**

29 Ring Homomorphisms, Quotient Rings **66**
29.1 Ring Homomorphisms 66
29.2 Quotient Rings 67

30 Properties of Ideals **68**
30.1 Properties of Ideals 69

31 Properties of Ideals (cont.) **70**

32 Maximal Ideals, Prime Ideals **72**

33 Euclidean Domains, PIDS, UFDs **74**
33.1 Euclidean Domains 74
33.2 Principal Ideal Domains 75
33.3 Unique Factorization Domains 76
33.4 Polynomial Rings 78

34 Polynomial Rings **79**

35 Field Extensions **81**

Definitions

1.1 Set 5
2.2 Well-defined 6
2.3 Image 6
2.4 Pre-image 6
2.5 Injective 6

2.6 Surjective . . . 7
2.7 Bijective . . . 7
2.8 Identity map . . . 7
2.9 Composite map . . . 7
2.10 Binary Relation . . . 7
2.11 Equivalence Relation . . . 7
2.13 Equivalence Class . . . 7
3.1 Divides . . . 8
3.2 Greatest Common Divisor . . . 8
3.3 Least Common Multiple . . . 8
3.4 Division Algorithm, Quotient, Remainder . . . 8
3.5 Euclidean Algorithm . . . 9
3.10 Prime . . . 10
4.1 Congruent . . . 11
4.2 Addition and Multiplication on $\mathbb{Z}/m\mathbb{Z}$ . . . 11
4.5 Binary Operation . . . 12
4.6 Group . . . 12
5.1 Monoid . . . 14
5.2 Abelian Group . . . 14
5.5 Order of a group . . . 16
5.6 Order of an element . . . 16
6.1 Dihedral Group . . . 16
7.1 Symmetric Group . . . 19
7.3 Cycle . . . 19
7.4 Length of Cycle . . . 19
7.5 Disjoint cycles . . . 19
7.9 Homomorphism . . . 21
7.10 Isomorphism . . . 21
7.11 Endomorphism . . . 21
7.12 Automorphism . . . 21
8.5 Subgroup . . . 24
9.2 Centralizer . . . 25
9.4 Center . . . 26
9.5 Normalizer . . . 26
10.2 Cyclic Group . . . 28
12.3 Subgroup generated by a subset . . . 32
12.6 Kernel . . . 33
12.7 Image . . . 34
13.3 Quotient Group . . . 36
14.2 Left Coset . . . 37
14.3 Right Coset . . . 37
15.2 Normal Subgroup . . . 38
16.2 Index . . . 39
18.2 Group Action . . . 43
18.5 Stabilizer . . . 44
19.1 Kernel of an action . . . 45
20.1 Orbit . . . 47
20.2 Transitive Action . . . 47
21.3 Conjugate . . . 50
21.4 Conjugacy classes . . . 50
21.5 Conjugate subsets . . . 50
23.2 p-groups, p-subgroups, and Sylow p-subgroups . . . 53
25.1 Ring . . . 55
25.2 Commutative ring . . . 55

25.3 Division ring . . . 56
25.4 Field . . . 56
26.1 Direct Product . . . 57
26.7 Finitely Generated Group . . . 59
26.8 Free Abelian Group . . . 59
26.10 Torsion . . . 60
26.11 Torsion Free Group . . . 60
26.12 Torsion Group . . . 60
27.1 Zero divisor . . . 62
27.2 Unit . . . 62
27.5 Integral Domain . . . 63
27.8 Subring . . . 63
28.1 Polynomial Ring . . . 64
29.1 Ring Homomorphism . . . 66
29.2 Kernel of Ring Homomorphisms . . . 66
29.3 Ring Isomorphism . . . 66
29.8 Operations on Cosets of an Ideal . . . 67
29.9 Ideal . . . 68
30.4 Sum of Ideals . . . 69
30.5 Product of Ideals . . . 69
30.6 Power of an ideal . . . 69
31.2 Ideal generated by a set . . . 70
31.3 Principal ideal . . . 70
31.4 Finitely generated ideal . . . 70
32.1 Maximal Ideal . . . 72
32.6 Prime Ideal . . . 73
33.1 Norm . . . 74
33.2 Euclidean Domain . . . 74
33.6 Multiples, Divisors . . . 75
33.7 Principal Ideal Domain . . . 75
33.11 Reducible/Irreducible Element . . . 76
33.12 Prime Element . . . 76
33.13 Associate Elements . . . 76
33.16 Unique Factorization Domain . . . 77
33.23 Polynomial rings in multiple variables . . . 79
35.2 Extension field . . . 81
35.3 Degree of K/F . . . 82

8/24/2022

Lecture 1

Introduction

Abstract algebra is the study of algebraic structures more general than the integers or reals/complex numbers.

It's the abstract encapsulation of composition (i.e. adding numbers, composing functions, etc.).

Here's a summary of the first 6-7 years of your mathematical education:

- 1 (unity)
- $\mathbb{N}$ natural numbers, i.e. $\{(0), 1, 2, 3, \ldots\}$
- $\mathbb{Z}$ integers, i.e. $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$
- $\mathbb{Q}$ rational numbers, i.e. $\{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0\}$
- $\mathbb{R}$ real numbers
- $\mathbb{C}$ complex numbers

At each stage, the sets gained properties with respect to addition $(+)$ and multiplication $(\times)$.

The integers with addition $(\mathbb{Z}, +)$ is an example of a *group*; the integers with addition and multiplication $(\mathbb{Z}, +, \times)$ is an example of a *ring*; the rationals with addition and multiplication $(\mathbb{Q}, +, \times_0$ is an example of a *field*.

The goal of this class is to define larger classes of these objects.

1.1 Notation

Definition 1.1: Set

A set is a collection of elements.

You can have a set of numbers, symbols, shapes, people, sets, turkeys, etc.

Here are some common notations we'll be using (P and Q are statements)

- $P \implies Q$ means "P implies Q".
- $P \iff Q$ means "P if and only if Q"
- $\forall$ means "for all"
- $\exists$ means "there exists"
- $\exists!$ means "there exists unique"

Regarding sets, we have the following notation (let S and T be two sets):

- If s is an object contained in S, we say that s is a member of S, notated by $s \in S$
- If s is not in S, we write $s \notin S$
- If S has finitely many elements, we say S is a finite set, and $|S|$ denotes the number of elements in S
- $S \subset T$ if every object in S is contained in T
- If $S \subset T$ and $T \subset S$ then $S = T$
- If S is not contained in T, then $S \not\subset T$
- The set of objects contained in both S and T is $S \cap T$
- The set of objects that is either in T or in S is $S \cup T$

- If S and T are disjoint, i.e. $S \cap T = \varnothing$, then $S \sqcup T$ is the *disjoint union* of S and T.
- $S \times T$ is the *Cartesian product* of S and T; we have $S \times T = \{(a, b) \mid a \in S, b \in T\}$
- The set containing no objects is the empty set $\varnothing$

Regarding subsets, we'll use $S \subset T$ to specify containment with the possibility that $S = T$; for strict subsets, we use the notation $S \subsetneq T$.

Regarding set notation, we have the following:

$$S = \{\text{notation for elements of } S \mid \text{conditions specifying being in } S\}.$$

For example, the even integers can be specified by $\{x \in \mathbb{Z} \mid 2 \mid x\}$.

8/26/2022

Lecture 2

Maps and Functions, Equivalence Relations

2.1 Maps and Functions

The notation $f : A \to B$ or $A \xrightarrow{f} B$ denotes that f is a map (or function) from A to B. The value of f at $a \in A$ is $f(a)$.

Here, A is called the domain of f, and B is called the codomain of f.

If specifying a function on elements, we write $f : a \mapsto b$ (i.e. "f sends a to b").

Example 2.1

For example,

$$\begin{aligned} f : \mathbb{N} &\to \mathbb{N} \\ a &\mapsto a^2 \end{aligned}$$

Definition 2.2: Well-defined

We say that f is *well-defined* if $a_1 = a_2 \implies f(a_1) = f(a_2)$, for all $a_1, a_2 \in A$.

Definition 2.3: Image

The set $f(A) = \{b \in B \mid b = f(a) \text{ for some } a \in A\}$. That is, $f(A)$ is the set of all $f(a)$ for $a \in A$.

Further $f(A) \subset B$ is called the *range* or *image* of f.

Definition 2.4: Pre-image

The set $f^{-1}(C) = \{a \in A \mid f(a) \in C\}$, where $C \subset B$. $f^{-1}(C)$ is called the *pre-image* of C under f.

Definition 2.5: Injective

We say that f is *injective* if $f(x) = f(y) \implies x = y$.

Definition 2.6: Surjective

We say that f is *surjective* if given any $b \in B$, $\exists a \in A$ such that $f(a) = b$.

Definition 2.7: Bijective

We say that f is *bijective* if it is both injective and surjective.

Definition 2.8: Identity map

We say that f is the *identity map* if $A = B$ and $f(a) = a$ for all $a \in A$.

We write $f = \mathrm{id}_A$.

Definition 2.9: Composite map

If we have $f : A \to B$ and $g : B \to C$, then the *composite map* is $g \circ f : A \to C$.

In other words, $(g \circ f)(a) = g(f(a))$.

2.2 Equivalence Relations

Definition 2.10: Binary Relation

Let A be a non-empty set. A *binary relation* on a set A is a subset R of $A \times A$, and we write $a \sim b$ if $(a, b) \in R$.

Definition 2.11: Equivalence Relation

We say that $\sim$ is an *equivalence relation* if $\sim$ is:

1. *Reflexive*: $x \sim x$ for all $x \in A$
2. *Symmetric*: If $x \sim y$, then $y \sim x$ for all $x, y \in A$
3. *Transitive*: If $x \sim y$ and $y \sim z$, then $x \sim z$ for all $x, y, z \in A$

Example 2.12

Is "$x \sim y$ iff x is a cousin of y" an equivalence relation (on the set of all people)?

No; $\sim$ is not reflexive and not transitive. You are not your own cousin, and your cousin's cousin is not still your cousin.

Definition 2.13: Equivalence Class

If $\sim$ defines an equivalence relation on A, then the *equivalence class* of $a \in A$ is

$$[a] = \{x \in A \mid x \sim a\}.$$

Example 2.14

On $\mathbb{Z} \times \mathbb{Z}$, "$x \sim y$ iff $2 \mid (x-y)$" (i.e. $x-y$ is divisible by 2) is an equivalence relation:

1. Reflexive: $x \sim x$, since $x - x = 0$ and $2 \mid 0$
2. Symmetric: If $x \sim y$, then $2 \mid (x-y)$; we also know that $2 \mid (y-x)$, since $y - x = -(x-y)$.
3. Transitive: If $x \sim y$ and $y \sim z$, then $2 \mid (x-y)$ and $2 \mid (y-z)$. Here, we have $y - z = (x-y) + (y-z)$, and 2 divides both terms.

What are the equivalence classes?

If x is even, then $x = 2n$ for some $n \in \mathbb{Z}$; here, $2 \mid (2n - y)$ if and only if y is even as well. This means that $[x]$ for even x is the set of all even numbers.

Similarly, if x is odd, then $x = 2n+1$ for some $n \in \mathbb{Z}$; here, $2 \mid (2n+1-y)$ if and only if y is odd as well. This means that $[x]$ for odd x is the set of all odd numbers.

Note that the symmetric and transitive properties imply that $y \in [x]$ iff $[y] = [x]$. The reflexive property implies that $x \in [x]$. This means that equivalence classes are non-empty, and their union is A. That is, A is a disjoint union of equivalence classes.

8/29/2022

Lecture 3

Properties of $\mathbb{Z}$

3.1 Greatest Common Divisors, Euclidean Algorithm

Definition 3.1: Divides

If $a, b \in \mathbb{Z}$ and $a \neq 0$, we say *a divides b* if there is an element $c \in \mathbb{Z}$ such that $b = ac$. We notate this by $a \mid b$ (i.e. b is divisible by a).

Definition 3.2: Greatest Common Divisor

If $a, b \in \mathbb{Z} \setminus \{0\}$, there is a unique positive integer d called the *greatest common divisor* of a and b, denoted by $\gcd(a,b)$. In particular, $d \mid a$ and $d \mid b$, and d is the greatest such integer, so if $e \mid a$ and $e \mid b$, then $e \mid d$.

Definition 3.3: Least Common Multiple

If $a, b \in \mathbb{Z} \setminus \{a\}$, there is a unique positive integer ℓ called the *least common multiple* of a and b, denoted by $\operatorname{lcm}(a,b)$. In particular, $a \mid \ell$ and $b \mid \ell$, and ℓ is the least such integer, so if $a \mid m$ and $b \mid m$, then $\ell \mid m$.

Definition 3.4: Division Algorithm, Quotient, Remainder

If $a, b \in \mathbb{Z}$ and $b \neq 0$, then $\exists! q, r \in \mathbb{Z}$ with $0 \leq r < |b|$ such that $a = qb + r$.

Here, q is the *quotient*, and r is the *remainder*.

Definition 3.5: Euclidean Algorithm

The *Euclidean algorithm* provides the GCD of two integers by iterating the division algorithm.

The procedure is as follows:

$$\begin{aligned} a &= q_0 b + r_0 \\ b &= q_1 r_0 + r_1 \\ r_0 &= q_2 r_1 + r_0 \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n \\ r_{n-1} &= q_{n+1} r_n \end{aligned}$$

Here, r_n is the last nonzero remainder, and we have $r_n = \gcd(a, b)$.

Here, notice that $|b| > |r_0| > \cdots > |r_n|$ by the way we defined the division algorithm. This means that this is a strictly decreasing sequence of positive integers, so there will always be a last nonzero remainder, and r_n exists.

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

Lemma 3.6

We claim that $\gcd(a, b) = \gcd(b, r_0)$, where $a = q_0 b + r_0$.

Proof. We have $r_0 = a - q_0 b$ by rearranging the given equation. If $d \mid a$ and $d \mid b$, then $d \mid (a - q_0 b)$, which means that $d \mid r_0$.

On the other hand, we have $r_0 + q_0 b = a$, so if $d \mid r_0$ and $d \mid b$, then $d \mid (r_0 + q_0 b)$.

This means that the set of common divisors of a and b is the same as the set of common divisors of b and r_0; this in turn means that the greatest common divisor is identical. □

Example 3.7

Find $\gcd(35, 20)$.

We have

$$\begin{aligned} 35 &= 1 \cdot 20 + 15 \\ 20 &= 1 \cdot 15 + 5 \\ 15 &= 3 \cdot 5 + 0 \end{aligned}$$

The last nonzero remainder is $5 = \gcd(35, 20)$.

Theorem 3.8: Bezout's Identity

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

Example 3.9

For our previous case of 35 and 20, we have

$$\begin{aligned} 5 &= 20 - 1 \cdot 15 \\ &= 20 - 1 \cdot (35 - 1 \cdot 20) \\ &= 2 \cdot 20 - 1 \cdot 35 \end{aligned}$$

In this case, we have $u = 2,\ v = -1$.

3.2 Primes

Definition 3.10: Prime

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

Lemma 3.11: Euclid's Lemma

Suppose $a, b \in \mathbb{Z}$ and p is a prime. If $p \mid ab$, then $p \mid a$ or $p \mid b$ (or both).

Proof. Suppose $p \mid ab$.

If $p \nmid a$, then a and p are coprime, i.e. $\gcd(a, p) = 1$. This means there exists $u, v \in \mathbb{Z}$ such that $au + pv = 1$. However, multiplying everything by b gives $abu + bpv = b$.

Since $p \mid ab$, we have $p \mid (abu + bpv)$, and therefore $p \mid b$.

The same logic applies if $p \nmid b$, resulting in $p \mid a$. This means that it must be the case that p divides at least one of a and b. □

Note that primality is important here. Consider the number 15; $15 \mid (3 \cdot 5)$ but $15 \nmid 3$ and $15 \nmid 5$.

Theorem 3.12: Fundamental Theorem of Arithmetic

If $n \in \mathbb{Z}$ and $n > 1$, then n can be factored uniquely into a product of primes

$$n = p_1^{d_1} p_2^{d_2} \cdots p_m^{d_m},$$

such that this factorization is unique up to ordering.

Theorem 3.13

There are infinitely many primes.

Proof. Suppose there are only finitely many primes $p_1 \dots p_r$. Then, we can compute $p_1 \cdots p_r + 1$.

If this number is prime, then we are done, and we have found a new prime.

If this number is not prime, we know that $p_1, \dots, p_n$ do not divide this number. However, the fundamental theorem of arithmetic states that we must be able to decompose it into the product of primes. As such, there must be some new prime we did not list.

In either case, there is always a new prime, so our assumption that there are only finitely many primes is false; there are in fact infinitely many primes. □

8/31/2022

Lecture 4

Congruences, Groups

4.1 Congruences

Suppose we fix a $m \in \mathbb{N}$. By the division algorithm, if $a \in \mathbb{Z}$, there exists unique q, r such that $a = mq + r$ for $0 \leq r < m$.

Definition 4.1: Congruent

a and b are *congruent* mod m or *congruent modulo* m if $m \mid a - b$.

This is an equivalence relation on the integers: "$a \sim b$ iff $m \mid (a-b)$" or equivalently "$a \sim b$ iff a and b have the same reminder when you divide by m".

The equivalence classes of $\mathbb{Z}$ under this relation are indexed by the possible remainders mod m. We call these *residue classes*.

For notation, we define

$$\mathbb{Z}/m\mathbb{Z} = \{[0], [1], \ldots, [m-1]\} = \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}.$$

Here, we have

$$\bar{a} = \{a, a+m, a+2m, \ldots\}.$$

This gives us a natural map

$$\begin{aligned}[\cdot] : \mathbb{Z} &\to \mathbb{Z}/m\mathbb{Z} \\ a &\mapsto [a]\end{aligned}$$

How do we work with these objects?

Definition 4.2: Addition and Multiplication on $\mathbb{Z}/m\mathbb{Z}$

We define addition and multiplication on $\mathbb{Z}/m\mathbb{Z}$ by

$$\begin{aligned}[a] \times [b] &= [a \times b] \\ [a] + [b] &= [a + b]\end{aligned}$$

Lemma 4.3

These operations (addition and multiplication) do not depend on the choice of representative. That is, it doesn't matter if we use $\overline{m}$ instead of $\bar{0}$; these operations still hold, and give the same results.

Proof. To see why this is the case, suppose $a_1 \equiv b_1 \pmod{m}$, which means $m \mid (a_1 - b_1)$, and $a_1 = b_1 + sm$ for some $s \in \mathbb{Z}$.

Suppose the same is true for a_2 and b_2, i.e. $a_2 \equiv b_2 \pmod{m}$, meaning $a_2 = b_2 + tm$ for some $t \in \mathbb{Z}$. Adding $a_1 + a_2$, we have

$$\begin{aligned}a_1 + a_2 &= b_1 + sm + b_2 + tm \\ &= b_1 + b_2 + (s+t)m \\ a_1 + a_2 &\equiv b_1 + b_2 \pmod{m}\end{aligned}$$

Multiplying $a_1 a_2$, we have

$$a_1 a_2 = (b_1 + sm)(b_2 + tm)$$

$$\begin{aligned} &= b_1 b_2 + b_1 tm + b_2 sm + stm^2 \\ &= b_1 b_2 + (b_1 t + b_2 s + stm)m \\ a_1 a_2 &\equiv b_1 b_2 \pmod{m} \end{aligned}$$

□

Here are some properties of $\mathbb{Z}/m\mathbb{Z}$:

- $[0] \in \mathbb{Z}/\mathbb{Z}$ behaves like $0 \in \mathbb{Z}$, as
$$[0] + [a] = [a].$$
- $[1] \in \mathbb{Z}/m\mathbb{Z}$ behaves like $1 \in \mathbb{Z}$, as
$$[1] \times [a] = [a].$$
However, $\underbrace{[1] + \cdots + [1]}_{m} = [0]$, which does not happen in $\mathbb{Z}$.
- If $rs \in [m]$, then we have $[r][s] = [rs] = [m] = [0]$; in other words, we can get $[0]$ more often in $\mathbb{Z}/m\mathbb{Z}$.

Lemma 4.4

For every $m \in \mathbb{N}$, $a \in \mathbb{Z}$, the congruence $ax \equiv 1 \pmod{m}$ has a solution in $\mathbb{Z}$ if and only if $\gcd(a, m) = 1$.

Proof. If $\gcd(a, m) = 1$, there exists integers $u, v \in \mathbb{Z}$ such that

$$au + vm = 1 \implies au \equiv 1 \pmod{m}.$$

□

4.2 Groups

Definition 4.5: Binary Operation

Let G be a set. A *binary operation* is a map of sets

$$* : G \times G \to G.$$

For $a, b \in G$, we write $a * b$ for $*(a, b)$.

Definition 4.6: Group

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

1. Associativity: $(a * b) * c = a * (b * c$
2. Identity: there exists some $e \in G$ such that $a * e = e * a = a$, for all $a \in G$
3. Inverses: Given $a \in G$, there exists some $b \in G$ such that $a * b = b * a = e$ (where e is the identity)

We will write a group as $(G, *)$, but sometimes the operation is implicit and we will just write G.

Example 4.7

Is $(\mathbb{Z}, +)$ a group?

1. Associativity: $a + b = b + a$ for all $a, b \in \mathbb{Z}$
2. The identity is 0
3. The inverse for $a \in \mathbb{Z}$ is $-a \in \mathbb{Z}$.

Thus, yes, $(\mathbb{Z}, +)$ is a group.

Example 4.8

Is $(\mathbb{Q}, +)$ a group?

1. Associativity: $a + b = b + a$ for all $a, b \in \mathbb{Q}$
2. The identity is 0
3. The inverse for $a \in \mathbb{Q}$ is $-a \in \mathbb{Q}$

Thus, yes, $(\mathbb{Q}, +)$ is a group.

Example 4.9

Is $(\mathbb{Z}/m\mathbb{Z}, +)$ a group?

1. Associativity: $[a] + [b] = [b] + [a]$ since associativity carries over from $\mathbb{Z}$
2. The identity is $[0]$
3. The inverse for $[a] \in \mathbb{Z}/m\mathbb{Z}$ is $[-a] \in \mathbb{Z}/m\mathbb{Z}$

Thus, yes, $(\mathbb{Z}/m\mathbb{Z}, +)$ is a group.

Example 4.10

Is $(\mathbb{Q} \setminus \{0\}, \times)$ a group?

1. Associativity: $ab = ba$ for all $a, b \in \mathbb{Q}$
2. The identity is 1
3. The inverse for $a \in \mathbb{Q}$ is $\frac{1}{a} \in \mathbb{Q}$; we have no issues here because 0 is excluded.

Thus, yes, $(\mathbb{Q} \setminus \{0\}, \times)$ is a group.

Example 4.11

Is $(\mathbb{Z} \setminus \{0\}, \times)$ a group?

No; there are no inverses. For example, 2 needs $\frac{1}{2} \notin \mathbb{Z} \setminus \{0\}$.

Example 4.12

Is $(\mathbb{Z}/m\mathbb{Z}, \times)$ a group?

1. Associativity: $[a][b] = [b][a]$ since associativity carries over from $\mathbb{Z}$

2. The identity is 1
3. The inverse for $[a] \in \mathbb{Z}/m\mathbb{Z}$ only exists if m is prime.

   This is because $ax \equiv 1 \pmod{m}$ exists only when $\gcd(a,x) = 1$.

This means that $(\mathbb{Z}/m\mathbb{Z}, \times)$ is a group only when m is prime.

Example 4.13

Is $\{e\}$ a group, where e is the identity element?

1. Associativity: $e * e = e$
2. The identity is e
3. The inverse for e is e

Thus, yes, $\{e\}$ is a group.

Example 4.14

Is $\varnothing$ a group?

No; there is no identity element.

9/2/2022

Lecture 5

Properties of Groups

If $(A, *)$ and $(B, \diamond)$ are groups, then $(A \times B, (*, \diamond))$ forms a group. Here, we denote

$$(*, \diamond) : A \times B \to A \times B \text{ such that } (a_1, b_1)(+, \diamond)(a_2, b_2) = (a_1 * a_2, b_1 \diamond b_2).$$

Definition 5.1: Monoid

A set with a binary operation is a *monoid* if associativity and identity hold (i.e. no need for inverses).

