PMATH 347

Group and Rings

Zhisu Wang
Taught by David McKinnon
University of Waterloo

Spring 2023

Contents

1 Introduction to Groups 3

1.1 Basic Axioms and Definitions . . . 3

1.2 Dihedral Groups . . . 4

1.3 Symmetric Groups and other groups . . . 4

1.4 Homomorhisms and Isomorphisms . . . 5

1.5 Group Actions . . . 7

1.6 Cyclic Group . . . 10

1.7 Lagrange's Theorem . . . 11

1.8 Normal Subgroup . . . 12

1.9 Universal Property of Quotients . . . 15

1.10 Conjugate Class . . . 16

1.11 Generators and Relations . . . 18

1.12 Orbit-Stabilizer Theorem . . . 21

1.13 Even Permutations . . . 22

1.14 Sylow's Theorem . . . 23

1.15 Isomorphisms of Finite Group . . . 26

2 Introduction to Rings 29

2.1 Basic Axioms and Definitions . . . 29

2.2 Subring Theorem . . . 31

2.3 Homomorhisms . . . 32

2.4 R-module . . . 33

2.5 Properties of Ideals . . . 34

2.6 Principal Ideal Domain . . . 39

2.7 Properties of R-modules . . . 40

2.8 Fundamental Theorem of Finitely Generated Abelian Group . . . 45

2.9 Chinese Remainder Theorem . . . 50

2.10 Final Exam . . . 51

1 Introduction to Groups

1.1 Basic Axioms and Definitions

Definition 1.1: Groups

A group is an ordered pair $(G, *)$ where G is a set and $*$ is a binary operation on G statisfying the following axioms:

1. (**Associativity**) $(a * b) * c = a * (b * c)$, for all $a, b, c \in G$
2. (**Existence of Identity**) there exists an element 1 in G, called an *identity* of G, such that for all $a \in G$ we have
$$a * 1 = 1 * a = a$$
3. (**Existence of Inverse**) for each $a \in G$, there is an element a^{-1} of G called an *inverse* of a, such that
$$a * a^{-1} = a^{-1} * a = 1$$

Definition 1.2: Subgroups

A subgroup of a group G is a subset $H \subset$ that is also a group using the same operation as G.

Theorem 1.1: Subgroup Theorem

Let G be a group, $H \subset G$ a nonempty subset. Then H is a subgroup of G if and only if
$$\forall a, b \in H, a \cdot b \in H \text{ and } a^{-1} \in H$$

Proof:

($\Rightarrow$) Trivial: list definitions.
($\Leftarrow$) We assume $a, b \in H$, $a^{-1} \in H$ for all $a, b \in H$. We want to show H is a subgroup of G. The fact that $ab \in H$ means that $H \cdot H \to H$ is well defined. So it makes sense to check $(1), (2), (3)$:

1. trivial.
2. check $1 \in H$. Choose $a \in H$. Then
$$1 = a \cdot a^{-1} \in H$$

because $a \cdot a^{-1} \in H$

3. trivial.

□

Definition 1.3: Order

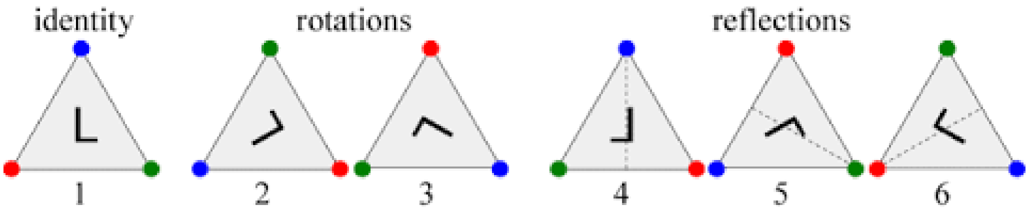
The order of an element $g \in G$, is the smallest positive integer n satisfying $g^n = 1$.