Note that groups are monoids, but monoids are not groups. In particular, $(\mathbb{Z}, +)$ is a group and thus also a monoid; $(\mathbb{Z}, \times)$ is not a group, as it does not have inverses, but it is a monoid, as it has associativity and identity.

Definition 5.2: Abelian Group

A group $(G, *)$ is called *Abelian* if it also satisfies $a * b = b * a$ for all $a, b \in G$, i.e. commutativity.

Example 5.3

An example of an Abelian group is $(\mathbb{Z}, +)$.

A non-example is the group $\mathrm{Gl}_n(\mathbb{R}) = \{\mathbf{M} \in M_n(\mathbb{R}) \mid \det(\mathbf{M}) \neq 0\}$ for $n \geq 2$, i.e. the set of $n \times n$ matrices with a nonzero determinant.

A square matrix has an inverse if and only if its determinant is nonzero, so all of these matrices have inverses. The group has the identity $\mathbf{I}_n$, and it is associative. However, matrices are not commutative, so it is a

non-Abelian group.

5.1 Properties of Groups

If G is a group under $*$, then

1. The identity of G is unique.

   Proof. Suppose we have two different identities e_1 and e_2. We then have

   $$e_1 * e_2 = e_2$$
   $$e_1 * e_2 = e_1$$

   Here, the first equation we use e_1 as the identity, and in the second equation we use e_2 as the identity. Since the LHS are equal, we have $e_1 = e_2$. This means that the identities are not actually different, and there is indeed only one unique identity. □

2. For each $a \in G$, a^{-1} is unique.

   Proof. Assume b and c are both inverses of a. Let e be the identity of G.

   By the inverse axiom, we have $a * b = e$ and $c * a = e$. We then have

   $$\begin{aligned} c &= c * e && \text{(identity)} \\ &= c * (a * b) && (e = a * b) \\ &= (c * a) * b && \text{(associativity)} \\ &= e * b && (e = c * a) \\ &= b && \text{(identity)} \end{aligned}$$

   As such, the inverses are not actually different, and there is indeed only one unique inverse a^{-1}. □

3. $(a^{-1})^{-1} = a$ for all $a \in G$.

   Proof. To show that $(a^{-1})^{-1} = a$, we need to show that a is the inverse of a^{-1}.

   Since a^{-1} is the inverse of a, then $a * a^{-1} = a^{-1} * a = e$. Switching the roles of a and a^{-1}, this also means that a is the inverse of a^{-1}. □

4. $(a * b)^{-1} = b^{-1} * a^{-1}$ for all $a, b \in G$.

   Proof. Let $c = (a * b)^{-1}$; this means that $(a * b) * c = e$. We then have

   $$\begin{aligned} (a * b) * c &= e \\ a * (b * c) &= e \\ a^{-1} * a * (b * c) &= a^{-1} * e \\ (a^{-1} * a) * (b * c) &= a^{-1} \\ b * c &= a^{-1} \\ b^{-1} * b * c &= b^{-1} * a^{-1} \\ c &= b^{-1} * a^{-1} \end{aligned}$$

   □

Lemma 5.4

Let G be a group, and let $a, b \in G$. The equations $a * x = b$ and $y * a = b$ have unique solutions for $x, y \in G$. In particular:

- If $a * u = a * v$, then $u = v$ (left-$*$ by a^{-1})
- If $u * b = v * b$, then $u = v$ (right-$*$ by b^{-1})

Definition 5.5: Order of a group

For a group G, the *order of a group* G is the number of elements in G, denoted $|G|$.

Definition 5.6: Order of an element

Let G be a group, with an element $x \in G$. The *order of an element* $x \in G$ is the smallest positive integer n such that $x^n = e$, denoted as $|x|$. That is, $\underbrace{x * x * \cdots * x}_{n} = e$.

If no positive power of x is the identity, then $|x| = \infty$.

Example 5.7

Consider the elements of $(\mathbb{Z}, +)$. The identity is $e = 0$.

We have $|0| = 1$, since we only need to add 0 once to get the identity.

We have $|1| = \infty$, since adding 1 will never get back to 0. The same reasoning holds for any non-zero element.

Example 5.8

Consider the elements of $(\mathbb{Z}/9\mathbb{Z}, +)$.

We have $|[6]| = 3$, since $[6] + [6] = [12] = [3] \neq [0]$, and $[6] + [6] + [6] = [18] = [0]$.

9/7/2022

Lecture 6

Dihedral Groups

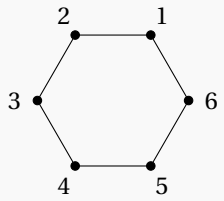
Definition 6.1: Dihedral Group

The elements of dihedral groups are symmetries of geometric objects.

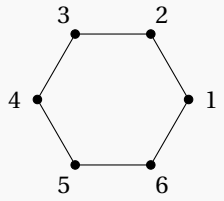
Consider a regular n-gon for $n \geq 3$.

Example 6.2

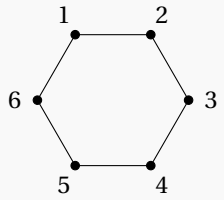
Consider a regular hexagon; what are the symmetries of this hexagon?



We can rotate by $\frac{2\pi}{6}$: (denoted by r)



Or, we can reflect vertically: (denoted by s)

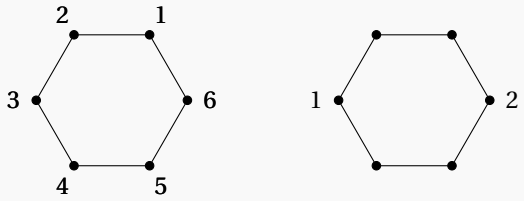


Observe that the symmetry of a hexagon gives a map

$$\{1,2,\ldots,6\} \to \{1,2,\ldots,6\}.$$

For example, $r(1) = 2$ and $s(3) = 5$; in other words, if σ is a symmetry, $\sigma(i) = j$ means that σ sends i to where j used to be.

This function determines the symmetry, but not every function gives you a symmetry. For example, there is no symmetry such that $\sigma(1) = 3$ and $\sigma(2) = 6$ simultaneously:



Let D_{2n} be the set of symmetries of the n-gon. We define $t_1 t_2$ to be the symmetry where we apply t_2 then apply t_1, for $t_1, t_2 \in D_{2n}$ (i.e. composition of functions).

To verify whether this is a group,

- This binary operation is associative, since composition of functions is associative
- The identity is to do nothing, i.e. the symmetry $\sigma(i) = i$ for all $i \in \{1,\ldots,n\}$
- The inverse of any symmetry is to undo the symmetry, i.e. if $\sigma(i) = j$, then $\sigma^{-1}(j) = i$.

D_{2n} is called the dihedral group of order $2n$. Some places write D_n, where n is the number of vertices, but the group has $2n$ elements, which is why we write D_{2n}.

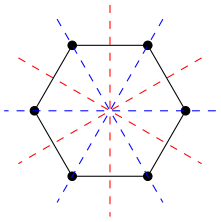
How do we know that there are $2n$ elements in D_{2n}? For any vertex i, we have n choices for where to send it in the

symmetry. However, vertex $i+1$ must be next to vertex i; we only have two choices for where this vertex goes (i.e. either before or after i). These two vertices will uniquely define the map, as the rest of the vertices must follow.

This means that there are $2n$ possible symmetries in D_{2n}, i.e. there are $2n$ elements of D_{2n}.

Explicitly, what are these symmetries?

There are n rotations about the center of the shape, i.e. rotations of $\frac{2\pi}{n}$ clockwise. There are n reflections through n lines of symmetry; if n is odd, these lines are through a vertex and a midpoint of the opposite side, and if n is even, $\frac{n}{2}$ symmetries are through opposite vertices and $\frac{n}{2}$ symmetries are through opposite sides.



To fix the notation, we will let r be the rotation clockwise around the origin by $\frac{2\pi}{n}$ radians, and we will let s be the reflection across the line through 1 and the origin.

Here are some observations:

- The rotations (for D_{12}) are: $1, r, r^2, r^3, r^4, r^5, r^6 = 1$, each rotating by $0, \frac{2\pi}{6}, \frac{4\pi}{6}, \frac{6\pi}{6} = \pi, \frac{8\pi}{6}, \frac{10\pi}{6}, 2\pi = 1$.

  Here, we've just found that $|r| = 6$. In general, $|r| = n$.

- The reflections are: $1, s, s^2 = 1$, since reflecting twice gets back the original.

  Here, we've just found that $|s| = 2$.

- $s \neq r^i$ for any i.

  This is because r preserves the orientation; i will always follow $i+1$. However, s does not preserve orientation; it flips the orientation.

- $sr^i \neq sr^j$ for any $0 \leq i \neq j < n$.

- $r^i \neq sr^j$ for any i, j.

Example 6.3

The elements of D_{12} are:

$$\{1, r, r^2, r^3, r^4, r^5, s, sr, sr^2, sr^3, sr^4, sr^5\}.$$

These elements are all distinct, and there are $2 \cdot 6 = 12$ of them.

In general, we have that

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

9/9/2022

Lecture 7

Symmetric Group, Homomorphisms, Isomorphisms

7.1 Symmetric Groups

Another example of groups we'll be working with are symmetric groups.

Definition 7.1: Symmetric Group

Let Ω be a nonempty set, and let S_Ω be the set of all bijections from Ω to itself (i.e. permutations of Ω).

Let $\sigma : \Omega \to \Omega, \tau : \Omega \to \Omega$ be permutations of Ω; $\sigma \circ \tau : \Omega \to \Omega$ is also a bijection.

We know that

- Function composition is associative, so the operation is associative.
- The identity of S_Ω is the permutation 1 such that $1(a) = a$ for all $a \in \Omega$.
- Every permutation also has an inverse $\sigma^{-1} : \Omega \to \Omega$ such that $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = 1$.

Together, this means that $(S_\Omega, \circ)$ is a group; we call it the *symmetric group* on the set Ω.

Usually, we'll take $\Omega = \{1, \dots, n\}$ and write S_n instead of S_Ω.

Example 7.2

Let $\Omega = \{1, 2, 3\}$.

Let σ be in S_3, such that we have $\sigma(1) = 2$, $\sigma(2) = 3$, and $\sigma(3) = 1$. We represent σ by the notation (123). That is, 1 goes to 2, 2 goes to 3, and 3 goes to 1. An alternative notation is

$$\begin{aligned} \sigma : 1 &\mapsto 2 \\ 2 &\mapsto 3 \\ 3 &\mapsto 1 \end{aligned}$$

This second notation is long for sets of many elements, so we prefer the first.

Let τ be in S_3, such that we have $\tau(1) = 2$, $\tau(2) = 1$, and $\tau(3) = 3$. We can represent τ by (12)(3); we can also write (12), omitting 3 because it goes to itself.

Definition 7.3: Cycle

A *cycle* is a string of integers representing an element of S_n which cyclically permutes the integers.

Definition 7.4: Length of Cycle

The *length of a cycle* is the number of integers that appear in it.

Definition 7.5: Disjoint cycles

Two cycles are called *disjoint* if they have no numbers in common.

Example 7.6

Here are all of the elements of S_3:

			notation
$\sigma_1(1)=1$	$\sigma_1(2)=2$	$\sigma_1(3)=3$	$1, e, (1)(2)(3)$
$\sigma_2(1)=1$	$\sigma_2(2)=3$	$\sigma_2(3)=2$	(23)
$\sigma_3(1)=3$	$\sigma_3(2)=2$	$\sigma_3(3)=1$	(13)
$\sigma_4(1)=2$	$\sigma_4(2)=1$	$\sigma_4(3)=3$	(12)
$\sigma_5(1)=2$	$\sigma_5(2)=3$	$\sigma_5(3)=1$	(123)
$\sigma_6(1)=3$	$\sigma_6(2)=1$	$\sigma_6(3)=2$	(132)

.

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

Example 7.7

For S_{13}, if we have

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

the inverse is

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

Note that $(2\ 13) = (13\ 2)$, since these cycles permute integers cyclically.

However, by convention, we write the smallest number first.

Composing $\sigma \circ \tau$ in S_n means that we read from right to left.

Example 7.8

For example, suppose we have $(123) \circ (12)(34)$, i.e. $\sigma = (123)$ and $\tau = (12)(34)$.

We have

$$\begin{aligned}
&\tau : 1 \mapsto 2,\ \sigma : 2 \mapsto 3 \\
&\quad \implies \sigma \circ \tau : 1 \mapsto 3 \\
&\tau : 3 \mapsto 4,\ \sigma : 4 \mapsto 4 \\
&\quad \implies \sigma \circ \tau : 3 \mapsto 4 \\
&\tau : 4 \mapsto 3,\ \sigma : 3 \mapsto 1 \\
&\quad \implies \sigma \circ \tau : 4 \mapsto 1 \\
&\tau : 2 \mapsto 1,\ \sigma : 1 \mapsto 2 \\
&\quad \implies \sigma \circ \tau : 2 \mapsto 2
\end{aligned}$$

This means we have $\sigma \circ \tau = (134)(2) = (134)$

Here are some notes:

- S_n is a non-abelian group for all $n \geq 3$. For example, we have $(12) \circ (13) = (132)$ and $(13) \circ (12) = (123)$.
- Disjoint cycles commute.
- The *order* of a permutation is the LCM of the lengths of the cycles in its cycle decomposition.
- The order of S_n is $n!$.

- A *transposition* is a cycle of length 2.

7.2 Homomorphisms and Isomorphisms

We have a notion of maps between sets, but we want to have a notion of "maps" between groups.

Definition 7.9: Homomorphism

Let $(G,*)$ and $(H,\diamond)$ be groups. A map $\phi : G \to H$ such that

$$\phi(x * y) = \phi(x) \diamond \phi(y)$$

is called a *homomorphism*.

In other words, a homomorphism is a map of sets that respects the group structure.

Note that when group operations are not specified, then we usually write $\phi(xy) = \phi(x)\phi(y)$, where the LHS uses the "product" in G, and the RHS uses the "product" in H.

Definition 7.10: Isomorphism

The map $\phi : G \to H$ is an *isomorphism* and G and H are said to be *isomorphic*, written $G \cong H$ if

1. ϕ is a homomorphism $\phi(xy) = \phi(x)\phi(y)$
2. ϕ is a bijection

Definition 7.11: Endomorphism

A homomorphism from a group to itself is called an *endomorphism*.

Definition 7.12: Automorphism

An endomorphism that is also an isomorphism is called an *automorphism*.

Example 7.13

Let us consider the map

$$\begin{aligned} \phi : (\mathbb{Z},+) &\to (\mathbb{Q},+) \\ x &\mapsto x \end{aligned}$$

Notice $\mathbb{Z} \subseteq \mathbb{Q}$; this is called the inclusion map.

We have $\phi(x+y) = x+y$, and $\phi(x)+\phi(y) = x+y$, so this is a homomorphism.

This is not an isomorphism, since it is not a bijection—it is injective, but not surjective.

Example 7.14

Consider the map

$$\begin{aligned} \phi : (\mathbb{Z},+) &\to (\mathbb{Z}/m\mathbb{Z},+) \\ x &\mapsto [x] \end{aligned}$$

We have $\phi(x+y) = [x+y] = [x] + [y] = \phi(x) + \phi(y)$, so this is a homomorphism.

This is not an isomorphism, since it is not a bijection—it is surjective, but not injective.

Example 7.15

For any group G, the identity map

$$\begin{aligned} \phi : G &\to G \\ x &\mapsto x \end{aligned}$$

is an isomorphism; it's injective and surjective, and it's also a homomorphism ($\phi(x+y) = x+y = \phi(x) + \phi(y)$

We can also say that this is an automorphism.

Example 7.16

For any group G and any group H, consider

$$\begin{aligned} \phi : G &\to H \\ g &\mapsto e_H \end{aligned}$$

Here, e_H is the identity element in H. This is called the trivial homomorphism.

This is definitely not an isomorphism, since it is neither injective nor surjective.

This is a homomorphism, since $\phi(g_1 g_2) = e_H = e_H * e_H = \phi(g_1)\phi(g_2)$.

Lemma 7.17

Let $(G, *)$, $(H, \circ)$, $(M, \diamond)$ 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. We have

$$\begin{aligned} g(f(x*y)) &= g(f(x) \circ f(y)) && (f \text{ homomorphism}) \\ &= g(f(x)) \diamond g(f(y)) && (g \text{ homomorphism}) \end{aligned}$$

This means that $g \circ f$ is indeed a homomorphism. □

9/12/2022

Lecture 8

Properties of Isomorphisms, Subgroups

Here are some properties of isomorphisms.

If $\phi : G \to H$ is an isomorphism, then:

1. $|G| = |H|$
2. G is abelian if and only if H is abelian
3. For all $x \in G$, $|x| = \left|\phi(x)\right|$

To prove the above properties, we have:

1. *Proof.* Since ϕ is an isomorphism, it must be bijective, meaning $|G| = |H|$. □

2. *Proof.* Suppose G is abelian; we have

$$\phi(xy) = \phi(x)\phi(y)$$
$$\phi(yx) = \phi(y)\phi(x)$$

Since the LHS are equal because G is abelian, the RHS must be equal, meaning $\phi(x)\phi(y) = \phi(y)\phi(x)$ for any $x, y \in G$. Since ϕ is a bijection and x, y are arbitrary, this means that we have $ab = ba$ for any $a, b \in H$; there will always exist some x, y such that $a = \phi(x)$ and $b = \phi(y)$.

Suppose H is abelian; we have

$$\phi(xy) = \phi(x)\phi(y) = \phi(y)\phi(x) = \phi(yx).$$

Here, the middle equality is due to the fact that H is abelian, and thus $\phi(x), \phi(y) \in H$ commute. Further, since ϕ is an isomorphism, it is bijective, and we must then have $xy = yx$ for any arbitrary $x, y \in G$, meaning G is abelian as well. □

3. First, a few lemmas:

Lemma 8.1

Let $\phi : G \to H$ be a homomorphism; then, $\phi(x^n) = \phi(x)^n$ for all $n \in \mathbb{Z}$.

Lemma 8.2

If $\phi : G \to H$ is a homomorphism, then $\phi(e_G) = e_H$.

Proof. We know that $e_G = e_G * e_G$; applying ϕ, we have

$$\phi(e_G) = \phi(e_G * e_G) = \phi(e_G) * \phi(e_G).$$

Since $\phi(e_G) \in H$, we can take the inverse to give

$$\phi(e_G)^{-1} * \phi(e_G) = \phi(e_G)^{-1} * \phi(e_G) * \phi(e_G)$$
$$e_H = e_H * \phi(e_G) = \phi(e_G)$$

□

Proof. Firstly, suppose for contradiction that $|\phi(x)| = \infty$ and suppose $|x| = n < \infty$. Then, $\phi(x)^n = \phi(x^n) = \phi(e_G) = e_H$. However, this means that $|\phi(x)| < \infty$, which is a contradiction.

Next, suppose for contradiction that $|\phi(x)| = n < \infty$ and suppose $|x| = \infty$. Then, $\phi(x^n) = \phi(x)^n = e_H = \phi(e_G)$. Since ϕ is an isomorphism, it is a bijection and as such $x^n = e_G$. However, this means that $|x| < \infty$, which is a contradiction.

This means that both $|\phi(x)|$ and $|x|$ must be infinite, or both $|\phi(x)|$ and $|x|$ are finite. We now only need to prove that in the finite case, both orders are equal.

Suppose $|x| = n$ and $|\phi(x)| = m$. We then have $\phi(x)^n = \phi(x^n) = \phi(e_G) = e_H$. This means that $m \leq n$, since we can't have any larger power than n that gives the identity; we could have a smaller power though.

Similarly, we have $\phi(e_G) = e_H = \phi(x)^m = \phi(x^m)$. Because ϕ is an isomorphism, it is bijective, and $x^m = e_G$. This implies that $n \leq m$, since we can't have any larger power than m that gives the identity.

Together, since $m \leq n$ and $n \leq m$, we must have $n = m$. □

Example 8.3

Consider S_3 and $\mathbb{Z}/6\mathbb{Z}$. Are these groups isomorphic (that is, does there exist an isomorphism between S_3 and $\mathbb{Z}/6\mathbb{Z}$)?

No; S_3 is not abelian, but $\mathbb{Z}/6\mathbb{Z}$ is abelian. This violates the property that isomorphic groups must both be abelian or both not be abelian.

Example 8.4

Consider $D_6 \cong S_3$.

Recall that

$$D_6 = \{r, s \mid r^3 = s^2 = 1, rs = sr^{-1}\}.$$

If we have $a : (123) \mapsto r$ and $b : (12) \mapsto s$, then a, b generate S_3, and satisfy the D_6 relations.

8.1 Subgroups

Definition 8.5: Subgroup

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

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

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

Think of subgroups as a subset that is also a group under the same operation as G.

Example 8.6

1. $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Q}, +)$.

   We have $0 \in \mathbb{Z}$, we have that $\mathbb{Z}$ is closed under addition, and the inverse $x^{-1} = -x$.
2. $(\mathbb{Q}, +)$ is a subgroup of $(\mathbb{R}, +)$
3. $(\mathbb{Q} \setminus \{0\}, \cdot)$ is a subgroup of $(\mathbb{R} \setminus 0, \cdot)$
4. If G is a group, then $H = G$ and $H = \{e\}$ are both subgroups of G.
5. If $m \in \mathbb{Z}$, then $m\mathbb{Z} \coloneqq \{ma \mid a \in \mathbb{Z}\}$ is a subgroup of $(\mathbb{Z}, +)$.

Example 8.7

Here are some non-examples:

1. $(\mathbb{Z}^+, +)$ is not a subgroup of $(\mathbb{Z}, +)$.

   The identity is not contained in $\mathbb{Z}^+$, and $-x$ is not in $\mathbb{Z}^+$, so there are no inverses either.
2. $(\mathbb{Z} \setminus \{0\}, \cdot)$ is not a subgroup of $(\mathbb{Q} \setminus \{0\}, \cdot)$.

   We don't have inverses, as $\frac{1}{x} \notin \mathbb{Z} \setminus \{0\}$ for $x \in \mathbb{Z} \setminus \{0\}$.

As a remark, the relation "is a subgroup of" is transitive; if H is a subgroup of G, and G is a subgroup of K, then H is a subgroup of K. This is not an equivalence relation though, since it is not symmetric.

Proposition 8.8

Let $H, K \subseteq G$ be subgroups. Then, $H \cap K$ is a subgroup of G.

Proof. 1. H and K are subgroups of G, so $e \in H$ and $e \in K$, so $e \in H \cap K$.

2. Let $x, y \in H \cap K$.

   Since H is a subgroup, $x, y \in H \implies x * y \in H$; similarly, since K is a subgroup, $x, y \in K \implies x * y \in K$. This means that $x, y \in H \cap K \implies x * y \in H \cap K$.

3. Let $x \in H \cap K$.

   Since H is a subgroup, $x \in H \implies x^{-1} \in H$; similarly, since K is a subgroup, $x \in K \implies x^{-1} \in K$. This means that $x \in H \cap K \implies x^{-1} \in H \cap K$.

With all these properties, we've shown that $H \cap K$ is a subgroup of G. □

9/14/2022

Lecture 9

More Subgroups

Proposition 9.1: Subgroup Criterion

A subset H of a group G is a subgroup iff

1. $H \neq \varnothing$
2. For $x, y \in H$, $x * y^{-1} \in H$.

Proof. If H is a subgroup of G, then $e \in H \implies H \neq \varnothing$, which satisfies the first criterion.

Further, if H is a subgroup, then it is closed under products and inverses, so if $x, y \in H$, then $y^{-1} \in H$ and $xy^{-1} \in H$, which satisfies the second criterion.

In the other direction, suppose H satisfies both criterion. Let $x \in H$; we know there exists such an element, because H is nonempty.

If we let $y = x$, then the second criterion gives $xy^{-1} = xx^{-1} = e \in H$, so the identity element is in H.

If we use the criterion on e and x, then we have $ex^{-1} = x^{-1} \in H$.

Finally, if $x, y \in H$, then $y^{-1} \in H$, and we can apply the criterion with x and y^{-1} to give $x(y^{-1})^{-1} = xy \in H$.

These three together show the three requirements of a subgroup. □

9.1 Examples of Subgroups

Let A be a nonempty subset of G.

Definition 9.2: Centralizer

We define $C_G(A) = \{g \in G \mid (\forall a \in A)(gag^{-1} = a)\}$. This is called the *centralizer* of A in G.

Notice that $gag^{-1} = a$ iff $ga = ag$ (by right-multiplying by g). This means that $C_G(A)$ is also the set of elements of G that commute with every element of A.

Proposition 9.3

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

Proof. First, we know that $C_G(A)$ is nonempty, since it contains the identity; e will always commute with any element. Equivalently, $e^{-1} = e$ so $eae^{-1} = a$ for all $a \in A$.

Next, if we have $x, y \in C_G(A)$, this means we have $xax^{-1} = a$ and $yay^{-1} = a$ for all $a \in A$. We further have

$$\begin{aligned} yay^{-1} &= a \\ y^{-1}yay^{-1} &= y^{-1}a \\ ay^{-1} &= y^{-1}a \\ ay^{-1}y &= y^{-1}ay \\ a &= y^{-1}ay \end{aligned}$$

This means that $y^{-1} \in C_G(A)$.

Next, suppose again that $x, y \in C_G(A)$. We have

$$\begin{aligned} (xy)a(xy)^{-1} &= xyay^{-1}x^{-1} \\ &= x(yay^{-1})x^{-1} \\ &= xax^{-1} && (y \in C_G(A)) \\ &= a && (x \in C_G(A)) \end{aligned}$$

This means that $xy \in C_G(A)$.

Together, we've shown that $C_G(A)$ satisfies all three properties of a subgroup. □

Definition 9.4: Center

Let $Z(G) = \{g \in G \mid (\forall x \in G)(xg = gx)\}$. This is the set of all elements commuting with all elements of G. This is called the *center* of G.

Note that $C_G(G) = Z(G)$. Further, since we've shown that the centralizer of any subset of G is a subgroup of G, we automatically get that $Z(G)$ is a subgroup of G.

Further, if G is abelian, the center $Z(G) = G$.

For the next example, let us define for elements g and a set A, $gAg^{-1} := \{gag^{-1} \mid a \in A\}$.

Definition 9.5: Normalizer

The *normalizer* of A in G is defined as $N_G(A) = \{g \in G \mid gAg^{-1} = A\}$.

Note that $g \in C_G(A)$ means that $gag^{-1} \in A$ for all $a \in A$, so $C_G(A) \subseteq N_G(A)$. (It's in fact a subgroup.)

Example 9.6

If G is abelian, then $C_G(G) = G$, and $C_G(A) = N_G(A) = G$. This is because everything commutes with everything else.

Example 9.7

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

We claim that $C_G(A) = A$.

Proof. Note that $rs = sr^{-1} \neq sr$, so s can't commute with all elements of A (in particular, it doesn't commute with r), so $s \notin C_G(A)$.

Further, note that r^i commutes with elements of A; we have $r^i r^j r^{-i} = r^{i+j-i} = r^j$. This means that $1, r, r^2, r^3 \in C_G(A)$.

We also know that $C_G(A)$ is a subgroup of G, so if sr^i were in $C_G(A)$, then we have $sr^i sr^{-i} \in C_G(A)$, but this implies that $s \in C_G(A)$, which we showed can't be the case. This is a contradiction, so none of sr^i are in $C_G(A)$. □

We also claim that $N_A(G) = G$.

Proof. Since $C_G(A) \subseteq N_G(A)$, we know that $\{1, r, r^2, r^3\} \subseteq N_G(A)$.

Checking s, we have

$$\begin{aligned} sAs^{-1} &= \{s1s^{-1}, srs^{-1}, sr^2s^{-1}, sr^3s^{-1}\} \\ &= \{1, r^3, r^2, r\} \end{aligned}$$

Here, we have $srs^{-1} = s(rs) = ssr^{-1} = r^{-1} = r^3$, and $sr^i s^{-1} = s(r^i s) = ssr^{-i} = r^{-i}$, using the identity $r^i s = sr^{-i}$.

This means that $sAs^{-1} = A$, and $s \in N_G(A)$. We also know that $1, r, r^2, r^3 \in N_G(A)$, and since $N_G(A)$ is a subgroup of G, we also know that $sr, sr^2, sr^3 \in N_G(A)$ as well. □

9/19/2022

Lecture 10

Cyclic Groups

Example 10.1

We claim that $Z(D_8) = \{1, r^2\}$.

Proof. Since $Z(D_8) \leq C_{D_8}(A) = A$, we know that $Z(D_8)$ is contained in A.

We also know that $rs = sr^{-1} \neq sr$, since $r^{-1} = r^3$. This means that $r \notin Z(D_8)$, as r does not commute with s.

Similarly, we know that $r^3 s = sr^{-3} \neq sr^3$, since $r^{-3} = r$. This means that $r^3 \notin Z(D_8)$.

However, we know that $r^2 s = sr^{-2} = sr^2$, since $r^{-2} = r^2$. This means that $r^2 \in Z(D_8)$.

We also have $1s = s1$, so $1 \in Z(D_8)$ as well.

All that is left is to show that 1 and r^2 commute with all sr^i:

$$(r^2)(sr^i) = sr^{-2}r^i = sr^i r^{-2} = (sr^i)(r^2).$$

We also have $(1)(sr^i) = (sr^i)(1)$, as desired.

Together, this all means that $Z(D_8) = \{1, r^2\}$. □

Definition 10.2: Cyclic Group

A group H is called a *cyclic group* if it is generated by 1 element. That is,

$$H = \langle x \rangle = \{x^n \mid n \in \mathbb{Z}\}.$$

Here, x is called a *generator* for H.

Example 10.3

Consider $\mathbb{Z}$ under $+$.

We have $(\mathbb{Z}, +) = \langle 1 \rangle = \{n \cdot 1 \mid n \in \mathbb{Z}\}$, since x^n under $(\mathbb{Z}, +)$ is just $n \cdot x$.

Notice that this is equivalent to $\langle -1 \rangle$.

Example 10.4

Consider $\mathbb{Z}/m\mathbb{Z}$ under $+$.

Similarly, we have $\mathbb{Z}/m\mathbb{Z} = \langle [1] \rangle = \{[1], [2], \ldots, [n-1], [0]\}$.

Notice that generators may not be unique (see Example 10.3).

Further, notice that cyclic groups are abelian.

Proof. Suppose $a, b \in H = \langle x \rangle$. As a result, we know that $a = x^\alpha$ and $b = x^\beta$, for some α, β.

This means that

$$ab = x^\alpha x^\beta = x^{\alpha+\beta} = x^{\beta+\alpha} = x^\beta x^\alpha = ba.$$

□

Proposition 10.5

Let $H = \langle x \rangle$. Then, $|H| = |x|$.

In other words, the order of a cyclic group H is the same as the order of the element x that generates H.

Proof. If $|x| = n$, then we know that $1, x, \ldots, x^{n-1}$ are all distinct (by a homework question). This means that H has at least n elements.

As such, it suffices to show that these are all the elements in H.

Suppose x^t is any power of x. We can use the division algorithm to write $t = nq + r$ for $0 \leq r < n$. This means that

$$x^t = x^{nq+r} = (x^n)^q x^r = 1^q x^r = 1 \cdot x^r = x^r \in \{1, \ldots, x^{n-1}\}.$$

As such, any x^t is equal to one of $\{1, \ldots, x^{n-1}\}$. This shows the result if x has finite order.

If $|x| = \infty$, the no power of x is the identity. Suppose we have $x^a = x^b$ for some a and b (WLOG suppose $a < b$). This means that $x^{b-a} = 1$, which is a contradiction; no power of x is the identity. As such, the only time where $x^a = x^b$ is if $a = b$.

This means that G has infinitely many distinct elements; no two distinct powers of x are the same. □

Proposition 10.6

If $|x| = n$, then $x^a = 1$ iff $n \mid a$.

Proof. Suppose $|x| = n$, and let $x^a = 1$. Suppose for contradiction that $n \nmid a$. This means that $\gcd(a, n) = d$ for some $d < n$.

By the Euclidean algorithm, we know that there exists $u, v \in \mathbb{Z}$ such that $nu + av = d$. This means that

$$x^d = x^{nu+av} = x^{nu}x^{av} = \left(x^n\right)^u \left(x^a\right)^v = 1^u 1^v = 1.$$

This is a contradiction, since we've just found a $d < n$ where $x^d = 1$, meaning $|x| = d < n$. As such, it must be the case that $n \mid a$.

Suppose $|x| = n$, and let $n \mid a$. This means that $a = nb$ for some $b \in \mathbb{Z}$, so $x^a = x^{nb} = (x^n)^b = 1^b = 1$. □

Theorem 10.7

Let G be a cyclic group. Then,

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

Proof.

1. Suppose $G = \langle x \rangle$. We can define the following map

$$\begin{aligned} \varphi : G &\to \mathbb{Z} \\ x^n &\mapsto n \end{aligned}$$

This map is well-defined; we have $x^a = x^b \implies a = b$, since we showed that elements of an infinite cyclic group are distinct.

We also have

$$\varphi(x^a x^b) = \varphi(x^{a+b}) = a + b = \varphi(x^a) + \varphi(x^b) = a + b,$$

so φ is a homomorphism.

We also know that φ is injective, since $a = b \implies x^a = x^b$. Since G contains all integer powers of x, each $n \in \mathbb{Z}$ has a pre-image, so φ is surjective. Since φ is injective and surjective, we've shown that φ is bijective.

This means that $G \cong (\mathbb{Z}, +)$, i.e. G is isomorphic to $(\mathbb{Z}, +)$.

2. Suppose $G = \langle x \rangle$, with $|x| = m$. We can define the following map

$$\begin{aligned} \varphi : G &\to \mathbb{Z}/m\mathbb{Z} \\ x^n &\mapsto [x] \end{aligned}$$

This map is well-defined; we have $x^a = x^b \implies a = b$, since each element of $\{1, x, x^2, \ldots, x^{m-1}\}$ are distinct, and each exponent $k > m$ maps to some element in this set, as $k = mq + r$ for $r < m$.

We also have

$$\varphi(x^a x^b) = \varphi(x^{a+b}) = [a + b] = [a] + [b] = \varphi(x^a) + \varphi(x^b).$$

We know that $|G| = |\mathbb{Z}/m\mathbb{Z}|$, so to show a bijection, it suffices to show only that φ is injective; in particular, suppose $\varphi(x^a) = \varphi(x^b)$, which means that $[a] = [b]$, which are distinct equivalence groups unless $a = b$, as desired.

□

9/19/2022

Lecture 11

Cyclic Groups (cont.)

A corollary of the theorem from last time is:

Corollary 11.1

Any two cyclic groups of the same order are isomorphic.

Proposition 11.2

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

Proof. Let $y = x^a$, and let $d = \gcd(n, a)$.

Then, $n = db$ and $a = dc$ for some $b, c \in \mathbb{Z}$. Further, since $d = \gcd(n, a)$, then $\gcd(b, c) = 1$.

We can then rewrite our claim; we want to show that $|y| = b$, as $|x^a| = \frac{n}{\gcd(n,a)} = \frac{n}{d} = b$.

Suppose we consider y^b:

$$y^b = x^{ab} = x^{dcb} = x^{dbc} = (x^{db})^c = (x^n)^c = 1^c = 1.$$

Here, we make use of the equations from earlier, and from the fact that $|x| = n$. This means that the order of y divides b, i.e. $|y| \mid b$ (by Proposition 10.6).

Further, let $k = |y|$; we've shown that $k \mid b$. Consider $y^k = x^{ak} = 1$.

This means that

$$\begin{aligned} n \mid ak &\implies db \mid ak \\ &\implies db \mid dck \\ &\implies b \mid ck && \text{(dividing out } d\text{)} \\ &\implies b \mid k && (\gcd(b, c) = 1) \\ &\implies b \mid |y| \end{aligned}$$

We've shown that $|y| \mid b$ and $b \mid |y|$, so it must be the case that $|y| = b$, as desired. □

Example 11.3

Consider $\mathbb{Z}/6\mathbb{Z} = \{[0], [1], [2], [3], [4], [5]\}$, and let $\mathbb{Z}/6\mathbb{Z} = \langle [1] \rangle$.

By Proposition 10.5, we know that $|[1]| = |\mathbb{Z}/6\mathbb{Z}| = 6$.

We can consider $[2] = [1] + [1] = [1]^2$, so

$$|[2]| = \frac{|[1]|}{\gcd(2, 6)} = \frac{6}{2} = 3.$$

(Here, $a = 2$ and $n = 6$.) We can continue this for the rest of the elements:

$$[3] = [1]^3 \qquad |[3]| = \frac{|[1]|}{\gcd(3, 6)} = \frac{6}{3} = 2$$

$$[4] = [1]^4 \qquad |[4]| = \frac{|[1]|}{\gcd(4, 6)} = \frac{6}{2} = 3$$

$$[5] = [1]^5 \qquad |[5]| = \frac{|[1]|}{\gcd(5,6)} = \frac{6}{1} = 6$$

Corollary 11.4

For a group G with $x \in G$. If x is relatively prime to $|G| = n$, then it generates the group.

Example 11.5

Consider D_{16}, i.e. symmetries of an octagon, and let $R = \langle r \rangle = \{1, r, r^2, \ldots, r^7\}$.

Let us look at $\langle r^2 \rangle = \{r^2, r^4, r^6, r^8 = 1\}$; this isn't a generator of R. Which elements *are* generators of R? All the powers that are relatively prime to 8, i.e. r^3, r^5, and r^7.

Checking $\langle r^3 \rangle$ as an example, we have $\langle r^3 \rangle = \{r^3, r^6, r^9 = r, r^4, r^7, r^{10} = r^2, r^5, r^8 = 1\}$.

Example 11.6

Consider $\mathbb{Z}/12\mathbb{Z}$; we have that [1], [5], [7], and [11] all generate $\mathbb{Z}/12\mathbb{Z}$, since they are all relatively prime to 12.

Theorem 11.7

If $H = \langle x \rangle$ is a cyclic group, then:

1. Every subgroup of H is cyclic.
2. If $|H| = n < \infty$, then for each positive integer a dividing n, there is a unique subgroup of H with order a. In particular, the subgroup is $\langle x^d \rangle$ for $d = \frac{n}{a}$.

Proof.

1. Let $K \leq H = \langle x \rangle$. If $K = \{1\}$, then K is generated by 1 and we're done.

   Otherwise, let $a = \min\{k > 0 \mid x^k \in K\}$. We claim that $\langle x^a \rangle$ generates K, i.e. $K = \langle x^a \rangle$.

   Suppose for contradiction that this is not the case, i.e. there exists an $x^b \in K$ such that $a \nmid b$. This means that we can use the division algorithm to conclude $b = aq + r$ with $0 < r < a$.

   We know that $x^b \in K$, and $x^{aq} \in K$, so by closure we know that $x^{b-aq} = x^r \in K$. However, we know that $r < a$, so a was not the minimum power in K; this is a contradiction.

   This means that $a \mid b$, and $x^b \in \langle x^a \rangle$, for any arbitrary b. As such, $\langle x^a \rangle = K$, as desired.

2. Suppose $a \mid n$, and take $\left\langle x^{\frac{n}{a}} \right\rangle$. We know that this subgroup has order $\frac{n}{\gcd\left(\frac{n}{a}, n\right)}$.

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

   We will leave uniqueness as an exercise.

□

9/21/2022

Lecture 12

Cyclic Groups (cont. II)

Example 12.1

Find the subgroups of $\mathbb{Z}/12\mathbb{Z}$.

Since each divisor of $|\mathbb{Z}/12\mathbb{Z}| = 12$ corresponds to a unique subgroup, and we have divisors $1,2,3,4,6,12$, we have the following subgroups:

- Order 12: $\langle[1]\rangle = \langle[5]\rangle = \langle[7]\rangle = \langle[11]\rangle$

  These are subgroups generated by elements coprime to 12.
- Order 6: $\langle[2]\rangle = \langle[10]\rangle$

  Subgroups of order 6 must be generated by elements $[x]$ such that $\gcd(x,12) = 2$, so that $\frac{12}{\gcd(x,12)} = 6$.
- Order 4: $\langle[3]\rangle = \langle[9]\rangle$

  Subgroups of order 4 must be generated by elements $[x]$ such that $\gcd(x,12) = 3$, so that $\frac{12}{\gcd(x,12)} = 4$.
- Order 3: $\langle[4]\rangle = \langle[8]\rangle$

  Subgroups of order 3 must be generated by elements $[x]$ such that $\gcd(x,12) = 4$, so that $\frac{12}{\gcd(x,12)} = 3$.
- Order 2: $\langle[6]\rangle$

  Subgroups of order 2 must be generated by elements $[x]$ such that $\gcd(x,12) = 6$, so that $\frac{12}{\gcd(x,12)} = 2$.
- Order 1: $\langle[12]\rangle$

  Subgroups of order 1 must be generated by elements $[x]$ such that $\gcd(x,12) = 12$, so that $\frac{12}{\gcd(x,12)} = 1$.

Notice that in $\mathbb{Z}/m\mathbb{Z}$, $\langle[a]\rangle \leq \langle[b]\rangle$ if and only if $\gcd(b,n) \mid \gcd(a,n)$, for $1 \leq a,b \leq n$.

12.1 Subgroups Generated by Subsets of a Group

Cyclic subgroups $\langle x\rangle$ are generated by a subset $\{x\}$ of the group containing a single element; this is the smallest subgroup of G containing x. We can generalize this to subsets of more than one element.

Proposition 12.2

For any nonempty collection of subgroups of G, the intersection of them is also a subgroup.

Proof. We've already talked about the intersection of two subgroups in Proposition 8.8; this is just an extension of it. □

Definition 12.3: Subgroup generated by a subset

If A is any subset of G, define

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

this is the *subgroup of G generated by A*. $\langle A\rangle$ is the minimal subgroup of G containing A.

This is a valid definition, but it isn't particularly helpful; we'd need to look at all possible subgroups containing A,

and take the intersection of all of them.

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

Let

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

Here, a_i and a_j don't necessarily need to be distinct. We also define $\overline{A} = \{1\}$ if A is empty.

In other words, $\overline{A}$ is the set of all finite products of elements in A and inverses of elements of A. Also note that A doesn't need to be finite in this definition; the only thing is that the $a_1^{\varepsilon_1} \cdots a_n^{\varepsilon_n}$ is a product of only finitely many elements in A.

Proposition 12.4

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

Proof. Using subgroup criterion, we'll see that $\overline{A}$ is a subgroup of A.

- $\overline{A}$ is not empty; even if A is empty, we defined $\overline{A} = \{1\}$.
- If $a, b \in \overline{A}$, we want to show that $ab^{-1} \in \overline{A}$ as well.

  We can write out a and b:

  $$a = a_1^{\varepsilon_1} \cdots a_n^{\varepsilon_n}$$
  $$b = b_1^{\delta_1} \cdots b_m^{\delta_m}$$

  We know that

  $$ab^{-1} = \left(a_1^{\varepsilon_1} \cdots a_n^{\varepsilon_n}\right)\left(b_1^{-\delta} \cdots b_m^{-\delta_m}\right).$$

  Here, we know that each base $a_i, b_i \in A$, and that $\varepsilon_i, \delta_i \in \pm 1$. This fits the criterion of being an element of $\overline{A}$, so $ab^{-1} \in \overline{A}$ as well.

Both criterion are met, so $\overline{A}$ is a subgroup of G.

We also know that $A \subseteq \overline{A}$, since all elements $a \in A$ are also in $\overline{A}$, as we can write a^1, which satisfies the criterion of being in $\overline{A}$.

Since $\overline{A} \leq G$ and $A \subseteq \overline{A}$, then $\langle A \rangle \subseteq \overline{A}$, since $\langle A \rangle$ is the minimal subgroup of G containing A.

Since $\langle A \rangle$ is a group containing A and it is closed under multiplication and inverses, $\overline{A} \subseteq \langle A \rangle$.

Together, this means that $\overline{A} = \langle A \rangle$. □

Example 12.5

Consider the subgroup $\langle (12), (13)(24) \rangle$ of S_4. It turns out that this is isomorphic to D_8.

12.2 Quotient Groups

Quotient groups are another way to get a smaller group from a group. Subgroups are one way to do so, where every element in a subgroup are also elements of the group. Quotient groups are slightly different.

Definition 12.6: Kernel

If $\varphi : G \to H$ is a homomorphism, the *kernel of* φ is the set

$$\operatorname{Ker}(\varphi) = \{g \in G \mid \varphi(g) = e\},$$

where e is the identity in H.

Definition 12.7: Image

If $\varphi : G \to H$ is a homomorphism, the *image of* φ in H (i.e. of G under φ in H) is the set

$$\mathrm{Im}(\varphi) = \{\varphi(x) \mid x \in G\}.$$

9/23/2022

Lecture 13

Quotient Groups

Proposition 13.1

Let H, G be groups, and let $\varphi : G \to H$ be a homomorphism. Then, $\mathrm{Ker}\,\varphi$ is a subgroup of G and $\mathrm{Im}\,\varphi$ is a subgroup of H.

Proof. First, we can prove that $\mathrm{Ker}(\varphi)$ is a subgroup of G.

Since e_G is such that $\varphi(e_G) = e_H$, we know that $e_G \in \mathrm{Ker}(\varphi)$. This means that $\mathrm{Ker}(\varphi) \neq \varnothing$.

Now, let $x, y \in \mathrm{Ker}(\varphi)$, such that $\varphi(x) = \varphi(y) = e_H$. Then, we have

$$\varphi(xy^{-1}) = \varphi(x)\varphi(y^{-1}) = \varphi(x)\varphi(y)^{-1} = e_H e_H^{-1} = e_H e_H = e_H.$$

This means that $xy^{-1} \in \mathrm{Ker}(\varphi)$. Together, we have that $\mathrm{Ker}(\varphi) \leq G$ by the subgroup criterion.

Next, we can prove that $\mathrm{Im}(\varphi)$ is a subgroup of H.

We know that $\varphi(e_G) = e_H \in \mathrm{Im}(\varphi)$, so $\mathrm{Im}(\varphi) \neq \varnothing$.

Now, let $x, y \in \mathrm{Im}(\varphi)$, and let $x = \varphi(a)$ and $y = \varphi(b)$, for some $a, b \in G$.

This means that we have $y^{-1} = \big(\varphi(b)\big)^{-1} = \varphi(b^{-1})$, so

$$xy^{-1} = \varphi(a)\varphi(b^{-1}) = \varphi(ab^{-1}).$$

This means that $xy^{-1} \in \mathrm{Im}\,\varphi$. Together, we have that $\mathrm{Im}(\varphi) \leq H$ by the subgroup criterion. □

13.1 Quotient Groups

Another way to get a smaller group from a group G apart from taking a subgroup is to form a quotient group. To understand quotient groups, we need to study homomorphisms first.

In particular, with a subgroup H of G (i.e. $H \leq G$), we have an injective homomorphism from H to G (i.e. $H \hookrightarrow G$). With a quotient group H of G, we have a surjective homomorphism from G to H (i.e. $G \twoheadrightarrow H$).

Recall that if $\varphi : G \to H$ is a homomorphism, the *fibers* of φ are sets of elements of G that are mapped to single elements of H.

In reference to Fig. 13.1, we can group the elements of G into groups, represented as rectangles, where each group maps to some element in H.

This suggests a natural multiplication of the fibers lying above the points; we'll see that this makes the set of fibers into a group.

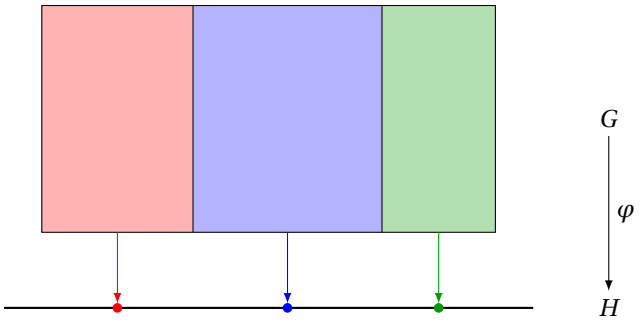


Figure 13.1: Illustration of fibers of φ

The idea is that G is partitioned into pieces (i.e. the fibers of φ), and we give these pieces/subsets the structure of a group.