Definition 1.4: Order of groups

The order of a group is its cardinalty. Ex: $\mid S_n \mid = n!$

1.2 Dihedral Groups

For each $n \in \mathbb{Z}^+, n \geq 3$, let D_{2n} be the set of symmetries of a regular n-gon, where a symmetry is any rigit motion of the n-gon which can be effected by taking a copy of the n-gon, moving this copt in any fashion in 3-space and then placing the copy back on the original n-gon so it exactly covers it.



An example of D_6

1.3 Symmetric Groups and other groups

Let $n \in \mathbb{N}$, the symmetry group of degree n is a group under function composition $\circ : \{1, \ldots, n\} \to \{1, \ldots, n\}$. In general,

$$\begin{aligned} S_n &= \text{symmetric group on n letters} \\ &= \{\text{permutation of } \{1, \ldots, n\}\} \\ &= \{\text{bijection } f : \{1, \ldots, n\} \to \{1, \ldots, n\}\} \end{aligned}$$

Example 1.0

How to generate a **disjoint cycle** notation for $G : \{1, \dots, n\} \to \{1, \dots, n\}$:

1. Keep iterating G until yu get back to 1:

$$1, G(1), G(G(1)) \dots$$

2. If there are any elements of {1, . . . , n} left, start over at step (1) with the samllest of them.

3. Keep going until you are done.

Example 1.1

Other examples of groups:

1. $\mathbb{Z}/n\mathbb{Z}$:

2. $GL_n(\mathbb{R}) = \{\text{invertible } n \times n \text{ matrices}\}$

3. $SL_n(\mathbb{R}) = \{n \times n \text{ matrices}, det = 1\}$

4. $SO_n(\mathbb{R}) = n \times n$ matrices M, $dist(Mv, Mu) = dist(v, u)$ for all v, u

5. Quaternion Group:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}$$

1.4 Homomorhisms and Isomorphisms

Definition 1.5: Abelian Group

A group G is **abelian** iff $ab = ba$ for every $a, b \in G$.

Definition 1.6: Direct Product

The direct product of groups G and H is the group $G \times H$.

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

with

$$(g, h)(g', h') = (gg', hh')$$

Definition 1.7: Homomorphism

Let G and H be groups. A homomorphism from G to H is a function $f : G \to H$ satisfying

$$f(ab) = f(a)f(b)$$

for all $a, b \in G$

We can derive $f(1) = f(a \cdot a^-1) = f(a)f(a^{-1}) = f(a)f(a)^{-1} = 1$, given $f(a^{-1}) = f(a)^{-1}$.

Definition 1.8: Isomorphism

An isomorphism from G to H is a homomorphism $f : G \to H$ with an inverse homomorphism $f^{-1} : H \to G$.

Theorem 1.2

A homomorphism $f : G \to H$ is an isomorphism iff it is 1-1 and onto.

Proof:

($\Rightarrow$) Trivial. f has inverse iff f is one-to-one and onto. ($\Leftarrow$) Let $f : G \to H$ be a bijective homomorphism. Since f is bijective, it has an inverse $f^{-1} : H \to G$. We want to show that f^{-1} is a homomorphism. Let $a, b \in H$. We want to show $f^{-1}(a)f^{-1}(b) = f^{-1}(ab)$. It is enough to show

$$f(f^{-1}(ab)) = f(f^{-1}(a)f^{-1}(b))$$

because f is injective. This is

$$ab = f(f^{-1}(a)f^{-1}(b))$$

so we want compute

$$\begin{aligned} f(f^{-1}(a)f^{-1}(b)) &= f(f^{-1}(a))f(f^{-1}(b)) \\ &= ab \end{aligned}$$

□

Example 1.2

1. $\det(GL_n(\mathbb{R}) \to \mathbb{R}^*)$ given by $det(A) = det(A)$. Note that

$$det(AB) = det(A)det(B)$$

This is a homomorphism, but not a isomorphism.