Example 13.2

Suppose $G = \mathbb{Z}$, and $H = \langle x \rangle$, where $|x| = n$. Consider the mapping

$$\begin{aligned} \varphi : \mathbb{Z} &\to \langle x \rangle \\ a &\mapsto x^a \end{aligned}$$

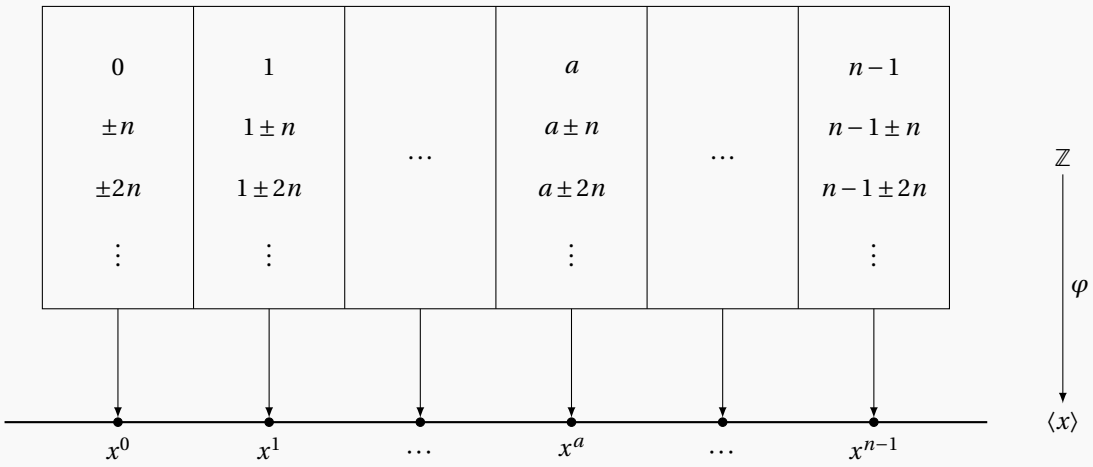
Here, we have $\varphi(a+b) = x^{a+b} = x^a x^b = \varphi(a)\varphi(b)$, so φ is a homomorphism.

We know that φ is surjective, since H has order n; the fiber of φ over x^a is then

$$\begin{aligned} \varphi^{-1}(x^a) &= \{m \in \mathbb{Z} \mid x^m = x^a\} \\ &= \{m \in \mathbb{Z} \mid x^{m-a} = 1\} \\ &= \{m \in \mathbb{Z} \mid (n \mid (m-a))\} \\ &= \{m \in \mathbb{Z} \mid m \equiv a \pmod{n}\} \end{aligned}$$

Note that the last set is exactly equal to $\bar{a}$, or $[a]$ in $\mathbb{Z}/n\mathbb{Z}$.

In the same illustration as before, we have



We know how to multiply in $H = \langle x \rangle$, i.e. $x^a x^b = x^{a+b}$. Further, the fibers of x^a, x^b, and x^{a+b} are $[a]$, $[b]$, and $[a+b]$ respectively.

The group operation (inherited from H) on the fibers of φ is then $[a] * [b] = [a+b]$. However, this is precisely the group $(\mathbb{Z}/n\mathbb{Z}, +)$; the identity is $n\mathbb{Z}$ ($[0]$), and the other fibers are $a + n\mathbb{Z}$ for $0 < a \leq n-1$.

As such, this is the group structure and the fibers of φ form the group $(\mathbb{Z}/n\mathbb{Z}, +)$.

The following is the formal definition of a quotient group.

Definition 13.3: Quotient Group

Let $\varphi : G \to H$ be a homomorphism with kernel K. The *quotient group* G/K "G mod K" is the group whose elements are the fibers of φ with group operation inherited from H (i.e. if X is the fiber above a and Y is the fiber above b, then $X * Y$ is the fiber above ab).

As a remark, this definition requires knowing φ explicitly. It is possible to define the group operation on fibers directly in terms of representatives, which we'll talk about next time.

9/26/2022

Lecture 14

Quotient Groups (cont.)

Last time, we talked about quotient groups, defining them in terms of the kernel of the homomorphism.

Today, we'll talk about another way to define quotient groups, defining multiplication in terms of representatives.

Proposition 14.1

Let $\varphi : G \to H$ be a surjective homomorphism with kernel K. Let $X \in G/K$ be a fiber above a (so $X = \varphi^{-1}(a)$). Then for any $u \in X$, $X = \{uk \mid k \in K\}$.

Proof. Take some $u \in X$; here, we have $\varphi(u) = a$. Let $uK = \{uk \in k \in K\}$. We want to show that $X = uK$.

First, we can show that $uK \subseteq X$.

For $k \in K$, we have

$$\begin{aligned} \varphi(uk) &= \varphi(u)\varphi(k) \\ &= \varphi(u) \cdot e && (k \in \operatorname{Ker}(\varphi)) \\ &= a \cdot e && (u \in X) \\ &= a \end{aligned}$$

This means that $uk \in X$; as such, we have that $\forall k \in K$, $uK \subseteq K$.

To show $X \subseteq uK$, let $g \in X$, and let $k = u^{-1}g$. We have

$$\begin{aligned} \varphi(k) &= \varphi(u^{-1})\varphi(g) \\ &= \varphi(u)^{-1}\varphi(g) && (u \in X, g \in X) \\ &= a^{-1} \cdot a \\ &= e \end{aligned}$$

This means that $k \in \operatorname{Ker}(\varphi)$, and since $k = u^{-1}g$, $g = uk \in uK$. Since any arbitrary element of X is in uK, we have that $X \subseteq uK$.

Together, we've shown that $X = uK$. □

Definition 14.2: Left Coset

For any subgroup $N \leq G$ and any $g \in G$, $gN = \{gn \mid n \in N\}$. We call this the *left coset* of N.

In this class, we'll just refer to this as the coset of N; we'll only make the distinction between the left and right cosets for one theorem.

For completeness, we have

Definition 14.3: Right Coset

For any subgroup $N \leq G$ and any $g \in G$, $Ng = \{ng \mid n \in N\}$. We call this the *right coset* of N.

Rephrasing Proposition 14.1, we've shown that the fibers of a homomorphism are the left cosets of the kernel. We've also shown that elements $X \in G/K$ are of the form gK.

Theorem 14.4

Let $\varphi : G \to H$ be a surjective homomorphism with kernel K. Then, the set of cosets gK with operation $uK * vK = uvK$ forms a group (the quotient group G/K).

Proof. Let $X, Y \in G/K$, and let $Z = XY \in G/K$.

We know that $X = \varphi^{-1}(a)$ and $Y = \varphi^{-1}(b)$ for some $a, b \in H$; we then have $Z = \varphi^{-1}(ab)$.

Let u, v be representatives of X and Y respectively. This means that $\varphi(u) = a$ and $\varphi(v) = b$.

By Proposition 14.1, we can write $X = uK$ and $Y = vK$. We now want to show that $uv \in Z$.

Since $Z = \varphi^{-1}(ab)$, we have

$$\begin{aligned} uv \in Z &\iff uv \in \varphi^{-1}(ab) \\ &\iff \varphi(uv) \in ab \\ &\iff \varphi(u)\varphi(v) = ab \end{aligned}$$

The last equation is true (since $\varphi(u) = a$ and $\varphi(v) = b$), so it must be the case that $uv \in Z$, and thus $Z = uvK$ (by Proposition 14.1). □

A next question would be: can we define G/N for any subgroup N in this way? We need a special kind of group to give G/N a group structure.

Proposition 14.5

We claim that if $\varphi : G \to H$ is a homomorphism with kernel K, then $gKg^{-1} \in K$ for all $g \in G$.

Proof. We want to show that $\varphi(gkg^{-1}) = e$ for all $k \in K$. We have

$$\begin{aligned} \varphi(gkg^{-1}) &= \varphi(g)\varphi(k)\varphi(g^{-1}) \\ &= \varphi(g)e\varphi(g)^{-1} \\ &= \varphi(g)\varphi(g)^{-1} \\ &= e \end{aligned}$$

This means that $gkg^{-1} \in K$ for all $g \in G$ and $k \in K$. □

This means that if we have a subgroup N of G such that $gNg^{-1} \in N$ for all $g \in G$, then we can show again that $uN * vN = uvN$, and the set of cosets of N forms the quotient group.

9/28/2022

Lecture 15

Quotient Groups (cont. II)

Continuing from last time, we want to show that if we have a subgroup N of G such that $gNg^{-1} \in N$ for all $g \in G$, then $g_1Ng_2N = g_1g_2N$, and doesn't depend on the choice of representative.

Proposition 15.1

Formally, we have a function from $G/N \times G/N \to G/N$, mapping $(xN, yN) \mapsto (xy)N$. We want to show that this doesn't depend on the representative, and if $x_1N = x_2N$ and $y_1N = y_2N$, then $x_1y_1N = x_2y_2N$.

Proof. We know that $x_1^{-1}x_2 \in N$ and $y_1^{-1}y_2 \in N$; this is because $x_1N = x_2N$, so $N = x_1^{-1}x_2N$, and in particular for $e \in N$, $x_1^{-1}x_2e = x_1^{-1}x_2 \in N$.

We want to show that $(x_1y_1)^{-1}x_2y_2 \in N$. Let us define

$$\begin{aligned} u &= (x_1y_1)^{-1}x_2y_2 \\ &= y_1^{-1}x_1^{-1}x_2y_2 \end{aligned}$$

We know that $x_1^{-1}x_2 \in N$, and that $y_1^{-1} \in G$. We then have

$$\begin{aligned} uy_2^{-1} &= y_1^{-1}x_1^{-1}x_2 \\ uy_2^{-1}y_1 &= y_1^{-1}x_1^{-1}x_2y_1 \end{aligned}$$

This is of the form gNg^{-1}, so the entire RHS is in N. This means that $uy_2^{-1}y_1 \in N$.

In particular, since $uy_2^{-1}y_1 \in N$ and $y_1^{-1}y_2 \in N$, then their product must also be in N, i.e. $uy_2^{-1}y_1 \cdot y_1^{-1}y_2 = u \in N$.

This then implies that $(x_1y_1)^{-1}x_2y_2 \in N$, or $x_1y_1N = x_2y_2N$. □

Definition 15.2: Normal Subgroup

A subgroup $N \leq G$ is called *normal* if $(\forall g \in G)(gNg^{-1} = N)$. We denote this as $N \trianglelefteq G$.

Notice that this is the same as saying every element of G normalizes N, i.e. $N_G(N) = \{g \in G \mid gNg^{-1} = N\} = G$.

Further, we are not saying that $gng^{-1} = n$; only that $gng^{-1} \in N$.

Also, notice that if G is abelian, then every subgroup of G is normal. This is because in this case, $gng^{-1} = n$ for all $g, n \in G$.

The claim from last time showed that the kernel of a homomorphism is a normal subgroup (Proposition 14.5). We want to show now that any normal subgroup can be realized as the kernel of some homomorphism.

Proposition 15.3

For $H \trianglelefteq G$, consider $\varphi : G \to G/H$, sending $x \mapsto xH$. We want to show that this is a homomorphism with $\text{Ker}(\varphi) = H$.

Proof. Notice that for all $x, y \in G$, $\varphi(xy) = xyH = xHyH = \varphi(x)\varphi(y)$, so φ is a homomorphism.

The identity element G/H is H, so $H \subseteq \text{Ker}(\varphi)$. For the other direction, consider any $x \in \text{Ker}(\varphi)$. We then have that $\varphi(x) = xH$ (from the map) and $\varphi(x) = H$ (since $x \in \text{Ker}(\varphi)$), so $xH = H$, and thus $x \in H$. □

We just looked at three perspectives on quotient groups:

- Fibers of homomorphisms
- Cosets of the kernel of a homomorphism
- Cosets of a normal subgroup

10/1/2022

Lecture 16

Lagrange's Theorem, Isomorphism Theorems

Theorem 16.1: Lagrange's Theorem

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

Proof. Let $|H| = n$ and let the number of cosets of H in G be k.

We know that the set of cosets of H partition G; we also know that the map $H \to gH$ mapping $h \mapsto gh$ is bijective (in HW), so $|H| = |gH| = n$.

Since G is partitioned into k disjoint subsets, each of which has cardinality n, we know that $|G| = k \cdot n$, and thus

$$k = \frac{|G|}{n} = \frac{|G|}{|H|}.$$

□

Definition 16.2: Index

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

Corollary 16.3

If G is a finite group and $x \in G$, then $|x| \mid |G|$. In particular, $x^{|G|} = 1$ for all $x \in G$.

Proof. We know that $|x| = |\langle x \rangle|$, so we can take the subgroup H generated by x.

Lagrange's theorem tells us that $|H| \mid |G|$, so $|x| \mid |G|$.

Because of this, we now can conclude that $x^{|G|} = 1$ (from Proposition 10.6). □

Corollary 16.4

Every group of prime order is cyclic.

Proof. Let $x \in G$, $x \neq 1$. We then know that $|\langle x \rangle| = |x| > 1$, and $|\langle x \rangle| \mid |G|$.

However, $|G|$ is prime, so $|\langle x\rangle| = |G|$ and therefore $G = \langle x\rangle$, so G is cyclic. □

Proposition 16.5

Every subgroup of index 2 is normal.

In particular, if $H \leq G$ and $[G : H] = 2$, then $H \trianglelefteq G$.

Proof. Let $g \in G \setminus H$.

Let the two left cosets of H in G be eH (with the identity e) and gH. We know that $eH = H$, so $gH = G \setminus H$.

Further, the two right cosets of H in G are Hg and $He = H$, so $Hg = G \setminus H$.

Together, this means that $gH = Hg \implies gHg^{-1} = H$ for all $g \in G$. This makes H normal, as claimed. □

As a remark, it is *not* true that every normal subgroup has index 2.

Further, the full converse to Lagrange's theorem is false; if G is a finite group and $n \mid |G|$, then G need not have a subgroup of order n. It turns out that it is true for $p \mid |G|$, which means that G has an element of order p.

In particular, Sylow's theorem says that if G has order $p^\alpha m$ for prime $p \nmid m$, then G has a subgroup of order p^α.

16.1 The Isomorphism Theorems

Let G and H be groups, with $e_G \in G$ and $e_H \in H$. Let $\varphi : G \to H$ be a homomorphism; recall that $\ker(\varphi) \subseteq G$ is a normal subgroup.

This means that we can form the quotient group $G/\ker(\varphi)$. Let $x, y \in G$ be in the same coset of $\ker(\varphi)$, i.e. $x\ker(\varphi) = y\ker(\varphi)$.

Recall that $x\ker(\varphi) = y\ker(\varphi)$ if and only if $x^{-1}y \in \ker(\varphi)$.

Further, we know that $x^{-1}y \in \ker(\varphi)$ if and only if $\varphi(x^{-1}y) = e_H$. This means that

$$\begin{aligned}
\varphi(x^{-1}y) = e_H &\iff \varphi(x^{-1})\varphi(y) = e_H \\
&\iff \varphi(x)^{-1}\varphi(y) = e_H \\
&\iff \varphi(x)\varphi(x)^{-1}\varphi(y) = \varphi(x) \\
&\iff \varphi(y) = \varphi(x)
\end{aligned}$$

That is, $\varphi(x) = \varphi(y)$ if and only if $x\ker(\varphi) = y\ker(\varphi)$. This means that φ is constant on each coset of $\ker(\varphi)$. This gives us a map of sets

$$\begin{aligned}
\psi : G/\ker(\varphi) &\to \operatorname{Im}(\varphi) \\
x\ker(\varphi) &\mapsto \varphi(x)
\end{aligned}$$

Here, ψ is well-defined because $x\ker(\varphi) = y\ker(\varphi) \implies \varphi(x) = \varphi(y)$.

10/3/2022

Lecture 17

Isomorphism Theorems

Theorem 17.1: First Isomorphism Theorem

Let G and H be groups, and let $\varphi : G \to H$ be a homomorphism. Then, $G/\operatorname{Ker}(\varphi) \cong \operatorname{Im}(\varphi)$.

Proof. Recall that we defined $\psi : G/\operatorname{Ker}(\varphi) \to \operatorname{Im}(\varphi)$ mapping $x\operatorname{Ker}(\varphi) \mapsto \varphi(x)$ is a well-defined map. Now we'll show that ψ is an isomorphism.

Note that by definition, the map is surjective; we defined the codomain to be elements of the form $\varphi(x)$. In particular, if $\varphi(x) \in \operatorname{Im}(\varphi)$, then we can take $x\operatorname{Ker}(\varphi)$ to be its pre-image.

Now, given $x, y \in G$,

$$\begin{aligned} \psi(x\operatorname{Ker}(\varphi)) &= \psi(y\operatorname{Ker}(\varphi)) \\ \varphi(x) &= \varphi(y) \\ x\operatorname{Ker}(\varphi) &= y\operatorname{Ker}(\varphi) \end{aligned}$$

The last equality comes from the fact that the kernel is always constant on the same coset, shown last time. This shows that ψ is injective.

Further, notice that

$$\begin{aligned} \psi(x\operatorname{Ker}(\varphi)\, y\operatorname{Ker}(\varphi)) &= \psi(xy\operatorname{Ker}(\varphi)) \\ &= \varphi(xy) \\ &= \varphi(x)\varphi(y) && (\varphi \text{ homomorphism}) \\ &= \psi(x\operatorname{Ker}(\varphi))\psi(y\operatorname{Ker}(\varphi)) \end{aligned}$$

This means that φ is a homomorphism.

Since ψ is a homomorphism and is a bijection, then ψ is an isomorphism from $G/\operatorname{Ker}(\varphi)$ to $\operatorname{Im}(\varphi)$. □

Example 17.2

Take the homomorphism $\varphi : (\mathbb{Z}, +) \hookrightarrow (\mathbb{Q}, +)$ with the inclusion mapping $x \mapsto x$.

The kernel of φ is $\{0\} = e_{(\mathbb{Z},+)}$, and the image is $\mathbb{Z} \subseteq \mathbb{Q}$.

The first isomorphism theorem tells us that $\mathbb{Z}/e_{(\mathbb{Z},0)} \cong \mathbb{Z}$. Here, each coset in $\mathbb{Z}/e_{(\mathbb{Z},0)}$ is a singleton set of a single element of $\mathbb{Z}$, so it makes sense that it is isomorphic to $\mathbb{Z}$.

Example 17.3

Take the homomorphism $\varphi : (\mathbb{Z}, +) \twoheadrightarrow (\mathbb{Z}/m\mathbb{Z}, +)$, mapping $a \mapsto [a]$.

The kernel $\operatorname{Ker}(\varphi) = m\mathbb{Z}$, and the image $\operatorname{Im}(\varphi) = \mathbb{Z}/m\mathbb{Z}$.

Here, by the first isomorphism theorem, we have $G = \mathbb{Z}$, so $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z}$, which is trivially true.

Example 17.4

Take the homomorphism $\varphi : G \to H$ mapping $g \mapsto e_H$.

The kernel $\ker(\varphi) = G$, and the image is $\text{Im}(\varphi) = e_H$.

The first isomorphism theorem tells us that $G/G \cong e_H$. Here, there is only one coset, containing the all elements in G.

Theorem 17.5: Third Isomorphism Theorem

Let G be a group and let H and K be normal subgroups of G.

If $H \leq K$, then $K/H \trianglelefteq G/H$ and $(G/H)/(K/H) \cong G/K$.

Proof. We will use the first isomorphism theorem on $\varphi : G/H \to G/K$, sending $gH \mapsto gK$.

If we can show that the kernel $\ker(\varphi) = K/H$, and that the image is G/K, then the first isomorphism theorem gives us that $(G/H)/(K/H) \cong G/K$.

Note that for $g_1K \in G/K$, we can take g_1H as the preimage, so that $\varphi(g_1H) = g_1K$. This means that φ is surjective, making $\text{Im}(\varphi) = G/K$.

The kernel is

$$\begin{aligned}\ker(\varphi) &= \{gH \in G/H \mid \varphi(gH) = K\} \\ &= \{gH \in G/H \mid gK = eK\} \\ &= \{gH \in G/H \mid g \in K\} \\ &= K/H\end{aligned}$$

□

Theorem 17.6: Correspondence Isomorphism Theorem

(Also known as the "third" isomorphism theorem, or the fourth isomorphism theorem.)

Let G be a group, with $N \trianglelefteq G$. Then, there is a natural bijection between subgroups of G containing N and subgroups of G/N.

10/10/2022

Lecture 18

Group Actions

Briefly, we'll end the isomorphism theorems with a small corollary of the first isomorphism theorem.

Corollary 18.1

Suppose $\varphi : G \to H$ is a homomorphism. Then,

1. φ is injective if and only if $\ker(\varphi) = \{e\}$.
2. $[G : \ker(\varphi)] = \left|\text{Im}(\varphi)\right|$

Proof. 1. Suppose φ is injective. Since φ is a group homomorphism, we must have $\varphi(e_G) = e_H$, where

$e_G \in G$ is the identity of G, and $e_H \in H$ is the identity of H.

Here, if $g \in \text{Ker}(\varphi)$, then $\varphi(g) = e_H$; since φ is injective, we must have that $g = e_G$. In particular, no other element can map to e_H; this means that $\text{Ker}(\varphi) = \{e_G\}$.

In the other direction, suppose $\text{Ker}(\varphi) = \{e_G\}$. Further, suppose that $\varphi(g_1) = \varphi(g_2)$ for $g_1, g_2 \in G$; we want to show that $g_1 = g_2$.

We have

$$\begin{aligned} \varphi(g_1) &= \varphi(g_2) \\ \varphi(g_1)\varphi(g_2)^{-1} &= e_H \\ \varphi(g_1 g_2^{-1}) &= e_H \\ g_1 g_2^{-1} &= e_G && (\text{Ker}(\varphi) = \{e_G\}) \\ g_1 &= g_2 \end{aligned}$$

As such, we've shown that φ is injective.

As a parenthetical, we can also use the 1st isomorphism theorem to prove this as well. In particular, $\text{Ker}(\varphi) = \{e_G\}$ is equivalent to saying that $G/\text{Ker}(\varphi) = G/\{e_G\} \cong \text{Im}(\varphi)$.

However, $G/\{e_G\} = G$, so we have that $G \cong \text{Im}(\varphi)$; since we have an isomorphism (which is bijective), then we must have an injection too.

2. Since $G/\text{Ker}(\varphi) \cong \text{Im}(\varphi)$, we know that $\left|G/\text{Ker}(\varphi)\right| = \left|\text{Im}(\varphi)\right|$. Further, by definition $\left|G/\text{Ker}(\varphi)\right| = [G : \text{Ker}(\varphi)]$ (since each element of $G/\text{Ker}(\varphi)$ is a coset of $\text{Ker}(\varphi)$ in G).

□

18.1 Group Actions

We want to define what it means for a group to "act" on a set. Firstly, we want to define a group acting on itself. By studying this, there are some interesting applications; in particular, we have a few theorems that arise:

- *Cayley's Theorem*: every group of order n is isomorphic to a subgroup of S_n.
- *Sylow's Theorems*: these theorems give a description of which and how many subgroups to expect of a given size, depending on the prime factorization of the group's order.

Definition 18.2: Group Action

Let G be a group, and let A be any set. A *group action* of G on A is a map $\cdot : G \times A \to A$ satisfying the following:

1. $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$

   Here, $g_1 g_2$ is the group operation, whereas $\cdot$ is the group action.

2. $1 \cdot a = a$, for all $a \in A$

   Here, $1 \in G$ is the group identity.

For each fixed $g \in G$, we can define a map $\sigma_g : A \to A$, mapping $a \mapsto g \cdot a$. There are a couple results that arise from studying this map.

Lemma 18.3

For each fixed $g \in G$, σ_g is a permutation of A. In other words, σ_G is bijective.

Moreover, the map $\varphi : G \to S_A$ (where S_A is the group of permutations of A) mapping $g \to \sigma_g$ is a homomorphism.

Proof. Firstly, we want to show that σ_g is a bijection. To show this, we can simply show that an inverse exists; in particular, we claim that $\sigma_{g^{-1}}$ is the inverse of σ_g.

The composition is

$$(\sigma_{g^{-1}} \circ \sigma_g)(a) = \sigma_{g^{-1}}(\sigma_g(a) = \sigma_{g^{-1}}(g \cdot a) = g^{-1} \cdot (g \cdot a) = (g^{-1}g) \cdot a = 1 \cdot a = a.$$

The other composition $(\sigma_g \circ \sigma_{g^{-1}})(a) = a$ as well by a similar computation.

Looking at φ, we need to check that $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$; we have

$$\begin{aligned}
\varphi(g_1 g_2)(a) &= \sigma_{g_1 g_2}(a) \\
&= (g_1 g_2) \cdot a \\
&= g_1 \cdot (g_2 \cdot a) \\
&= \sigma_{g_1}(\sigma_{g_2}(a)) \\
&= \big(\varphi(g_1)\varphi(g_2)\big)(a)
\end{aligned}$$

This means that φ is a homomorphism. □

We call φ the *permutation representation* associated with the action of G on A.

Proposition 18.4

There is a bijective correspondence between actions of G on A and homomorphisms $G \to S_A$.

Proof. Given an action $\cdot : G \times A \to A$, we've already seen how to go from an action to a homomorphism. In particular, we can define $\varphi : G \to S_A$ visa the permutation representation.

Given a homomorphism $\psi : G \to S_A$, we can define a group action

$$\begin{aligned}
G \times A &\to A \\
(g, a) &\mapsto \psi(g)(a)
\end{aligned}$$

□

Definition 18.5: Stabilizer

The *stabilizer* of a in G is the set $G_a = \{g \in G \mid g \cdot a = a\}$.

One can check that $G_a \leq G$.

10/12/2022

Lecture 19

Group Actions (cont.)

Definition 19.1: Kernel of an action

The *kernel* of an action of G on A is $\{g \in G \mid (\forall a \in A)(g \cdot a = a)\}$.

Notice that the kernel of an action is the stabilizer of *every* element $a \in A$.

Further, as a remark, the kernel of the action is the kernel of its permutation representation.

Example 19.2

Let $g \cdot a = a$ for all $g \in G$ and $a \in A$; this is called the trivial action.

This gives us the trivial homomorphism

$$\begin{aligned} \varphi : G &\to S_A \\ g &\mapsto e \end{aligned}$$

for e the identity element of S_A (i.e. the identity permutation).

Example 19.3

For any nonempty set A, suppose we define the group action of S_A on A by $\sigma \cdot a = \sigma(a)$ for all $\sigma \in S_A$ and $a \in A$.

Here, we have the homomorphism

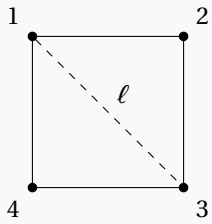
$$\begin{aligned} \varphi : S_A &\to S_A \\ \sigma &\mapsto \sigma \end{aligned}$$

(i.e. the identity homomorphism).

Example 19.4

Let $G = D_8$, and $A = \{1,2,3,4\}$.

Here, r is rotation as usual, and let s be the reflection across the line ℓ below:



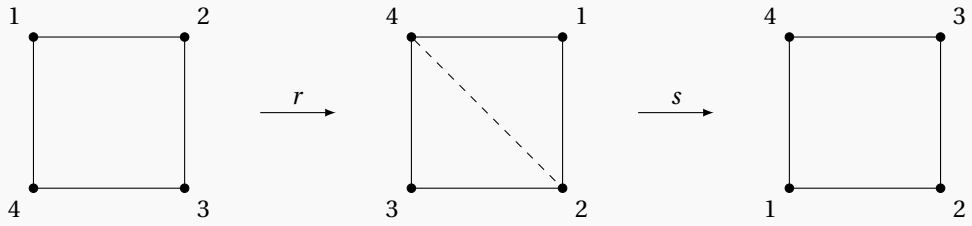
Here, we have the homomorphism

$$\begin{aligned} \varphi : D_8 &\to S_4 \\ r &\mapsto (1234) =: \sigma_r \\ s &\mapsto (24) =: \sigma_s \end{aligned}$$

In particular, since the permutation representation is a homomorphism, we have $\varphi(sr) = \varphi(s)\varphi(r)$, so

$$\varphi(sr) = \sigma_{sr} = \sigma_s \circ \sigma_r = (24)(1234) = (14)(23).$$

Pictorially, we have



Further, notice that the stabilizer of vertex 1 and vertex 3 is $\langle s \rangle$, and the stabilizer of vertex 2 and vertex 4 is $\langle sr^2 \rangle$.

The kernel of G on A is therefore $\{1\}$ (i.e. the identity of D_8, which is the intersection of all stabilizers among all vertices).

Proposition 19.5

Let G be a group acting on a nonempty set A. The relation on A defined by $a \sim b$ if and only if $a = g \cdot b$ for some $g \in G$ is an equivalence relation.

Further, for each $a \in A$, the number of elements in the equivalence class of a is $[G : G_a]$, i.e. the index of the stabilizer of a.

Proof. First, we can show that this is an equivalence relation:

- Reflexivity: Since $a = 1 \cdot a$ (for the identity $1 \in G$), we have $a \sim a$.
- Symmetry: Suppose $a \sim b$; this means that $a = g \cdot b$ for some $g \in G$, so we have

  $$g^{-1} \cdot a = g^{-1} \cdot (g \cdot b) = g^{-1} g \cdot b = 1 \cdot b = b.$$

  Since $g^{-1} \in G$, we have $b \sim a$.
- Transitivity: Suppose $a \sim b$ and $b \sim c$; this means that $a = g \cdot b$ and $b = h \cdot c$ for some $g, h \in G$. This means that

  $$a = g \cdot b = g \cdot (h \cdot c) = (gh) \cdot c.$$

  Since $gh \in G$, we have $a \sim c$.

Next, we can show that $[G : G_a]$ is the number of elements in the equivalence class of a. To do this, we can set up a bijection between the (left) cosets of G_a in G and the elements in the equivalence class of a.

Suppose we define $C_a = \{g \cdot a \mid g \in G\}$, i.e. C_a contains the elements in an equivalence class of a.

Suppose we have $b = g \cdot a \in C_a$; recall that $G_a = \{g \in G \mid g \cdot a = a\}$. Here, we have that gG_a is a left coset of G_a in G.

We can then define the map $b = g \cdot a \mapsto gG_a$, sending elements of C_a to left cosets of G_a in G.

This map is surjective, since for any $g \in G$, $g \cdot a$ is an element of C_a; we can always find the preimage of any coset gG_a.

Further, this map is injective:

$$g \cdot a = h \cdot a$$
$$h^{-1} \cdot g \cdot a = h^{-1} \cdot h \cdot a$$
$$(h^{-1}g) \cdot a = 1 \cdot a$$

This means that $h^{-1}g \in G_a$, and in particular $gG_a = hG_a$.

Since the map is both injective and surjective, this map is a bijection, showing that the number of left cosets of G_a in G is equal to the number of elements in the equivalence class of a. □

10/14/2022

Lecture 20

Group Actions (cont. 2)

Definition 20.1: Orbit

Let G be a group acting on a nonempty set A. The equivalence class $\{g \cdot a \mid g \in G\}$ is called the *orbit* of G containing a, denoted $\text{orb}(a)$.

Definition 20.2: Transitive Action

Let G be a group acting on a nonempty set A. The action of G on A is called *transitive* if there is only one orbit.

That is, given any $a, b \in A$, there exists a g such that $a = g \cdot b$.

Example 20.3

For example, D_8 acts transitively on the 4 vertices $A = \{1,2,3,4\}$.

Example 20.4

If G acts trivially on A, then $G_a = G$ for all $a \in A$; further, we have $\text{orb}(A) = a$ for all $a \in A$. That is, orbits are single elements.

This means that the action is transitive if and only if $|A| = 1$.

20.1 Groups acting on themselves

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

That is, the operation $G \times A \to A$ for $G = A$, mapping $(g, a) \mapsto g \cdot a = ga$. Here, ga is the product of two elements $g, a \in G$.

We can check that this action satisfies the two axioms of a group action:

- We have $g_1 \cdot (g_2 \cdot a) = g_1 \cdot (g_2 a) = g_1 g_2 a = (g_1 g_2) \cdot a$, so the first axiom is satisfied.
- We also have $1 \cdot a = 1a = a$ for all $a \in A$, so the second axiom is also satisfied.

If we generalize this to left multiplication on a *set* of elements on G, i.e. suppose G is a group, with $H \leq G$ and $A = \{gH \mid g \in G\}$.

We define the action of G on A as $g \cdot aH = gaH$ for all $g \in G$ and $a \in A$. One can also check that this is a group action.

If A has n elements $\{a_1H, \ldots, a_nH\}$, indexed from 1 to n, we one can describe σ_g as $\sigma_g(i) = j$ if and only if $ga_iH = a_jH$.

Example 20.5

Consider $G = D_8$ and $H = \langle s \rangle$. Let $A = \{1H, rH, r^2H, r^3H\}$, with labels 1 through 4 in order, respectively.

Let us compute σ_s.

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

This means that $\sigma_s = (24)$.

Similarly, $\sigma_r = (1234)$.

The permutation representation is a homomorphism, so these two elements determine $\varphi : G \to S_4$.

Theorem 20.6

Let G be a group, with $H \leq G$. Let $A = \{gH \mid g \in H\}$, and let G act by left multiplication on A. Then,

1. G acts transitively on A
2. The stabilizer in G of $1H \in A$ is H.
3. The kernel of the associated permutation representation is $\bigcap_{x \in G} xHx^{-1}$.

Proof.

1. Let $aH, bH \in A$, and let $g = ba^{-1}$.

   Then, $g \cdot aH = ba^{-1}aH = bH$, so arbitrary elements of A lie in the same orbit. This means that G acts transitively on A.

2. The stabilizer of $1H$ is
$$\{g \in G \mid g \cdot 1H = 1H\} = \{g \in G \mid gH = H\} = H.$$

3. The kernel of the action is
$$\begin{aligned} \{g \in G \mid (\forall x \in G)(gxH = xH)\} &= \{g \in G \mid (\forall x \in G)(x^{-1}gxH = H)\} \\ &= \{g \in G \mid (\forall x \in G)(x^{-1}gx \in H)\} \end{aligned}$$
   This means that $\exists h \in H$ such that $x^{-1}gx = h$; this allows us to conclude $g = xhx^{-1}$, or $g \in xHx^{-1}$.
$$\begin{aligned} &= \{g \in G \mid (\forall x \in G)(g \in xHx^{-1})\} \\ &= \bigcap_{x \in G} xHx^{-1} \end{aligned}$$

□

Corollary 20.7: Cayley's Theorem

Every group is isomorphic to a subgroup of some symmetric group. If $|G| = n$, then G is isomorphic to a subgroup of S_n.

Proof. Let $H = 1$ (the trivial group) and apply the previous theorem.

That is, take the permutation representation $\varphi : G \to S_G$. The kernel $\text{Ker}(\varphi) = \bigcap_{x \in G} xHx^{-1}$. With $H = 1$, the kernel $\text{Ker}(\varphi) = 1$.

By the first isomorphism theorem, $G \cong \text{Im}(\varphi) \leq S_G$. □

10/19/2022

Lecture 21

Conjugation Action

Continuing on with Cayley's theorem, we have the following corollary.

Corollary 21.1

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

Proof. Let $H \leq G$, and let $[G : H] = p$ (i.e. the index of H in G is p).

Consider the permutation representation coming from G acting on cosets of H, i.e. acting on $\{gH \mid g \in G\}$, containing p different cosets. This permutation representation is $\varphi : G \to S_p$.

Let $K = \text{Ker}(\varphi)$, and let $[H : K] = k$. Then,

$$[G : K] = [G : H] \cdot [H : K] = pk.$$

Since H has p left cosets, G/K is isomorphic by the first isomorphism theorem to a subgroup of S_p.

So, $|G/K| = pk$ must divide $p!$ by Lagrange's theorem. In particular, $k \mid \frac{p!}{p}$, or $k \mid (p-1)!$.

However, all prime divisors of $(p-1)!$ are less than p, but p was the smallest prime dividing $|G|$ by assumption. This means that p is also the smallest prime dividing $|G/K|$, so k can't have a prime factor smaller than p, and $k \mid (p-1)!$ means k can't have a prime factor larger than p, so $k = 1$.

In particular, this means $[H : K] = 1$ and $H = K \trianglelefteq G$. □

Proposition 21.2

Let G be a group, and let H be a subgroup of G with $[G : H] = n < \infty$. Then, there exists a normal subgroup N of G such that $N \leq H$ and $[G : N] \mid n!$.

Proof. Let $X = \{x_1 H, \ldots, x_n H\}$, and let $\varphi : G \to S_X \cong S_n$, mapping $g \mapsto \sigma_g$. Here, we have $\sigma_g(x_j H) = g x_j H$.

Since φ is a homomorphism, let $N = \text{Ker}(\varphi)$; by the third item in Theorem 20.6, we know that the kernel of this action is a subgroup of H, i.e. $N \leq H$.

Additionally, by the first isomorphism theorem, we know that G/N is isomorphic to a subgroup of S_x, so by

Lagrange's theorem,

$$[G:N] = |G/N| \,|\, |S_x|.$$

That is, $[G:N] \mid n!$. □

21.1 Groups acting on themselves by conjugation

Let G be a group and let $A = G$, and let G act on A via $g \cdot a = gag^{-1}$ for all $g \in G$ and $a \in A$.

We can check that this is a group action:

- We have for all $g_1, g_2 \in G$ and $a \in A$,

$$\begin{aligned} g_1 \cdot (g_2 \cdot a) &= g_1 \cdot g_2 a g_2^{-1} \\ &= g_1 g_2 a g_2^{-1} g_1^{-1} \\ &= (g_1 g_2) a (g_1 g_2)^{-1} \\ &= g_1 g_2 \cdot a \end{aligned}$$

- Additionally, for all $a \in A$, $1 \cdot a = 1a1^{-1} = a$.

Definition 21.3: Conjugate

Two elements a and b are said to be *conjugate* in G if there exists a $g \in G$ such that $b = gag^{-1}$.

Equivalently, a and b are in the same orbit under the conjugation action.

Definition 21.4: Conjugacy classes

The orbits of G under the conjugation action are called the *conjugacy classes of* G.

Note that if G is abelian, this action is trivial; $gag^{-1} = a$ for all $a \in G$, since $ga = ag$ for all $a, g \in G$.

If $|G| > 1$, the action is *not* transitive, because $\{1\}$ is always in its own conjugacy class, and $\{a\}$ is a conjugacy class for any $a \in Z(G)$.

We can generalize this action; in particular, instead of acting on elements of G, we can act on subsets of G.

If $S \subseteq G$, define $gSg^{-1} = \{gsg^{-1} \mid s \in S\}$. A group acts on $\mathscr{P}(G)$ via $g \cdot S = gSg^{-1}$ for any $g \in G$ and $S \in \mathscr{P}(G)$.

Definition 21.5: Conjugate subsets

Two subsets S and T are *conjugate* in G if there is some $g \in G$ such that $T = gSg^{-1}$.

For the action by conjugation, the stabilizer is

$$G_S = \{g \in G \mid gSg^{-1} = S\} = N_G(S).$$

That is, the stabilizer is the normalizer of S in G.

Proposition 21.6

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 an element $s \in G$ is $[G : G_s] = [G : N_G(s)] = [G : C_G(s)]$.

As a remark, the action of G partitions G into conjugacy classes.

10/19/2022

Lecture 22

Class Equation, Sylow Theorems

Theorem 22.1: Class Equation

Let G be a finite group, and let $g_1, \dots, g_r$ be representatives of distinct conjugacy classes of G not contained in the center $Z(G)$.

Then,

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

That is, the order of G is the size of the center plus the sum across all indices of the center of g_i in G.

Proof. We can write $Z(G) = \{1, z_2, \dots, z_m\}$, and let g_i be a representative of K_i, a conjugacy class not in the center.

Since each element in the center is in its own conjugacy class, the set of conjugacy classes are

$$\{1\}, \{z_2\}, \dots, \{z_m\}, K_1, \dots, K_r.$$

Since these classes partition G, we have

$$\begin{aligned} |G| &= \sum_{i=1}^{m} |\{z_i\}| + \sum_{i=1}^{r} |K_i| \\ &= \sum_{i=1}^{m} 1 + \sum_{i=1}^{r} |K_i| && \text{(singleton sets)} \\ &= |Z(G)| + \sum_{i=1}^{r} [G : C_G(g_i)] \end{aligned}$$

The last simplification from $|K_i| = [G : C_G(g_i)]$ is due to the orbit-stabilizer theorem, i.e. the size of the orbit is the index of the stabilizer. □

Example 22.2

If G is abelian, then $|G| = |Z(G)|$, since all elements are in the center of G.

Example 22.3

Consider $D_8 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$.

The conjugacy classes of D_8 are:

$$\{1\}, \{r^2\}, \{r, r^3\}, \{s, sr^2\}, \{sr, sr^3\}.$$

For the conjugacy class of r, we have $r^i r r^{-i} = r$, but $sr^i r r^{-i} s = srs = r^3$; this means that the conjugacy class is $\{r, r^3\}$.

For the conjugacy class of s, we have $r^i s r^{-i} = sr^{-2i}$, which is equal to sr^2 if i is odd, and equal to s if i is even. We also have $sr^i sr^{-i}s = sr^i rss = sr^{2i}$, which gives the same results. This means that the conjugacy class is $\{s, sr^2\}$.

For the conjugacy class of sr, we have $r^i sr r^{-i} = sr^{-i} r r^{-i} = sr^{-2i+1}$, which gives sr if i is even, and sr^3 if i is odd. We also have $sr^i sr r^{-i} s = ssr^{-i} r r^{-i} s = r^{-2i+1} s = sr^{2i-1}$, which gives the same result. This means that the conjugacy class is $\{sr, sr^3\}$.

The class equation gives us

$$|D_8| = |Z(G)| + \left(\left|\{r, r^3\}\right| + \left|\{s, sr^2\}\right| + \left|\{sr, sr^3\}\right|\right) = 8.$$

Theorem 22.4

If p is prime, and G is a group of order p^a for $a \geq 1$, then G has a nontrivial center (i.e. $Z(G)$ is more than just the identity).

Proof. If $a = 1$, then $|G| = p$. We also know that every group of prime order is cyclic, and thus is abelian. This means that $G = Z(G)$, and $Z(G)$ is not trivial.

For $a > 1$, we know that $C_G(g_i) \neq G$ for all i, so p divides $\frac{|G|}{|C_G(g_i)|} = \frac{p^a}{p^n}$ for some $n < a$

Since $p \mid |G|$ and $p \mid [G : C_G(g_i)]$, then in the class equation, we have

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

which forces $p \mid |Z(G)|$. This means that $Z(G)$ is nontrivial; it has at least p elements (it can't have 0 elements, and must be a multiple of p). □

Corollary 22.5

If $|G| = p^2$ for some prime p, then G is abelian.

Proof. We know that $Z(G)$ is nontrivial by the previous theorem. Since $Z(G)$ is a subgroup of G, its order $|Z(G)|$ must be a divisor of $|G| = p^2$. That is, $|Z(G)|$ is either p or p^2.

If $|Z(G)| = p^2$, then $G = Z(G)$, so G is abelian.

Otherwise, if $|Z(G)| = p$, then $|G/Z(G)| = |G|/|Z(G)| = p$, which means $G/Z(G)$ is a group of prime order, and is abelian. This means that G must also be abelian (which we proved in HW). □

10/21/2022

Lecture 23

Sylow Theorems

Today, we'll be talking about Sylow theorems. Recall Lagrange's theorem: the order of a subgroup $H \leq G$ must divide the order of G if G is finite.

The full converse to Lagrange is not true in general; Sylow theorems are a partial converse.

As an initial (long) warm-up, we have the following lemma.

Lemma 23.1: Cauchy's Theorem

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

Proof. We will proceed by induction on $|G|$.

We know that $|G| > 1$, so our base case is if $|G| = 2$ (or generally, $|G| = p$).

This means that every element of G other than the identity has order p (because G is cyclic and abelian, as it has prime order).

Suppose $|G| > p$ (and $p \mid |G|$). Take an $x \in G$ such that x is not the identity in G. We have two cases: either $p \mid |x|$, or $p \nmid |x|$.

In the first case, if $p \mid |x|$, then $|x| = pn$ for some $n \in \mathbb{Z}$. Here, take x^n; we know that $|x^n| = p$, since $|x^n| = \frac{pn}{\gcd(pn,n)} = \frac{pn}{n} = p$. This means that we've found an element of order p, and we're done.

In the second case, suppose $p \nmid |x|$. Here, let $N = \langle x \rangle$. Because G is abelian, we know that $N \trianglelefteq G$. This means that we can take the quotient group G/N.

We have $|G/N| = |G|/|N| < |G|$ if $|N| > 1$. Since $p \nmid |N|$ and $p \mid |G|$ by assumption, we know that $p \mid |G/N|$.

By the inductive hypothesis, sine $|G/N| < |G|$, we know that there exists an element of order p in G/N, since G/N is finite, abelian, and has an order divisible by p.

The elements of G/N are of the form gN for $g \in G$; suppose this element we found of order p is $\overline{y} = yN$ for some $y \in N$. Note that $y \notin N$ (this is not the identity coset, otherwise this coset would have order $1 \neq p$).

We do know that $y^p \in N$ though, since the order of yN is p; we'd have $(yN)^p = y^p N = N$.

We can look at the cyclic group $\langle y^p \rangle$, and we can look at the cyclic group $\langle y \rangle$. We know that $\langle y^p \rangle \subseteq \langle y \rangle$ (since $y^p \in \langle y \rangle$). However, $y \notin N$, but $\langle y^p \rangle \notin N$, so $\langle y^p \rangle \neq \langle y \rangle$. This means that $\left|\langle y^p \rangle\right| < \left|\langle y \rangle\right|$.

As before, we have $\left|y^p\right| = \frac{|y|}{\gcd(|y|,p)}$. Looking at the denominator, we know that $\gcd(\left|y\right|, p) \neq 1$, since this means that $\left|y^p\right| = \frac{|y|}{1} = \left|y\right|$, which we've proved is false. This means that the GCD would have to be equal to p (as the GCD must be a divisor of p), and we can conclude $\left|y^p\right| = \frac{|y|}{p}$, so $p \mid \left|y\right|$.

However, we've done this case before; we'd have $\left|y\right| = pn$ for some $n \in \mathbb{Z}$, and $\left|y^n\right| = p$. Since $y^n \in G$, we've found our element of G of order p.

In both cases, we're able to find an element of G of order p; by the principles of induction, all finite abelian groups with order divisible by p contain an element of order p. □

Definition 23.2: p-groups, p-subgroups, and Sylow p-subgroups

Let G be a group and let p be a prime.

- A group of order p^α for some $\alpha \geq 0$ is called a *p-group*.

  Subgroups of order p^α are called *p-subgroups*.
- If G is of order $p^\alpha m$ where $p \nmid m$, then p^α is called a *p-Sylow subgroup* (or a *Sylow p-subgroup*).
- The set of Sylow p-subgroups of G will be denoted $\mathrm{Syl}_p(G)$ and the number of Sylow p-subgroups of G will be denoted $n_p(G)$.

Note that Sylow p-subgroups are also p-subgroups, but not the other way around.

10/24/2022

Lecture 24

Sylow Theorems (cont.)

Theorem 24.1: Sylow 1

Let G be a group of order $p^\alpha m$ where p is a prime not dividing m. Then, there exists a Sylow p-subgroup. That is, $\mathrm{Syl}_p(G) \neq \varnothing$.

Proof. We proceed by induction on $|G|$. With $|G| = 1$, we have nothing to prove.

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

If $p \mid |Z(G)|$, by Lemma 23.1, $Z(G)$ has an element of order p, and therefore a subgroup of order p. Let us call this subgroup N.

Let $\overline{G} = G/N$; here, we have

$$\left|\overline{G}\right| = \frac{|G|}{|N|} = \frac{p^\alpha m}{p} = p^{\alpha-1} m.$$

By the inductive hypothesis, $\overline{G}$ has a subgroup $\overline{P}$ of order $p^{\alpha-1}$. Let P be the subgroup of G containing N such that $P/N = \overline{P}$. We know such a subgroup exists, because the third isomorphism theorem states that subgroups of G containing N are in bijection with subgroups of G/N.