2. $q : \mathbb{Z} \to \mathbb{Z}/7\mathbb{Z}$ which is $q(n) = n \mod 7$, where

$$q(m + n) = q(m) + q(n)$$

This is a homomorphism, but not isomorphism.

3. $i : S_n \to S_{n+1}$. Let $\sigma \in S_n$, $\sigma : \{1, \dots, n\} \to \{1, \dots, n\}$. Define $i(\sigma) : \{1, \dots, n+1\} \to \{1, \dots, n + 1\}$ such that

$$[i(\sigma)](k) = \begin{cases} \sigma(k) & \text{if } k \in \{1, \dots, n\} \\ k & \text{if k = n + 1} \end{cases}$$

It turns out that i is a homomorphism, but not isomorphism. To prove the former, we need to show

$$i(\sigma \circ \tau) = i(\sigma) \circ i(\tau)$$

This turns out to be straightforward and annoying.

4. $\log : \mathbb{R}^* \to R$ where $\log(xy) = \log(x) + \log(y)$. This is an isomorphism.

1.5 Group Actions

Definition 1.9: Group Actions

A group action of group G on a set S is a homomorphism $\phi : G \to \text{Sym}(S)$ where $\text{Sym}(S) = \{f : S \to S, \text{ f bijective}\}$ (a permutation).

Example 1.3

1. $\phi : GL_n(\mathbb{R}) \to \text{Sym}(\mathbb{R})$ is a map

$$M \to \{\vec{v} \to M\vec{v}\}$$

This is an action

2. $\phi : GL_n(\mathbb{R}) \to \text{Sym}(\mathbb{R}^n)$ is a map $M \to \{\vec{v} \to (detM)\vec{v}\}$ This is an action.

3. $\phi : S_n \to S_n$ given by $\phi(\sigma) = \sigma$. This is an action of S_n on $\{1, \dots, n\}$.

4. $\phi : G \to \text{Sym}(S)$ such that

$$\phi(g) = id$$

this is a trivial action

> 5. $\phi : D_n \to \text{Sym}(n\text{-gon})$ such that $\phi(\sigma) = \sigma$. This is an action of D_n on a regular n-gon.

Definition 1.10: Free, Faithful, Transitive

An action $\phi : G \to \text{Sym}(S)$ is

1. **Free** iff $\phi(g)$ fixes no elment of S unless $g = 1$, that is,

$$[\phi(g)](s) = s \implies g = 1$$

2. **Faithful** iff ϕ is injective. That is every element g of G moves something in S (except $g = 1$).

3. **Transitive** iff for every $x, y \in S$, there is some $g \in G$ such that

$$[\phi(g)](x) = y$$

Note that every free action is faithful.

Definition 1.11: Orbit

Let $\phi : G \to \text{Sym}(S)$ be an action and let $x \in S$ be an element. The **orbit** of x is

$$O_x = \{gx \mid g \in G\} \subset S$$

where $gx = [\phi(g)](x)$.

Notice that if $x \in O_y$, then $gy = x \implies y = g^{-1}x \implies y \in O_x$ since $x \in O_x (g = 1)$, we see that the orbits O_x partition S.

Definition 1.12: Stabilizer

Let $x \in S$. The **stabilizer** of x is

$$\text{stab}(x) = \{g \in G \mid gx = x\}$$

Let G be a group acts on itself by left multiplication: give $\phi : G \to \text{Sym}(G)$ such that

$$\phi(g) = \{x \to gx\}$$

This is an action. We need to check

$$\phi(gn) = \phi(g)\phi(n)$$

We have

$$\begin{aligned}[\phi(g)\phi(h)](x) &= [\phi(g)]([\phi(h)](x)) \\ &= [\phi(g)](hx) \\ &= ghx \\ &= [\phi(gh)](x)\end{aligned}$$

The action is free: $gx = x \Leftrightarrow (gx)x^{-1} = xx^{-1} \Leftrightarrow g = 1$.
Since it's free, it's automatically faithful.
It is also transive: for any x, y, we have $y = (yx^{-1})x$.
For any x, $\text{stab}(x) = 1$ and $Q_x = G$. Say G is a finite group. Then we can number the elements of G $1, \dots, n$. So $\text{Sym}(G) \cong \text{Sym}(\{1, \dots, n\}) = S_n$. So this action gives an injective homomorphism $G \to S_n$. In particular, every finite group is isomorphic to a subgroup of S_n, where $n = |G|$. This is the Cayley's Theorem.