This means that $|P| = |P/N| \cdot |N| = p^{\alpha-1} \cdot p = p^\alpha$. As such, we've found a subgroup P that is a Sylow p-subgroup of G.

Next, suppose $p \nmid |Z(G)|$. Let $g_1, \ldots, g_r$ be representatives of distinct non-central conjugacy classes of G. The class equation gives us

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

If $p \mid [G : C_G(g_i)]$ for all i, this would imply that $p \mid |Z(G)|$—this is because p divides the LHS of the class equation, so it must divide the RHS as well. This is a contradiction, so it must be the case that $p \nmid [G : C_G(g_i)]$ for some i.

For this i, let $H = C_G(g_i)$; we know that $|H| = p^\alpha k$ for some k such that $p \nmid k$. This is because $\left|C_G(g_i)\right| = |G|/[G : C_G(g_i)]$ (since cosets of $C_G(g_i)$ are each of the same size, partitioning G; $|G|$ divided by the number of cosets gives the size of a coset, including $C_G(g_i)$); we know $p \nmid [G : C_G(g_i)]$, so $|H| = p^\alpha k$.

Since $g_i \notin Z(G)$, we know that $C_G(g_i) \neq G$, so $|H| \leq |G|$. By induction, H has a Sylow p-subgroup P, but $|P| = p^\alpha$, so P is also a Sylow p-subgroup of G. □

Theorem 24.2: Sylow 2

Let G be a group of order $p^\alpha m$ where p is a prime not dividing m. If P is a Sylow p-subgroup of G and Q is any p-subgroup of G (i.e. $|Q| = p^\beta$). Then, there exists a $g \in G$ such that $Q \leq gPg^{-1}$. That is, Sylow p-subgroups are conjugate.

In particular, any two Sylow p-subgroups of G are conjugate in G.

Theorem 24.3: Sylow 3

Let G be a group of order $p^\alpha m$ where p is a prime not dividing m. The number of Sylow p-subgroups of G is of the form $1 + kp$ for some $k \in \mathbb{Z}$ (i.e. $n_p(G) \equiv 1 \pmod{p}$).

Moreover, $n_p(G) = [G : N_G(P)]$ for any $P \in \mathrm{Syl}_p(G)$; this means that $n_p(G) \mid m$.

Example 24.4

Consider S_3. We know that $|S_3| = 6 = 2^1 \cdot 3 = 3^1 \cdot 2$.

Sylow 1 tells us that there exists a Sylow 2-subgroup (of order 2), and there exists a Sylow 3-subgroup (of order 3).

The Sylow 2-subgroups are $\langle(12)\rangle$, $\langle(23)\rangle$, and $\langle(13)\rangle$. We can also verify by Sylow 3 that $n_2(S_3) = 3 \equiv 1 \pmod 2$.

The only Sylow 3-subgroup is $\langle 123\rangle$ (equivalent to $\langle(132)\rangle$). Again, we can verify by Sylow 3 that $n_3(S_3) = 1 \pmod 3$.

10/26/2022

Lecture 25

Rings

So far, we've been talking about groups, which are sets with a single binary operation. Now, we'll move on to talk about *rings*, which are sets with two binary operations. One operation gives group structure, and another is associative with an identity (the two operations must also be compatible).

There have been multiple definitions of rings in the past from the 1870s through the 1920s; Dedekind and Hilbert studied rings but did not have a formal definition, Fraenkel had too strict of a definition, and Noether gave the modern definition of rings.

Definition 25.1: Ring

A *ring* R is a set with two binary operations $+$ and $\times$, satisfying

1. $(R, +)$ is an (abelian) group
2. $\times$ is associative: $(a \times b) \times c = a \times (b \times c)$ for all $a, b, c \in R$
3. The distributive law holds for all a, b, c:

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

4. There is a multiplicative identity 1 such that $1 \times a = a \times 1 = a$ for all $a \in R$

Definition 25.2: Commutative ring

A ring is called *commutative* if multiplication is commutative.

As a remark, there is a debate as to whether rings should have the identity; in this class, they do.

The 1921 definition of Noether did not include it, but in the 1960s people started using it. It'll likely be assumed in most books you'll use in classes after this class.

Note that $1 \in R$ implies that $(R,+)$ is abelian; we have the following two equations from the distributive law:

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

This means that $a+b+a+b = a+a+b+b$, leading to the commutativity; $(R,+)$ is thus abelian.

Some people say "ring with unit", or omit the identity by writing "rng".

Definition 25.3: Division ring

A ring R is called a *division ring* if every nonzero element $a \in R$ has a multiplicative inverse; i.e. there exists a $b \in R$ such that $ba = ab = 1$.

Definition 25.4: Field

A commutative division ring is called a *field*.

Example 25.5

Here are some examples (and non-examples) of rings:

- The zero ring is $R = \{0\}$; here $0 = 1$, and the ring is commutative.
- $(\mathbb{Z},+,\times)$, where $+$ and $\times$ are defined as usual. This is also a commutative ring.
- $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$, and $(\mathbb{C},+,\times)$, where $+$ and $\times$ are defined as usual. These are all also commutative rings.
- $(\mathbb{Z}/n\mathbb{Z},+,\times)$ is also a commutative ring.
- Let R be a ring; $M_n(R)$ (i.e. the $n \times n$ matrices with elements in R) is a ring for $n \geq 2$, but it is not commutative.
- $(2\mathbb{Z},+,\times)$ is not a ring, because there is no multiplicative identity; it would be 1, but $1 \notin 2\mathbb{Z}$.
- $(\mathbb{Q}\setminus\{0\},+,\times)$ is not a ring, because there is no additive identity; it would be 0, but it is excluded.

Example 25.6

Here are some examples (and non-examples) of fields:

- $(\mathbb{Z},+,\times)$ is not a field, since not all elements have multiplicative inverses
- $(\mathbb{Q},+,\times)$ is a field
- $(\mathbb{Z}/n\mathbb{Z},+,\times)$ is a field if and only if n is prime

Example 25.7

As a more abstract example, let X be a nonempty set, and let A be any ring.

The collection of all set maps $f: X \to A$ is a ring with $+$ and $\times$ defined as

$$(f+g)(x) = f(x) + g(x)$$
$$(fg)(x) = f(x)g(x)$$

The ring axioms follow, because the axioms hold for A. $1 \in R$ is the constant function $1(x) = x$ for all $x \in x$. Further, R is commutative if and only if A is commutative.

Lemma 25.8

Let R be a ring. Then,

1. $0a = a0 = 0$ for all $a \in R$
2. $(-a)b = a(-b) = -(ab)$ for all $a, b \in \mathbb{R}$
3. $(-a)(-b) = ab$
4. $-a = (-1)a$

Proof.

1. We have
$$0a = (0+0)a = 0a + 0a,$$
which means that $0a = 0$ after subtracting $0a$ from both sides.
2. We have
$$ab + (-a)b = (a + -a)b = 0b = 0,$$
which means that $-(ab) = (-a)b$. The same argument applies for $a(-b)$.
3. We have
$$(-a)(-b) + a(-b) = (-a + a)(-b) = 0(-b) = 0.$$
This means that $(-a)(-b) = -a(-b) = -(-ab)$ by the second item. This means that $(-a)(-b) = ab$.
4. We have $(-1)a + (1)a = (-1+1)a = 0a$, so $(-1)a + a = 0$ and $(-1)a = -a$.

□

10/28/2022

Lecture 26

Direct Products, Finitely Generated Abelian Groups

Definition 26.1: Direct Product

Let $(G_1, *_1), \ldots, (G_n, *_n)$ be groups. The *direct product* $(G_1 \times \cdots \times G_n, *)$ is the set of n-tuples $(g_1, g_2, \ldots, g_n)$ where $g_i \in G_i$ with the operation defined component-wise

$$(g_1, g_2, \ldots, g_n) * (h_1, h_2, \ldots, h_n) = (g_1 *_1 h_1, g_2 *_2 h_2, \ldots, g_n *_n h_n).$$

Example 26.2

Suppose $G_1 = \mathbb{Z}$ with operation $+$, $G_2 = S_3$ with operation $\circ$, and $G_3 = \mathbb{Q} \setminus \{0\}$ with operation $\times$. We'd have

$$(n, \sigma, v) * (m, \tau, w) = (n + m, \sigma \circ \tau, v \times w).$$

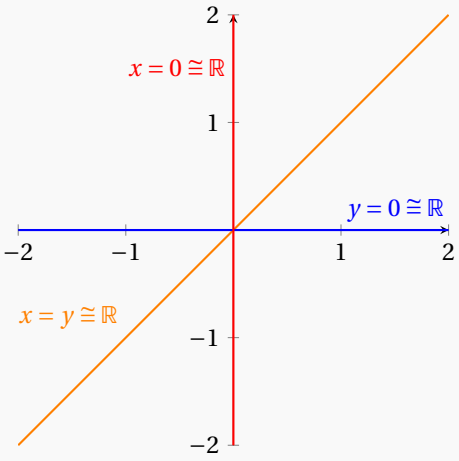
Proposition 26.3

If $G_1, \ldots, G_n$ are groups, their direct product is a group of order $|G_1| \times |G_2| \times \cdots \times |G_n|$.

Further, $G_1 \times \cdots \times G_n$ contains an isomorphic copy of each G_i.

Example 26.4

For example, take $\mathbb{R} \times \mathbb{R}$. Any line through the origin is a copy of $\mathbb{R}$.



Formally, we have the following proposition.

Proposition 26.5

Let $G_1, \dots, G_n$ be groups and let $G = G_1 \times \cdots \times G_n$. The following all hold:

1. For each fixed i,
$$G_i \cong \{(1, \dots, 1, g_i, 1, \dots, 1) \mid g_i \in G_i\}.$$
Identifying G_i with this subgroup (we'd need to view G_i as this group, since as-is G_i is not a subgroup of G), we have $G_i \trianglelefteq G$ and $G/G_i \cong G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n$.
2. For each fixed i, the map $\pi_i : G \to G_i$ defined by $(g_1, \dots, g_n) \mapsto g_i$ is a surjective homomorphism with kernel
$$\operatorname{Ker}(\pi_i) = \{(g_1, \dots, g_{i-1}, 1, g_{i+1}, \dots, g_n) \mid g_j \in G_j, j \neq i\}.$$
This kernel is also isomorphic to $G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n$.
3. If $x \in G_i$, $y \in G_j$ for $i \neq j$, then $xy = yx$; here, we're viewing x and y as
$$x = (1, \dots, 1, g_i, 1, 1, \dots, 1)$$
$$y = (1, \dots, 1, 1, g_{i+1}, 1, \dots, 1)$$

Proof. 1. By the subgroup criterion, $H = \{(1, \dots, 1, g_i, 1, \dots, 1) \mid g_i \in G_i\}$ is a subgroup of G. In particular, H is nonempty, and for any $x, y \in H$, we have
$$\begin{aligned} xy^{-1} &= (1, \dots, 1, x, 1, \dots, 1) * (1, \dots, 1, y^{-1}, 1, \dots, 1) \\ &= (1, \dots, 1, xy^{-1}, 1, \dots, 1) \in H \end{aligned}$$
Let $\psi : G_i \to H$ be the map sending $g_i \mapsto (1, \dots, 1, g_i, 1, \dots, 1)$. This is an isomorphism of G_i and H (the verification is straightforward), so we can identify G_i with H.

For the rest of the statement, consider the homomorphism
$$\begin{aligned} \varphi : G &\to G_1 \times G_2 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n \\ (g_1, \dots, g_n) &\mapsto (g_1, \dots, g_{i-1}, g_{i+1}, \dots, g_n) \end{aligned}$$

(i.e. delete g_i from the tuple). It is straightforward to check that φ is a homomorphism, and it is surjective. Further, the kernel is

$$\text{Ker}(\varphi) = \{(g_1, \dots, g_n) \mid g_i = 1, j \neq i\} = G_i.$$

By the first isomorphism theorem, $G_i \trianglelefteq G$, since it is the kernel of the homomorphism, and further

$$G/\underbrace{G_i}_{\text{Ker}(\varphi)} \cong \underbrace{G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n}_{\text{Im}(\varphi)}.$$

□

Example 26.6

For example, let $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ for prime p. Then, G has exactly $p+1$ subgroups of order p.

Proof. Every non-identity element in G has order p, and each generates a cyclic subgroup of order p.

By Lagrange's theorem, distinct subgroups of order p intersect trivially. Specifically, the intersection of two subgroups is a subgroup, which must divide p; since the subgroups are distinct, their intersection must then have order 1 (and thus are trivial).

This means that the $p^2 - 1$ non-identity elements are partitioned into subsets of size $p-1$ (i.e. excluding the identity), so there must be $\frac{p^2-1}{p-1} = p+1$ subgroups of order p. □

26.1 Fundamental Theorem of Finitely generated Abelian Groups

Definition 26.7: Finitely Generated Group

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 (ex. by $A = \{a_1, \dots, a_n\}$) and G is abelian, then every element x can be written as

$$x = a_1^{\lambda_1} \times \cdots \times a_n^{\lambda_n},$$

for $\lambda_i \in \mathbb{Z}$.

Definition 26.8: Free Abelian Group

If G is finitely generated by $A = \{a_1, \dots, a_n\}$, and all the a_i are of infinite order, then G is a *free abelian group* of rank n.

Example 26.9

For example, consider $\mathbb{Z}^r = \mathbb{Z} \times \cdots \times \mathbb{Z}$, the direct product of r copies of $\mathbb{Z}$.

$\mathbb{Z}^r$ is a free abelian group of rank r, since it is generated by $\{(1,0,\dots),(0,1,\dots),\dots,(0,\dots,0,1)\}$, where each element has infinite order.

Definition 26.10: Torsion

An element $x \in G$ is called *torsion* if it is of finite order.

We denote the subgroup of torsion elements by $T_G \subset G$, and we call it the *torsion subgroup*.

Definition 26.11: Torsion Free Group

If $T_G = \{e\}$ for e the identity, then G is called *torsion free*.

Definition 26.12: Torsion Group

If $T_G = G$, then G is a *torsion group*.

Theorem 26.13: Fundamental Theorem of Finitely Generated Abelian Groups

Let G be a finitely generated abelian group. Then,

1. We have
$$G \cong \mathbb{Z}^r \times \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_s\mathbb{Z},$$
such that $r, n_i \in \mathbb{Z}$, $r \geq 0$, each $n_i \geq 2$, and $n_{i+1} \mid n_i$ for all $1 \leq i \leq s-1$.
2. The above expression is unique.

Here, r is called the rank of G, and n_i are called the invariant factors of G.

Because the expression is unique, two finitely generated abelian groups are isomorphic if and only if they have the same rank and list of invariant factors.

Further, a finitely generated group is finite if and only if its rank is 0. This gives an effective way of listing all finite abelian groups of a given order.

To list these groups, we need to enumerate $n_1, \ldots, n_s$ such that

1. $n_j \geq 2$ for all $j \in \{1, \ldots, s\}$
2. $n_{i+1} \mid n_i$ for all $i \in \{1, \ldots, s-1\}$
3. $n_1 \cdots n_s = n$

Note that n_1 is the largest of the invariant factors. Since each $n_i \mid n$, then if $p \mid n$, then $p \mid n_i$ for some i (since the product of n_i's is equal to n). This then implies that $p \mid n_j$ for all $j \leq i$, so every prime factor of n divides n_1.

In particular, if n is the product of distinct primes, then $n = n_1$. This leads us to the following corollary.

Corollary 26.14

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

Example 26.15

Suppose $n = 180 = 2^2 \cdot 3^2 \cdot 5$. Here are the possible n_1 values:

$$n_1 = 2^2 \cdot 3^2 \cdot 5 = 180$$
$$n_1 = 2 \cdot 3^2 \cdot 5 = 90$$

$$n_1 = 2^2 \cdot 3 \cdot 5 = 60$$
$$n_1 = 2 \cdot 3 \cdot 5 = 30$$

For each one of these possible values, we need to determine the possible $n_2, n_3, \ldots$:

- If $n_1 = 2^2 \cdot 3^2 \cdot 5$, then $G \cong \mathbb{Z}/180\mathbb{Z}$, and we're done.
- If $n_1 = 2 \cdot 3^2 \cdot 5$, then $n_2 = 2$ and $G \cong \mathbb{Z}/90\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
- If $n_1 = 2^2 \cdot 3 \cdot 5$, then $n_2 = 3$ and $G \cong \mathbb{Z}/60\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.
- If $n_1 = 2 \cdot 3 \cdot 5$, then $n_2 = 2 \cdot 3$ and $G \cong \mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

  Note that n_2 can't be 2 or 3, because then $n_3 \nmid n_2$.

This means that the classification of abelian groups of order 180 is:

Invariant factors	Groups	Largest order
(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 to list out the possible classifications is through "elementary divisors".

Theorem 26.16

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

1. $G \cong A_1 \times \cdots \times A_k$ for $|A_i| = p_i^{\alpha_i}$
2. For every $A \in \{A_1, \ldots, A_k\}$,
$$A \cong \mathbb{Z}/p^{\beta}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{\beta_t}\mathbb{Z},$$
for $\beta_1 \geq \beta_2 \geq \cdots \geq \beta_t \geq 1$ and $\beta_1 + \cdots + \beta_t = \alpha$.

This decomposition is unique.

Example 26.17

For the same case of $|G| = 180 = 2^2 \cdot 3^2 \cdot 5$, we must have $G \cong A_1 \times A_2 \times A_3$, where $|A_1| = 2^2$, $|A_2| = 3^2$, and $|A_3| = 5$.

Here, $A_1 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, or $\mathbb{Z}/4\mathbb{Z}$. Similarly, $A_2 \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, or $\mathbb{Z}/9\mathbb{Z}$. Lastly, we must have $A_3 \cong \mathbb{Z}/5\mathbb{Z}$.

So, together, we have one of the following:

$$G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$$
$$G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$$
$$G \equiv \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$$
$$G \equiv \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$$

Here, we can make use of the following proposition:

Proposition 26.18

If $m, n \in \mathbb{Z}$, where $m, n > 0$, then $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/mn\mathbb{Z}$ if and only if $\gcd(m, n) = 1$.

This means that we can combine the direct products to create the invariant factors:

$$\begin{aligned} G &\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \\ &\cong \mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \\ G &\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \\ &\cong \mathbb{Z}/90\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \\ G &\cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \\ &\cong \mathbb{Z}/60\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \\ G &\cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \\ &\cong \mathbb{Z}/180\mathbb{Z} \end{aligned}$$

10/31/2022

Lecture 27

Subrings, Zero Divisors, Units

Definition 27.1: Zero divisor

Let R be a ring. A nonzero element a of R is called a *0-divisor* if there is a nonzero element $b \in R$ such that $ab = 0$ or $ba = 0$.

Definition 27.2: Unit

Let R be a ring. A nonzero element u of R is called a *unit* in R if there is some $v \in R$ such that $uv = vu = 1$.

The set of units is denoted $R^\times$.

As a remark, for a ring R, $R^\times$ forms a group under multiplication, which we call the group of units of R.

We can reframe the definition of a field to say that it is a commutative ring F with $1 \neq 0$ in which every nonzero element is a unit. That is, $F^\times = F \setminus \{0\}$.

Lemma 27.3

A zero divisor cannot be a unit.

Proof. Suppose for contradiction that we have a zero divisor that is also a unit. That is, we have an $a \in R$ such that $a \in R^\times$ and there exists a nonzero $b \in R$ such that $ab = 0$.

Since $a \in R^\times$, we have $va = 1$ for some $v \in R$; this means that

$$v(ab) = (va)b = 1b = b,$$

so $v(ab) = v(0) = 0 = b$. This is a contradiction, so such an a cannot exist; a zero divisor cannot be a unit. □

Example 27.4

Here are some examples of rings and their zero divisors and units:

- In $\mathbb{Z}$, there are no 0-divisors, and the only units are ± 1. This means that $\mathbb{Z}^\times = \{-1, 1\}$.

- In $\mathbb{Z}/n\mathbb{Z}$, every nonzero element is either a 0-divisor or a unit.

  In particular, if $[a] \in \mathbb{Z}/n\mathbb{Z}$ such that $\gcd(a,n) = 1$, then $[a]$ is a unit. Otherwise, let $b = \frac{n}{\gcd(a,n)}$. We have $b < n$ since $\gcd(a,n) \neq 1$, so $[b] \neq [n] = [0]$. Then, $[a] \cdot [b] = [0]$, so $[a]$ is a zero divisor.

  Further, any nonzero element is a unit if and only if every integer $0 < a < n$ is relatively prime to n. Note that this is true if and only if n is prime. This means that $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is prime.

Definition 27.5: Integral Domain

A commutative ring where $1 \neq 0$ is called an *integral domain* if it has no zero divisors.

Proposition 27.6: Cancellation law

Let R be a ring without zero divisors, and let $a, b, c \in R$. If $ab = ac$, then either $a = 0$ or $b = c$.

Proof. If $ab = ac$, then $ab - ac = 0 \implies a(b-c) = 0$. Since R has no zero divisors, then $a = 0$ or $b - c = 0$, as desired. (Otherwise, if $a \neq 0$ and $b - c \neq 0$, then we've found two nonzero elements that multiply to zero, and thus have found a zero divisor.) □

Corollary 27.7

Any finite integral domain is a field.

Proof. Let $a \neq 0 \in R$. The map $x \mapsto ax$ from $R \to R$ is injective, because $ax_1 = ax_2 \implies x_1 = x_2$ by the cancellation law (we have $ax_1 - ax_2 = 0$, and since $a \neq 0$, we must have $x_1 = x_2$).

Since R is finite, and this is an injective map from R to itself, the map must also be surjective. However, this means that there must exist some $b \in R$ such that $ab = 1$; a is a unit in R.

Since a was an arbitrary nonzero element, every nonzero element is a unit in R, so R is a field. □

Definition 27.8: Subring

A *subring* of a ring R is an additive subgroup of R that is closed under multiplication and contains the multiplicative identity of R.

Note that it is sufficient to show that a subset of R is nonempty, closed under subtraction and multiplication, and has the multiplicative identity.

Example 27.9

We have the following examples of subrings:

- $\mathbb{Z} \subseteq_{subring} \mathbb{Q} \subseteq_{subring} \mathbb{R}$.
- If R is a subring of a field F then R is an integral domain.

  Proof. R is already a ring, and it is also commutative, since $a, b \in R \subseteq F$, so $ab = ba$. We only need to show that there are no zero divisors.

  Suppose $0 \neq a \in R \subseteq F$. Note that if a is a zero divisor, there must exist some nonzero $b \in R$ such that $ab = 0$ in R. However, looking at the same equation in F, since $a \neq 0$, then $a \in F^\times$, so it must be the

case that $b = 0$ (otherwise, we have a nonzero b such that $ab \neq 1$, contradicting the fact that $a \in F^\times$).

This is a contradiction, a being a zero divisor necessitates a corresponding nonzero b such that $ab = 0$; this means that a must not be a zero divisor, and there are no zero divisors in R. □

11/2/2022

Lecture 28

Polynomial Rings—Introduction

We'll be talking about polynomial rings later on in the semester, but it's a useful source of examples, so we'll talk about it a little bit now.

Definition 28.1: Polynomial Ring

Let R be a commutative ring with $1 \neq 0$. Then, $R[x]$ ("R adjoin x") is the set of polynomials with coefficients in R.

Here, we have

$$R[x] = \{a_0 + a_1 x + \cdots + a_n x^n \mid a_i \in R\}.$$

Conventionally, for a polynomial $f(x) = a_0 + a_1 x + \cdots + a_n x^n$, if n is the largest integer such that $a_n \neq 0$, then the degree of f is n. If $a_n = 1$, then f is *monic*.

The operations in $R[x]$ are as follows:

- Addition:

$$(a_0 + a_1 x + \cdots + a_n x^n) + (b_0 + b_1 x + \cdots + b_n x^n) = (a_0 + b_0) = (a_1 + b_1)x + \cdots + (a_n + b_n)x^n.$$

- Multiplication:

$$(a_0 + a_1 x + \cdots + a_n x^n) \cdot (b_0 + b_1 x + \cdots + b_n x^n) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^n + \cdots + (a_n b_n)x^{2n}.$$

  Here, the coefficient of x^k is $\sum_{i=0}^{k} a_i b_{k-1}$.

These operations make $R[x]$ into a ring. Further, R is a subring of $R[x]$.

Example 28.2

This gives more examples of subrings:

$$\mathbb{Z}[x] \subseteq_{subring} \mathbb{Q}[x] \subseteq_{subring} \mathbb{R}[x].$$

Example 28.3

Consider the ring $\mathbb{Z}/3\mathbb{Z}[x]$. Here, this is the ring of polynomials with coefficients in $\mathbb{Z}/3\mathbb{Z}$, i.e. $a_i \in \{0, 1, 2\}$.

For example, let $p(x) = x^2 + 2x + 1$, and $q(x) = x^3 + x + 2$.

We have

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

We also have

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

$$= x^5 + 2x^4 + x^3 + x^3 + 2x^2 + x + 2x^2 + 4x + 2$$
$$= x^5 + 2x^4 + 2x^3 + 4x^2 + 5x + 2$$
$$= x^5 + 2x^4 + 2x^3 + x^2 + 2x + 2$$

As a remark, the coefficient ring makes a difference on the behavior of the resulting polynomials. We'll be more precise latter, but the polynomial x^2+1 in $\mathbb{Z}[x]$ cannot be factored (i.e. it is "irreducible"), whereas the same polynomial in $\mathbb{C}[x]$ can be factored as $x^2+1=(x+i)(x-i)$, and the same polynomial in $\mathbb{Z}/2\mathbb{Z}[x]$ can be factored as $x^2+1=(x+1)^2$.

The properties of R also affect $R[x]$; the polynomial ring inherits some properties from R.

Proposition 28.4

Let R be an integral domain, and let $p(x)$, $q(x)$ be nonzero elements of $R[x]$. Then, the following hold:

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. Let $p(x) = a_n x^n + \cdots + a_0$, and $q(x) = b_m x^m + \cdots + b_0$, for $a_n, b_m \neq 0$. Here, $\deg(p(x)) = n$ and $\deg(q(x)) = m$.

The product $p(x)q(x) = a_n b_m x^{n+m} + \cdots + a_0 b_0$. Because $a_n, b_m \neq 0$, then $a_n b_m \neq 0$ either. Further, we know that x^{m+n} is the largest power of x in the product, so

$$\deg(p(x)q(x)) = n + m = \deg(p(x)) + \deg(q(x)).$$

2. We will show containments in both directions.

If $p(x)$ is a unit of $R[x]$, then there exists a $q(x)$ such that $p(x)q(x) = 1$. We know that $\deg(1) = 0$, so by part (1), we know that $\deg(p(x)) + \deg(q(x)) = \deg(1) = 0$. This means that $\deg(p(x)) = \deg(q(x)) = 0$, since the degree must be nonnegative.

Further, this means that $p(x)$ and $q(x)$ are constants and $p(x)q(x) = 1$. This means that $p(x)$ and $q(x)$ are units of R; that is, $(R[x])^\times \subseteq R^\times$.

In the other direction, if $a, b \in R^\times$, then $ab = 1$, and $ab = 1$ in $R[x]$ as well. This means $a, b \in (R[x])^\times$; that is, $R^\times \subseteq (R[x])^\times$.

Together, $(R[x])^\times = R^\times$.

3. If $p(x) \neq 0$ and $q(x) \neq 0$, then $p(x)q(x) \neq 0$; since p and q are arbitrary, this means that $R[x]$ has no zero divisors, and thus is an integral ring.

□

As a remark, if R has zero divisors, then so does $R[x]$, notably because $R \subseteq R[x]$. Further, if S is a subring of R, then $S[x]$ is a subring of $R[x]$.

11/9/2022

Lecture 29

Ring Homomorphisms, Quotient Rings

So far, we've talked about rings and subrings; today, we'll talk about ring homomorphisms and quotient rings.

29.1 Ring Homomorphisms

Definition 29.1: Ring Homomorphism

Let R and S be rings. A *ring homomorphism* is a map $\varphi : R \to S$ satisfying the following:

1. $\varphi(a+b) = \varphi(a) + \varphi(b)$
2. $\varphi(ab) = \varphi(a)\varphi(b)$

Definition 29.2: Kernel of Ring Homomorphisms

The kernel of φ is

$$\text{Ker}(\varphi) = \{r \in R \mid \varphi(r) = 0\}.$$

That is, the kernel of φ is the set of elements in R that map to the additive identity; it's the kernel of φ as an additive group homomorphism.

Definition 29.3: Ring Isomorphism

A bijective ring homomorphism is a *ring isomorphism*.

Example 29.4

Consider $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ mapping $a \mapsto [a]$.

We know that

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

This means that π is a ring homomorphism.

We have $\text{Ker}(\pi) = \{x \in \mathbb{Z} \mid \pi(x) = [0]\}$; the only x that gets sent to zero are multiples of n, i.e. for all in $x \in n\mathbb{Z}$.

Note that the kernel here is not a subring, because $n\mathbb{Z}$ does not have the multiplicative identity.

Note that in general $\text{Ker}(\varphi)$ is an additive subgroup of R (not necessarily a subring, as the previous example shows).

Example 29.5

Consider $\varphi : \mathbb{Q}[x] \to \mathbb{Q}$ such that $p(x) \mapsto p(0)$, i.e. we map p to its constant term.

We can check whether φ is a homomorphism:

- $\varphi(p(x) + q(x)) = p(0) + q(0) = \varphi(p(x)) + \varphi(q(0))$
- $\varphi(p(x)q(x)) = p(0)q(0) = \varphi(p(x))\varphi(q(x))$

Here, the kernel is the set of all polynomials with a constant term of 0.

Example 29.6

Let $n \in \mathbb{Z}$, and define $M_n : \mathbb{Z} \to \mathbb{Z}$ where $x \mapsto nx$.

We can check whether φ is a homomorphism:

- $M_n(x+y) = n(x+y) = nx + ny = M_n(x) + M_n(y)$
- $M_n(xy) = n(xy) = nxy \neq n^2xy = nxny = M_n(x)M_n(y)$

Since $M_n(xy) \neq M_n(x)M_n(y)$, in general this is not a ring homomorphism.

Note that M_n is only a homomorphism if $n = 0$ or $n = 1$; if $n = 0$, this is the trivial homomorphism, and if $n = 1$, this is the identity homomorphism.

Proposition 29.7

If $\alpha \in \text{Ker}(\varphi)$, then $r\alpha$ and αr are in $\text{Ker}(\varphi)$ for all $r \in R$.

Proof. Suppose $r \in R$, and let $\alpha \in \text{Ker}(\varphi)$. We have

$$\varphi(r\alpha) = \varphi(r)\varphi(\alpha) = \varphi(r) \cdot 0 = 0.$$

This means $r\alpha \in \text{Ker}(\varphi)$. We also have

$$\varphi(\alpha r) = \varphi(\alpha)\varphi(r) = 0 \cdot \varphi(r) = 0.$$

This means $\alpha r \in \text{Ker}(\varphi)$ as well. □

29.2 Quotient Rings

Quotient rings are defined similarly to quotient groups.

Let R and S be rings, and consider the surjective homomorphism $\varphi : R \to S$, where $\text{Ker}(\varphi) = I$.

Since I is an additive subgroup of R, the first isomorphism theorem tells us that $R/I \cong S$, with $r + I$ mapping to $\varphi(r)$.

We want R/I to be a ring as well, i.e. we want $\varphi(r_1) + \varphi(r_2) = \varphi(r_1 + r_2)$; this means we want

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

This is how we'll define addition on cosets of I.

Similarly, we want $\varphi(r_1)\varphi(r_2) = \varphi(r_1 r_2)$.

$$(r_1 + I) \cdot (r_2 + I) = (r_1 r_2) + I.$$

This is how we'll define multiplication on cosets of I.

Definition 29.8: Operations on Cosets of an Ideal

Let R and S be rings, and consider the surjective homomorphism $\varphi : R \to S$, where $\text{Ker}(\varphi) = I$.

If the following hold:

$$(r + I) + (s + I) = (r + s) + I$$
$$(r + I) \cdot (s + I) = (rs) + I$$

Then R/I is a ring, because S is a ring.

Similar to how kernels are normal subgroups, the kernel properties then motivate the following definition of *ideals*.

Definition 29.9: Ideal

Let R be a ring. $I \subseteq R$ is called an *ideal of* R if

- $(I,+) \leq (R,+)$
- For all $r \in R, i \in I$, $ri \in I$ and $ir \in I$.

Corollary 29.10

A subset $I \subseteq R$ is an ideal if and only if it is the kernel of some ring homomorphism.

11/14/2022

Lecture 30

Properties of Ideals

Similar to groups, we have

Theorem 30.1: First Isomorphism Theorem (Rings)

If $\varphi : R \to S$ is a ring homomorphism, then

$$R/\operatorname{Ker}(\varphi) \cong \operatorname{Im}(\varphi).$$

Example 30.2

We saw that $n\mathbb{Z}$ was an ideal of $\mathbb{Z}$; this is the kernel of the ring homomorphism $\varphi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, mapping $x \to [x]$.

Example 30.3

Another example is with $R = \mathbb{Z}[x]$; let $I := \{\sum_{i=1}^{n} a_i x^i \mid a_0 = a_1 = 0\}$ (i.e. I contains polynomials whose terms are of at least degree 2). We claim that I is an ideal in R.

We know that $(I,+) \leq (R,+)$, because the sum of 2 polynomials with all terms of at least degree 2 will again have terms of at least degree 2. It also has the identity $a_0 = 0$, and for the inverse we can take the negative (i.e. $g^{-1} := -g$).

Now, given $f(x) \in \mathbb{Z}[x]$, we have $f(x) \cdot I \subseteq I$ and $I \cdot f(x) \subseteq I$, since the degrees are additive when you multiply.

Two polynomials $p(x)$, $q(x)$ are in the same coset of I if and only if they differ by a polynomial with $a_0 = a_1 = 0$; this is because

$$\begin{aligned} p(x) + I = q(x) + I &\iff p(x) - q(x) \in I \\ &\iff p(x) - q(x) \text{ has } a_0 = a_1 = 0 \end{aligned}$$

The complete set of representatives of R/I is given by polynomials $ax + b$, where $\{(ax+b) + I\} = \overline{ax+b}$; the cosets are uniquely defined by the terms of degree 0 and 1.

Note that in R/I (i.e. $\mathbb{Z}[x]/I$), we have $\bar{x} \cdot \bar{x} = \bar{x}^2 = 0$, because $\bar{x}^2 \in I$. This means that R/I has zero divisors, even if $R = \mathbb{Z}[x]$ does not.

30.1 Properties of Ideals

Definition 30.4: Sum of Ideals

Let I and J be ideals of R. The sum of I and J is

$$I + J = \{a + b \mid a \in I, b \in J\}.$$

Definition 30.5: Product of Ideals

Let I and J be ideals of R. The product of I and J is the set of all finite sums of elements of the form ab with $a \in I$ and $b \in J$. That is,

$$IJ = \left\{ \sum_{i=1}^{n} a_i b_i \,\middle|\, a_i \in I, b_i \in J, n \geq 1 \right\}.$$

Definition 30.6: Power of an ideal

Let I be an ideal of R. For $n \geq 1$, the nth power of I, denoted I^n, is the set consisting of all finite sums of elements of the form $a_1 \cdots a_n$ with $a_i \in I$ for all i. That is,

$$I^n = \left\{ \sum_{i=1}^{k} a_{i_1} \cdots a_{i_n} \,\middle|\, a_{i_j \in I} \right\}.$$

As a remark, $I + J$ and IJ are also ideals. In fact, $I + J$ is the smallest ideal containing both I and J, and $IJ \subseteq I \cap J$.

Also note that $\{ab \mid a \in I, b \in J\}$ is not necessarily closed under addition, so this is in general not an ideal—this is why we define the product of ideals as above.

Example 30.7

In $\mathbb{Z}$, let $I = 6\mathbb{Z}$ and $J = 10\mathbb{Z}$. Then,

$$I + J = \{6x + 10y \mid x, y \in \mathbb{Z}\}.$$

Note that every integer in $I + J$ is divisible by $\gcd(6, 10) = 2$, which means that $I + J \subseteq 2\mathbb{Z}$.

In addition, $2 = 6 \cdot (2) + 10 \cdot (-1)$, so $2 \in I + j$, which means that every multiple of 2 is in $I + J$. This means $2\mathbb{Z} \subseteq I + J$ as well.

Together, since $I + J \subseteq 2\mathbb{Z}$ and $2\mathbb{Z} \subseteq I + J$, we know that $2\mathbb{Z} = 6\mathbb{Z} + 10\mathbb{Z}$.

As a remark, this is true in general:

$$m\mathbb{Z} + n\mathbb{Z} = \gcd(m, n)\mathbb{Z}.$$

Example 30.8

With the same $I = 6\mathbb{Z}$ and $J = 10\mathbb{Z}$, the product IJ is the set of all finite sums of elements of $6x \cdot 10y = 60xy$. This means that $IJ = 60\mathbb{Z}$.

11/16/2022

Lecture 31

Properties of Ideals (cont.)

Example 31.1

Following up from last time's example of IJ for $I = 6\mathbb{Z}$ and $J = 10\mathbb{Z}$, here is an example of a product of ideals that is not simply the product of elements from I and J.

Suppose we take I as the set of polynomials with an even constant term, in the polynomial ring $\mathbb{Z}[x]$.

We can see that $2 \in I$ and $x \in I$, and since $4 = 2 \cdot 2$ and $x^2 = x \cdot x$, $x^2 + 4 \in I \cdot I$.

However, we can't write $x^2 + 4$ as a single product of two elements in I.

Now, let R be a commutative ring.

Definition 31.2: Ideal generated by a set

Let $A \subseteq R$ be a subset of R, a commutative ring. We define (A) to be the ideal generated by A.

This is also the smallest ideal of R containing A, and can be expressed as

$$(A) = \bigcap_{\substack{\text{ideals} \\ I \supseteq A}} I.$$

Definition 31.3: Principal ideal

An ideal generated by a single element is called a *principal ideal*.

Definition 31.4: Finitely generated ideal

An ideal generated by a finite set is called *finitely generated*.

For notation, when $A = \{a\}$, we'll write (a) for the ideal generated by $\{a\}$, and when $A = \{a_1, \dots, a_n\}$, we'll write $(a_1, a_2, \dots, a_n)$.

As a remark, another (perhaps more intuitive) way to interpret (A) is as

$$(A) = \{r_1 a_1 + \cdots r_n a_n \mid r_i \in R, a_i \in A, n \in \mathbb{Z}^+\}.$$

That is, (A) is the set of all finite sums of elements ra with $r \in R$ and $a \in A$.

Example 31.5

The trivial ideal is $0 = (0)$, and for an ideal R, we also have $R = (1)$. Both of these are principal ideals.

Example 31.6

In $\mathbb{Z}$, $n\mathbb{Z}$ can be expressed as (n) and every ideal of $\mathbb{Z}$ is of this form. This means that every ideal of $\mathbb{Z}$ is principal.

In particular, $(m,n) = (\gcd(m,n))$; this is because

$$(m,n) = \{r_1 m + r_2 n \mid r_1, r_2 \in \mathbb{Z}\}$$

Letting $d = \gcd(m,n)$ and rewriting in terms of $m' = \frac{m}{d}$ and $n' = \frac{n}{d}$, we have

$$\begin{aligned} &= \{r_1 m' d + r_2 n' d \mid r_1, r_2 \in \mathbb{Z}\} \\ &= \{(r_1 m' + r_2 n')d \mid r_1, r_2 \in \mathbb{Z}\} \\ &= \{rd \mid r \in \mathbb{Z}\} \\ &= (d) = (\gcd(m,n)) \end{aligned}$$

Here we use the fact that $r_1 m' + r_2 n' \in \mathbb{Z}$ since $\mathbb{Z}$ is a ring.

Further, if $m, n \in \mathbb{Z}$, then $n\mathbb{Z} \subseteq m\mathbb{Z} \iff m \mid n$.

Example 31.7

In $\mathbb{Z}[x]$, the ideal $(2,x)$ is not principal. To see why, first we can express

$$(2,x) = \{2p(x) + xq(x) \mid p(x), q(x) \in \mathbb{Z}[x]\}.$$

Note that $(2,x) \neq \mathbb{Z}[x]$, since $1 \notin (2,x)$; this means that it is not the entire ring $\mathbb{Z}[x]$.

Now suppose for contradiction that $(2,x) = (a(x))$ for some polynomial $a(x) \in \mathbb{Z}[x]$.

Since $2 \in (a(x))$ by assumption, there must exist a $p(x)$ such that $2 = a(x)p(x)$, which means that $a(x)$ and $p(x)$ must have degree 0. Since 2 is prime, this means that $a(x), p(x) \in \{\pm 1, \pm 2\}$.

If $a(x) = \pm 1$, then $(a(x)) = \mathbb{Z}[x]$; however, $1 \notin (2,x)$ so this cannot be the case. This means that $a(x) = \pm 2$.

However, we also know that $x \in (a(x))$ by assumption, so there must exist a $q(x)$ such that $x = 2 \cdot q(x)$. However, $q(x)$ has integer coefficients, so this is impossible—we can't have $2q(x)$ have a coefficient of 1 for the x term.

This means that $(2,x) \neq (a(x))$ for any $a(x) \in \mathbb{Z}$, so $(2,x)$ is not principal.

Proposition 31.8

Let I be an ideal of R.

1. $I = R$ if and only if I contains a unit
2. If R is commutative, then R is a field if and only if its only ideals are (0) and R.

Proof.

1. In the forward direction, suppose $I = R$. This means that I contains 1, which is a unit.

   In the opposite direction, suppose $u \in I$ is a unit.This means that there is some inverse $v \in R$ such that $uv = 1$. This means that
   $$r = r \cdot 1 = r(vu) = (rv)u \in I,$$
   since $rv \in R$ and $u \in I$, so $(rv)u \in I$. In particular, this means that any $r \in R \implies r \in I$, so $R = I$ (since we already know $I \subseteq R$).

2. In the forward direction, suppose R is a field. This means that every nonzero element is a unit, so this follows from the previous claim—every nontrivial ideal I of R must contain a unit, and thus $I = R$. This means the only two possible ideals of R are (0) and R.

In the opposite direction, suppose (0) and R are the only ideals. Let $u \in R$ be nonzero. Since $(u) = R$ (as it is not trivial), we must have $1 \in (u)$, so there exists a v such that $1 = uv$. This means that u is a unit.

Since we chose an arbitrary nonzero u, this shows that all nonzero elements in R are units, so R must be a field.

□

Corollary 31.9

If R is a field, then any nonzero ring homomorphism from R into another ring is an injection.

Proof. We know that $\ker(\varphi)$ is an ideal of R; since R is a field, this means that $\ker(\varphi) = 0$ or $\ker(\varphi) = R$. We've assumed that φ is not the zero homomorphism, so $\ker(\varphi) \neq R$, and thus $\ker(\varphi) = 0$. This means that φ must be an injection. □

11/18/2022

Lecture 32

Maximal Ideals, Prime Ideals

An important class of ideals are ideals that are not contained in any other proper ideal.

Definition 32.1: Maximal Ideal

An ideal M of R is *maximal* if $M \neq R$ and the only ideals containing M are M and R.

The existence of maximal ideals follows from *Zorn's lemma*.

Lemma 32.2: Zorn's lemma

Let $(A, \leq)$ be a partially ordered set. If every chain $x_1 \leq x_2 \leq \cdots$ has an upper bound in A, then A has a maximal element.

Note that this is equivalent to the axiom of choice.

Proposition 32.3

Let R be a ring. Every ideal $I \neq R$ is contained in a maximal ideal of R.

Proof. Let I be an ideal of R not equal to R. We define

$$S = \{K \mid K \text{ is an ideal and } I \subseteq K \subset R\},$$

and let S be ordered by inclusion. Consider a chain C: $J_1 \subseteq J_2 \subseteq \cdots$ in S.

Let $J = \bigcup_i J_i$. We can see that J is an ideal of R (in HW), and this union must also contain I. Further, $J \neq R$, because otherwise we'd have a unit in J, so there must have been a unit in some J_i, which makes this $J_i = R$, which contradicts our definition of S.

This means that J is an upper bound of this chain, so by Zorn's lemma, there exists a $M \in S$ that is maximal. □

.

From now on, let R be a commutative ring.

Proposition 32.4

Let R be a commutative ring. M is a maximal ideal of R if and only if R/M is a field.

Proof. If M is maximal, then there are no ideals containing it other than M and R.

This means that all ideals of R containing M correspond to ideals of R/M (by the correspondence isomorphism theorem). Since M is maximal, this means that the only ideals of R/M are R/M and $M/M = 0$. As such, R/M is a field.

The same argument can be applied in reverse for the other direction. □

Example 32.5

Here are some examples of maximal ideals.

- $n\mathbb{Z} \subset \mathbb{Z}$ is maximal if and only if $\mathbb{Z}/n\mathbb{Z}$ is a field. That is, $n\mathbb{Z}$ is maximal when n is prime.
- $(2, x)$ in $\mathbb{Z}[x]$ is maximal. We can check by taking $\mathbb{Z}[x] \to \mathbb{Z}/2\mathbb{Z}$, sending $p(x) \mapsto p(0) \bmod 2$.

  We can show that $\ker(\varphi) = (2, x)$, so by the first isomorphism theorem $\mathbb{Z}[x]/(2, x) \cong \mathbb{Z}/2\mathbb{Z}$. Since $\mathbb{Z}/2\mathbb{Z}$ is a field, $(2, x)$ is maximal.
- Similarly, (x) in $\mathbb{Z}[x]$ is not maximal. We can take $\varphi : \mathbb{Z}[x] \to \mathbb{Z}$ sending $p(x) \mapsto p(0)$, and we can similarly show that $\ker(\varphi) = (x)$. This means that $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$ Since $\mathbb{Z}$ is not a field, (x) is not maximal.

Definition 32.6: Prime Ideal

Suppose R is commutative. An ideal P is a *prime ideal* if $P \neq R$ and whenever the product $ab \in P$ for $a, b \in R$, then either $a \in P$ or $b \in P$.

Example 32.7

In $\mathbb{Z}$, the prime ideals are $p\mathbb{Z}$ where p is prime, along with the zero ideal.

This is because any $x \in p\mathbb{Z}$ must have $p \mid x$, so if $x = ab$ for some $a, b \in \mathbb{Z}$, then we must have $p \mid a$ or $p \mid b$ (otherwise ab has no factors of p, a contradiction). This means that either $a \in p\mathbb{Z}$ or $b \in p\mathbb{Z}$.

Proposition 32.8

Let R be a commutative ring. P is a prime ideal if and only if R/P is an integral domain.

Proof. If P is a prime ideal, then $P \neq R$ and $ab \in P$ implies that $a \in P$ or $b \in P$.

Consider R/P. Here, let $\overline{a} := a + P$. We have that $a \in P \iff \overline{a} = 0$; this is because if $a \in P$, then $\overline{a} = a + P = P = 0 + P = \overline{0}$.

Since P is a prime ideal, we know that $\overline{R} \neq \overline{0}$, since $P \neq R$, and whenever $\overline{a}\overline{b} = \overline{0}$, we must have $\overline{a} = 0$ or $\overline{b} = 0$, which is the definition of an integral domain.

The same logic in reverse can show the opposite direction. □

Corollary 32.9

Every maximal ideal is prime.

Proof. Since every field is an integral domain, all maximal ideals M has R/M as a field, which is an integral domain, making M a prime ideal. □

Example 32.10

(x) is a prime ideal of $\mathbb{Z}[x]$. With the same reasoning as before, we can see that $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$, which is an integral domain.

11/21/2022

Lecture 33

Euclidean Domains, PIDS, UFDs

33.1 Euclidean Domains

The motivational question for Euclidean domains is: which rings have the division algorithm?

Firstly, we need to define a notion of "size" in a ring.

Definition 33.1: Norm

Let R be an integral domain.

Any function $N: R \to \mathbb{Z}^+ \cup \{0\}$ with $N(0) = 0$ is called a *norm*.