Theorem 1.3: Cayley's Theorem

Every group G is isomorphic to some subgroup of $S_{|G|}$.

Example 1.4

Let G acts on itself by conjugation:$\phi : G \to \text{Sym}(G)$ such that

$$\phi(g) = \{x \to gxg^{-1}\}$$

We check

$$\begin{aligned}[\phi(g)\phi(h)](x) &= [\phi(g)]([\phi(h)](x)) \\ &= [\phi(g)](hxh^{-1}) \\ &= ghxh^{-1}g^{-1} \\ &= (gh)x(gh)^{-1}\end{aligned}$$

This action is not free (if $G \neq \{1\}$) since $gxg^{-1} = x \Rightarrow gx = xg$ which happens if $x = g$. It's sometimes faithful and sometimes not. It is not transitive, for example, 1 is fixed by every element of G. For any x,

$$\begin{aligned} \text{stab}(x) &= \text{centralizer of } x \\ &= \{g \mid gx = xg\} \\ O_x &= \text{the conjugacy class of } x \end{aligned}$$

1.6 Cyclic Group

Let G be a group, $g \in G$ any element. The subgroup of G generated by g is

$$\begin{aligned} \langle g \rangle &= \{g^n \mid n \in \mathbb{Z}\} \\ &= \{\ldots, g^{-3}, g^{-2}, g^{-1}, 1, g, g^2, \ldots\} \end{aligned}$$

Since $\langle g \rangle$ is closed under multiplication and inversion, it is a subgroup.

Definition 1.13: Cyclic Group

A cyclic group of G is a group of the form $\langle g \rangle$ for some $g \in G$.

Example 1.5

1. $G = \mathbb{Z}, g = 1$. Then

$$\langle g \rangle = \{\ldots, -3, -2, -1, 0, 1, 2, \ldots\} = \mathbb{Z}$$

so $\mathbb{Z}$ is itself a cyclic group.

2. $G = \mathbb{Z}/n\mathbb{Z}, g = 1$. Then

$$\langle g \rangle = \{0, 1, 2, \ldots, n-1\} = \mathbb{Z}/n\mathbb{Z}$$

Theorem 1.4

Let G be a group, $g \in G$ any element. Then if g has infinite order,

$$\langle g \rangle \cong \mathbb{Z}$$

and if g has finite order n,

$$\langle g \rangle \cong \mathbb{Z}/n\mathbb{Z}$$

Proof:

(1) Define a function $\phi : \mathbb{Z} \to \langle g \rangle$ such that

$$\phi(n) = g^n$$

ϕ is onto. If g has infinite order, then ϕ is also injective:

$$\begin{aligned} &\phi(n) = \phi(m) \\ \Leftrightarrow &g^n = g^n \\ \Leftrightarrow &g^{n-m} = 1 \\ \Leftrightarrow &n = m \end{aligned}$$

so if g has infinite order, ϕ is the desired isomorphism $\langle g \rangle \cong \mathbb{Z}$.
(2) If g has finite order n, then ϕ is well defined mod n. If $k \equiv 1 \mod n$, then

$$\phi(k) = g^k = 1 = \phi(1)$$

So if g has order n, we can define $\bar{\phi} : \mathbb{Z}/n \to \langle g \rangle$ by

$$\bar{\phi}(k \text{ mod n}) = \phi(k) = g^k$$

$\bar{\phi}$ is onto because ϕ is onto. And $\langle g \rangle$ has n elements $\{1, g, g^2, \ldots, g^{n-1}\}$, so $\bar{\phi}$ is also injective and is therefore an isomorphism. □

1.7 Lagrange's Theorem

Theorem 1.5: Lagrange's Theorem

Let G be a group, $H \subset G$ a subgroup. Then $|G|$ is divisible by $|H|$.