Definition 33.2: Euclidean Domain

An integral domain R is a *Euclidean domain* if there exists a norm N on R such that for any two $a, b \in R$ with $b \neq 0$, there exists $q, r \in R$ with $a = qb + r$ and $r = 0$ or $N(r) < N(b)$.

Euclidean domains are integral domains where you can do the division algorithm (and thus we can do the Euclidean algorithm).

Example 33.3

Here are some examples of Euclidean domains:

- Fields are Euclidean domains.

  In particular, for any $a, b \neq 0$ in F, we will always have $a = qb + 0$, since we can take $q = ab^{-1}$, and define $N(a) = 0$ for all $a \in F$.

  Here we don't actually need to do the division algorithm, since we can always take the inverse.

- $\mathbb{Z}$ is a Euclidean domain with norm given by $N(a) = |a|$, just like how we defined the division algorithm at the beginning of the class.

- If F is a field, then $F[x]$ is a Euclidean domain with norm $N(p(x)) = \deg(p(x))$.

  Here, F must be a field, because we must be able to divide arbitrary coefficients.

Proposition 33.4

Every ideal in a Euclidean domain is principal.

Proof. If I is the zero ideal, then it is already principal, so there is nothing to show.

So, suppose $I \neq 0$. Let d be any nonzero element of I of minimal norm in I. (We know there will always be one, since norms can only take on nonnegative integer values.)

Since $d \in I$, then $(d) \subseteq I$, since (d) contains all multiples of d in I. It then suffices to show that $I \subseteq (d)$.

Let a be any element of I with $a = qd + r$, where $r = 0$ or $N(r) < N(d)$. This means that $r = a - qd$.

We know that $a, q, d \in I$, so $r \in I$ as well. However, we chose d to be a nonzero element of minimal norm in I, so r must be zero (otherwise we'd get a contradiction).

This means that $a = qd + 0 \in (d)$. Since a was arbitrary, this means that $I \subseteq (d)$.

Together, this means that $I = (d)$. □

Example 33.5

For $R = \mathbb{Z}[x]$, we saw that $(2, x)$ was not principal, so $R = \mathbb{Z}[x]$ is not a Euclidean domain.

Definition 33.6: Multiples, Divisors

Let R be a commutative ring, and let $a, b \in R$ where $b \neq 0$.

1. a is a *multiple* of b if there exists some $x \in R$ such that $a = xb$.

   Here, we say that $b \mid a$, i.e. b *divides* a.

2. A greatest common divisor of a and b is a nonzero element d such that
   - $d \mid a$ and $d \mid b$
   - If $d' \mid a$ and $d' \mid b$, then $d' \mid d$.

Note that $b \mid a$ if and only if $a \in (b)$, which is true if and only if $(a) \subseteq (b)$.

This means that if $d \mid b$ and $d \mid a$, then $(a, b) \subseteq (d)$. We can then rephrase the definition of a greatest common divisor with the following:

- $(a, b) \subseteq (d)$
- If $(a, b) \subseteq (d')$, then $(d) \subseteq (d')$.

33.2 Principal Ideal Domains

Definition 33.7: Principal Ideal Domain

A *principal ideal domain* (PID) is an integral domain in which every ideal is principal.

Corollary 33.8

Every Euclidean domain is a principal ideal domain.

Example 33.9

Since every field was a ED, then every field is a PID.

Similarly, for $\mathbb{Z}[x]$, since $(2, x)$ is not principal, then $\mathbb{Z}[x]$ is not a PID.

Recall that previously, we showed that every maximal ideal is prime, but not every prime ideal is maximal. PIDs give us a special case:

Proposition 33.10

Every nonzero prime ideal in a PID is maximal.

Proof. Let (p) be a nonzero prime ideal in a PID, and let (m) be such that $(p) \subseteq (m)$.

To show that (p) is maximal, we need to show that $(m) = (p)$, or $(m) = R$.

Since $p \in (m)$, there exists some $r \in R$ such that $p = rm$. Since p is prime, and we know $rm \in (p)$, it must be the case that either $r \in (p)$ or $m \in (p)$.

If $m \in (p)$, then $(m) \subseteq (p)$; since we assumed that $(p) \subseteq (m)$, this means that $(m) = (p)$ and we're done—any ideal containing (p) must be equal to (p).

If $r \in (p)$, then $r = ps$ for some $s \in R$. This means that

$$p = rm = psm \iff p - psm = 0 \iff p(1 - sm) = 0.$$

Since R is an integral domain and $p \neq 0$, this means that $1 - sm = 0 \implies 1 = sm \in (m)$, so $(m) = R$, and we're done. □

33.3 Unique Factorization Domains

The motivation for UFDs is the question: in which rings can we factor uniquely (i.e. similar to the fundamental theorem of arithmetic)?

Firstly, we need to define some terms.

Definition 33.11: Reducible/Irreducible Element

Let R be an integral domain, and let $r \in R$.

r is *irreducible* if it is nonzero, not a unit, and whenever $r = ab$ for $a, b \in R$, then at least one of a and b is a unit. Otherwise, r is *reducible*.

Here, it can be useful to think of irreducibility with polynomials (ex. in $\mathbb{Q}[x]$); it's defined similarly.

Definition 33.12: Prime Element

Let R be an integral domain, and let $p \in R$ be nonzero.

p is called *prime* if (p) is a prime ideal.

Definition 33.13: Associate Elements

Let R be an integral domain. Two elements a and b are called *associates* if $a = ub$ for some unit $u \in R^\times$.

Proposition 33.14

In an integral domain, if an element $p \neq 0$ is prime, then p is irreducible.

Proof. Suppose p is prime; this means that (p) is a prime ideal.

Suppose we can write $p = ab \in (p)$. Since (p) is a prime ideal, then either $a \in (p)$ or $b \in (p)$.

If $a \in (p)$, then there exists some $r \in R$ such that $a = pr$, which means that $p = ab = prb \implies p(1 - rb) = 0$. Since we are in an integral domain, this means that $1 = rb$, and thus b is a unit.

A similar logic applies if we assume $b \in (p)$; we have that a must be a unit.

This means that p must be irreducible; expressing $p = ab$ implies that at least one of a and b is a unit. □

Proposition 33.15

In a PID, a nonzero element is prime if and only if it is irreducible.

Proof. By Proposition 33.14, we know that a prime element must be irreducible. It then suffices to show that in a PID, an irreducible element must be prime.

Let p be an irreducible element in a PID R. If M is an ideal containing (p), then we have $M = (m)$; we're in a PID.

Since $p \in (m)$, then $p = mr$ for some $r \in R$. Further, since p is irreducible, then by definition at least one of r or m must be a unit.

If r is a unit, then $(p) = (m)$. If m is a unit, then $(m) = (1) = R$ if m is a unit.

This means that the only ideals containing (p) are (p) or $(1) = R$, so (p) is a maximal ideal, and since maximal ideals are prime ideals, this means that p is prime. □

With the idea of irreducible elements, we can now define a unique factorization domain.

Definition 33.16: Unique Factorization Domain

A *unique factorization domain* (UFD) is an integral domain R in which every nonzero element that is not a unit satisfies:

1. $r = p_1 \cdots p_n$ where $p_i \in R$ are irreducible
2. The decomposition is unique up to associates (i.e. if $r = q_1 q_2 \cdots q_m$ where q_i are irreducible, then $m = n$ and there is a reordering such that p_i and q_i are associates for all i.)

Example 33.17

Here are some examples of UFDs:

- Any field is a UFD. This is because every nonzero element is a unit, so both points are vacuously satisfied.
- $\mathbb{Z}$ is a UFD.

A non-example is $\mathbb{Z}[2i] = \{a + 2bi \mid a, b \in \mathbb{Z}\}$ for $i^2 = -1$.

This is an integral domain, but not a UFD. For example, we have $4 = 2 \cdot 2 = (-2i)(2i)$. Since $i \notin \mathbb{Z}[2i]$, as we always add multiples of $2i$, then we find that 2 and $2i$ are not associates, and 2 and $-2i$ are not associates

either.

Theorem 33.18

Every PID is a UFD

The proof of the above theorem is not in scope for this course.

Similar to PIDs, we have the following:

Proposition 33.19

In a UFD, a nonzero element is prime if and only if it is irreducible.

So far, we have the following hierarchy of rings:

$$\text{Fields} \subset \text{ED} \subset \text{PID} \subset \text{UFD} \subset \text{ID}.$$

All of these containments are strict as well:

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

A tabular summary is as follows:

Field	ED	PID	UFD	ID
only ideals are 0 and F	all ideals principal	all ideals principal		
no prime elements	$p \neq 0$ prime iff p irreducible	$p \neq 0$ prime iff p irreducible	$p \neq 0$ prime iff irreducible	$p \neq 0$ prime $\implies$ p irreducible
no prime elements	nonzero prime ideal is maximal	nonzero prime ideal is maximal		

Here, the gray text corresponds to an implied property from the parent set.

33.4 Polynomial Rings

Theorem 33.20

Let F be a field. The polynomial ring $F[x]$ is a Euclidean domain.

Specifically, if $a(x), b(x) \in F[x]$, for $b(x) \neq 0$, then there are unique $q(x)$ and $r(x)$ in $F[x]$ such that $a(x) = q(x)b(x) + r(x)$ with $r = 0$ or $\deg(r(x)) < \deg(b(x))$.

Corollary 33.21

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

Proof. This follows directly from the fact that Euclidean domains are PIDs, and PIDs are UFDs. □

Example 33.22

For example, $\mathbb{Q}[x]$ is a PID.

Recall that $(2, x)$ was not principal in $\mathbb{Z}[x]$, which made $\mathbb{Z}[x]$ not a PID. However, here, 2 is a unit in $\mathbb{Q}$, so $(2, x) = \mathbb{Q}[x]$.

Definition 33.23: Polynomial rings in multiple variables

The polynomial ring in variables $x_1, \dots, x_n$ with coefficients in R is denoted as $R[x_1, \dots, x_n]$. This is defined inductively with $R[x_1, \dots, x_n] = R[x_1, \dots, x_{n-1}][x_n]$.

The degree of a polynomial in $R[x_1, \dots, x_n]$ is the largest degree among its monomials.

Here, elements of $R[x_1, \dots, x_n]$ look like sums of $a x_1^{d_1} \cdots x_n^{d_n}$ for $a \in R$ and all $d_i \geq 0$ (these are monomials). The degree of each monomial is the sum $\sum_{i=1}^{n} d_i = d$.

Example 33.24

For example, in $\mathbb{Z}[x, y]$, we can have a polynomial $p(x, y) = 2x^3 + xy - y$, and the degree is $\deg(p(x, y)) = 3$, since $2x^3$ is the monomial with highest degree.

Similarly, we can also have $q(x, y) = 5x^4 + x^2 y^3 + x$, with degree $\deg(q(x, y)) = 5$.

11/28/2022

Lecture 34

Polynomial Rings

Continuing on from last time, we'll talk more about polynomial rings and their properties.

Example 34.1

From last time, we know $\mathbb{Q}[x]$ is a PID, but if we look at $\mathbb{Q}[x, y]$, this is not a PID.

However, this is not inconsistent with our theorem from prior, since $\mathbb{Q}[x]$ is not a field; recall that the theorem only states that if F is a field, then $F[x]$ is a ED (and thus a PID); here, $\mathbb{Q}[x, y] = \mathbb{Q}[x][y]$, but $\mathbb{Q}[x]$ is not a field, so the theorem does not apply.

So far, we've been talking about polynomial rings with coefficients coming from fields—what about rings?

Theorem 34.2

R is a UFD if and only if $R[x]$ is a UFD.

As a remark, it follows that a polynomial ring in any number of variables is a UFD is also a UFD (through an inductive argument).

Example 34.3

We have that $\mathbb{Z}[x]$ is a UFD, and $\mathbb{Z}[x]$ is also a UFD, but neither are PIDs.

A next question to answer is: how do we determine which elements are irreducible?

Lemma 34.4: Gauss's Lemma

Let R be a UFD. Let F be the smallest ring containing R in which all nonzero elements of R are units. (F is called the 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 34.5

Let R be a UFD, and let F be the field of fractions of R.

Suppose the GCD of the coefficients of $p(x) \in R[x]$ is 1. Then, $p(x)$ is irreducible in $R[x]$ if and only if $p(x)$ is irreducible in $F[x]$.

Proof. In the forward direction, we already know that if $p(x)$ is reducible in $F[x]$, then $p(x)$ is reducible in $R[x]$, from Gauss's lemma. In the contrapositive, this means that if $p(x)$ is irreducible in $R[x]$, then $p(x)$ is irreducible in $F[x]$.

In the other direction, we want to show that if $p(x)$ is irreducible in $F[x]$, then $p(x)$ is irreducible in $R[x]$. Equivalently, we want to show that if $p(x)$ is reducible in $R[x]$, then $p(x)$ is reducible in $F[x]$.

Suppose $p(x)$ is reducible in $R[x]$. Since the GCD of the coefficients of $p(x)$ is equal to 1, we can express $p(x) = a(x)b(x)$ where neither $a(x)$ nor $b(x)$ are constant polynomials in $R[x]$. (Otherwise, we'd have $p(x) = a(x) \cdot d$, and the GCD of the coefficients of $p(x)$ is equal to some multiple of d.)

This same factorization would apply in $F[x]$ (since $R[x] \subseteq F[x]$), which means that $p(x)$ is reducible in $F[x]$. The contrapositive gives our desired result; if $p(x)$ is irreducible in $F[x]$, then $p(x)$ is irreducible in $R[x]$. □

As a remark for a special case, if $p(x)$ is monic (i.e. leading term is 1) and irreducible in $R[x]$, then $p(x)$ is irreducible in $F[x]$. This is because $\gcd(1, \ldots) = 1$.

Proposition 34.6

Let F be a field, and let $p(x) \in F[x]$.

$p(x)$ has a factor of degree 1 if and only if $p(x)$ has a root in F.

Proof. In the forward direction, suppose $p(x)$ has a factor of degree 1. This means that we can write

$$p(x) = (x - \alpha)p'(x) \implies p(\alpha) = 0.$$

As such, $p(x)$ has a root at α.

In the other direction, suppose $p(\alpha) = 0$. Since $F[x]$ is a ED, we can apply the division algorithm to give

$$p(x) = q(x)(x - \alpha) + r.$$

We know that $\deg(r) = 0$, since this must be strictly less than the degree of $x - \alpha$.

Since $p(\alpha) = 0$, this means that $r = 0$, which means that we have $p(x) = q(x)(x - \alpha)$, giving $(x - \alpha)$ as a factor of degree 1. □

Corollary 34.7

A polynomial of degree 2 or 3 over a field F is reducible if and only if it has a root in F.

Proof. The forward direction follows similarly to the proposition; having a factor of degree 1 implies a root in F.

In the opposite direction, the only way to reduce a polynomial of degree 2 or 3 over a field F is to split it into $p(x) = a(x)b(x)$ where at least one of $a(x)$ or $b(x)$ is of degree 1, which means that if $p(x)$ is reducible, then there must be a factor of degree 1, and thus $p(x)$ has a root in F. □

Proposition 34.8: Eisenstein's Criterion

Let P be a prime ideal of an integral domain R. Let $f(x) = x^n + a_{n-1}a^{n-1} + \cdots + a_0$ be a polynomial in $R[x]$ of degree $n \geq 1$. If $a_{n-1} \cdots a_0 \in P$ and $a_0 \notin P^2$, then $f(x)$ is irreducible in $R[x]$.

Corollary 34.9: Eisenstein's Criterion for $\mathbb{Z}$

Let p be a prime in $\mathbb{Z}$. Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ for $n \geq 1$ in $\mathbb{Z}[x]$. Suppose $p \mid a_i$ for all $0 \leq i \leq n-1$ but $p^2 \nmid a_0$.

Then, $f(x)$ is irreducible in $\mathbb{Z}[x]$, and thus $f(x)$ is irreducible in $\mathbb{Q}[x]$ (using Corollary 34.5).

Example 34.10

1. Consider $x^4 + 10x + 5$. Using the Eisenstein criterion with $p = 5$, this polynomial is irreducible.
2. Consider $x^n - p$. Using the Eisenstein criterion with p, this polynomial is irreducible for all n.
3. Consider $x^4 + 1$. Since no prime divides 1, we cannot apply Eisenstein's criterion directly. However, if we make the substitution $x \mapsto x + 1$, then we get the resulting polynomial $x^4 + 4x^3 + 6x^2 + 4x + 2$, which we can see is irreducible by Eisenstein's criterion for $p = 2$. This means that the original polynomial must also be irreducible.

11/30/2022

Lecture 35

Field Extensions

Recall that a field F is a commutative ring in which every nonzero element is a unit (ex. $\mathbb{Q}$ or $\mathbb{R}$). We've also seen that if F is a field, then $F[x]$ is a Euclidean domain.

A next question is: given any field F and a polynomial $p(x) \in F[x]$, does there exist a larger field K containing F such that $p(x)$ has a root in K?

Example 35.1

Suppose $F = \mathbb{R}$, and $p(x) = x^2 + 1$ in F. We know that $x^2 + 1$ is irreducible in F, but it contains a root in $\mathbb{C}$.

Definition 35.2: Extension field

If K is a field containing a subfield F, then K is an *extension field* of F, denoted K/F.

Definition 35.3: Degree of K/F

The *degree* of K/F, denoted $[K:F]$, is the dimension of K as a vector space over F. That is, $\dim_F K = [K:F]$.

Note that if K/F is a field extension, a basis of K over F is a subset $\{x_1,\dots,x_n\} \subseteq K$ such that every $x \in K$ can be uniquely expressed as a linear combination

$$x = \lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_n x_n,$$

where $\lambda_i \in F$.

Example 35.4

Here are some examples of extension fields and their degrees:

- $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a,b \in \mathbb{Q}\}$ is a field extension of $\mathbb{Q}$, and $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$, since we have a basis $\{1,\sqrt{2}\}$.

  Think of $\mathbb{Q}(\sqrt{2})$ as $\mathbb{Q}[x]$ with $x = \sqrt{2}$; since $(\sqrt{2})^2 = 2$, $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a,b \in \mathbb{Q}\}$.
- Similarly, $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2\}$ is a field extension of $\mathbb{Q}$ with $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}] = 3$, since we have a basis $\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2\}$.
- Consider $\mathbb{Q}(\omega)$ for $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$; here, $\omega^3 = 1$ and $\omega \neq 1$, so $\frac{\omega^3-1}{\omega-1} = \omega^2 + \omega + 1 = 0$, and $\omega^2 = -\omega - 1$.

  This means that a basis is $\{1,\omega\}$, so $[\mathbb{Q}(\omega):\mathbb{Q}] = 2$.

An important class of field extensions comes from finding roots of polynomials.

Firstly, recall Corollary 31.9; since the only ideals of a field F are 0 and F, any homomorphism $\varphi : F \to F'$ between fields F and F' must either be the zero homomorphism (if $\operatorname{Ker}(\varphi) = R$) or it is injective (if $\operatorname{Ker}(\varphi) = 0$). This means that the image of the homomorphism is either 0, or it is isomorphic to F (by the first isomorphism theorem, since we have $\operatorname{Im}(\varphi) \cong F/0 \cong F$).

Theorem 35.5

Let F be a field, and let $p(x) \in F[x]$ be an irreducible polynomial. Then there exists a field K containing an isomorphic copy of F in which $p(x)$ has a root. (That is, there exists a field extension K/F in which $p(x)$ has a root.)

Proof. Consider $K = F[x]/(p(x))$. Since $F[x]$ is a PID and $p(x)$ is irreducible, we know that $(p(x))$ is prime (Proposition 33.15). Further, since in PIDs, prime ideals are maximal (Proposition 33.10), we know that $(p(x))$ is maximal. This implies that K is a field (Proposition 32.4).

We now also want to show that there exists an isomorphic copy of F in K. To do so, consider $\pi : F[x] \to F[x]/(p(x)) = K$, and consider $\varphi = \pi|_F$, (i.e. π restricted to $F \subseteq F[x]$). Let this homomorphism be $\varphi : F \to F[x]/(p(x))$.

Since φ is a homomorphism between fields, we know that φ must either be a zero homomorphism, or injective. Since $\varphi(1) = 1 \in K$, we know that φ is not the zero homomorphism, so it must be injective; this means that the image $\operatorname{Im}(\varphi) \subseteq K$ is isomorphic to F.

Now, we need to check that K contains a root of $p(x)$. Suppose we write $\overline{x} = \pi(x)$, i.e. $\overline{x}$ is the image of x in K through π. This means that we have

$$\begin{aligned} p(\overline{x}) &= \overline{p(x)} && \text{(since } \pi \text{ is a homomorphism)} \\ &= p(x) \pmod{p(x)} && \text{(in } F[x]/(p(x))\text{)} \\ &\equiv 0 \end{aligned}$$

This means that K does contain a root of $p(x)$ (namely, $\overline{x} \in K$). □

Theorem 35.6

Let $p(x) \in F[x]$ be an irreducible polynomial of degree n, and let $K = F[x]/(p(x))$.

If $\theta = x \bmod p(x) \in K$, then the elements $\{1, \theta, \theta^2, \dots, \theta^{n-1}\}$ are a basis for K as a vector space over F.

Hence, $[K : F] = n$ and

$$K = \{a_0 + a_1\theta + a_2\theta^2 + \cdots + a_{n-1}\theta^{n-1} \mid a_0, a_1, \dots, a_{n-1} \in F\}.$$

Proof. Let $a(x) \in F[x]$. Since $F[x]$ is a Euclidean domain, we can divide by $p(x)$ to get

$$a(x) = q(x)p(x) + r(x),$$

where $r(x) = 0$ or $\deg(r(x)) < \deg(q(x))$. Since $q(x)p(x) \in (p(x))$, we have that

$$a(x) \equiv r(x) \pmod{p(x)}.$$

This means that every residue class in K is represented by a polynomial of degree $< n$. This means that $\{1, \theta, \theta^2, \dots, \theta^{n-1}\}$ span K (i.e. the images of $\{1, x, x^2, \dots, x^{n-1}\}$ under the quotient span K).

To prove linear independence, suppose that $\{1, \theta, \theta^2, \dots, \theta^{n-1}\}$ are not linearly independent. That is, suppose there exists some $b_0, b_1, \dots, b_{n-1} \in F$ that are not all zero such that

$$b_0 + b_1\theta + b_2\theta^2 + \cdots + b_{n-1}\theta^{n-1} \equiv 0 \pmod{p(x)}.$$

(That is, the LHS is equivalent to 0 in K.) This means that

$$p(x) \mid b_0 + b_1\theta + b_2\theta^2 + \cdots + b_{n-1}\theta^{n-1},$$

but $n = \deg(p(x))$, and this would imply that $n < n - 1$, which is a contradiction.

This means that $1, \theta, \dots, \theta^{n-1}$ form a basis for the extension K/F, and as such $[K : F] = n$. □

You can think of the elements of $F[x]/(p(x))$ as polynomials of degree $< n$ in θ such that $\theta \in K$ with $p(\theta) = 0$.

Example 35.7

Consider $\mathbb{R}[x]/(x^2 + 1)$. This field is isomorphic to $\mathbb{C}$ through $a + b\theta \mapsto a + bi$.

Here, this is an extension of $\mathbb{R}[x]$ of degree 2 where $x^2 + 1$ has a root $\theta^2 + 1 = 0$. This means that $\theta^2 = -1$, and θ can be seen as i in $\mathbb{C}$.

Similarly, $\mathbb{Q}[x]/(x^2 + 1) \cong \mathbb{Q}(i)$, which is an extension of $\mathbb{Q}$ of degree 2 (since $\{1, i\}$ forms a basis).

Example 35.8

Consider $F = \mathbb{Q}$ and $p(x) = x^3 - 2$. By Eisenstein's criterion, we know that $p(x)$ is irreducible (2 divides all non-leading coefficients, and $4 \nmid (-2)$).

Let θ denote a root of $p(x)$ in $\mathbb{Q}[x]/(x^3 - 2)$. Then, we have

$$\mathbb{Q}[x]/(x^3 - 2) \cong \{a + b\theta + c\theta^2 \mid a, b, c \in \mathbb{Q}\}.$$

Here, $\theta^3 = 2$.