Proof:

There is an action of H on G by left multiplication.

$$\phi : H \to \text{Sym}(G), [\phi(h)](g) = hg$$

The orbit of 1 under this actions is H.
The orbit of g is

$$Hg = \{hg \mid h \in H\}$$

> and there is a bijection
>
> $$H \to Hg$$
>
> $$h \to hg \text{ inverse } a \to ag^{-1}$$
>
> so G is the disjoint union of the orbits, all of which are size $|H|$. That is,
>
> $$|G| = (|H|)(\# \text{ of orbits})$$
>
> □

Remark: Hg is a **right coset** of H in G. The number of right cosets is the index of H in G, and it written $[G : H] = \#$ of right H-cosets in G. If G is finite, then

$$[G : H] = \frac{|G|}{|H|}$$

Definition 1.14: Cosets

For any $N \leq G$ and any $g \in G$. Let

$$gN = \{gn \mid n \in N\} \text{ and } Ng = \{ng \mid n \in N\}$$

are called respectively a left coset and a right coset of N in G.

Corollary 1.6

Let G be a group, $x \in G$ any element. Then $|G|$ is divisible by the order of x.

Proof:

> Lagrange apllied to $\langle g \rangle$. □

1.8 Normal Subgroup

Consider $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$. This is the smallest subgroup of G that contains g. Let G be a group, $S \subset G$ a subset of G. The smallest subgroup of G that contains S is

$$\begin{aligned}\langle S \rangle &= \bigcap_{H \subset G \text{ subgroup}, S \subset H} H \\ &= \{a_1^{n_1} a_2^{n_2} a_3^{n_3} \cdots a_r^{n_r} \mid a_1, \ldots, a_r \in S, n_1 \ldots, n_r \in \mathbb{Z}\}\end{aligned}$$

Say $f : G \to H$ is a homomorphism, how do we tell if f is injective?

Definition 1.15: Kernel

The **kernel** of f is

$$\ker(f) = \{g \in G \mid f(g) = 1\}$$

Theorem 1.7

f is 1-1 iff $\ker f = \{1\}$.

Proof:

($\Rightarrow$) Trivial

($\Leftarrow$) Say $\ker f = \{1\}$. We want to show f is 1-1. Say

$$\begin{aligned} & f(a) = f(b) \\ \implies & f(a)f(b)^{-1} = 1 \\ \implies & f(a)f(b^{-1}) = 1 \\ \implies & f(ab^{-1}) = 1 \\ \implies & ab^{-1} \in ker f = \{1\} \\ \implies & ab^{-1} = 1 \\ \implies & a = b \end{aligned}$$

□

$ker f$ is a subgroup of G:

$$f(a) = 1 \Rightarrow f(a^{-1}) = f(a)^{-1} = 1$$

and

$$f(a) = 1, f(b) = 1 \Rightarrow f(ab) = f(a)f(b) = 1$$

and

$$f(1) = 1$$

Say $a \in ker f$, $g \in G$. Then $f(gag^{-1}) = f(g)f(a)f(g)^{-1} = 1$. So $gag^{-1} \in ker f$. In particular $ker f$ is closed under conjugation. gag^{-1} is the conjugate of a by g.

Definition 1.16: Normal Subgroup

A subgorup $H \subset G$ is **normal** iff for every $h \in H$, $g \in G$, we have

$$ghg^{-1} \in H \Leftrightarrow gHg^{-1} \in H$$

Theorem 1.8

Let $H \subset G$ be a subgroup. Then H is normal **iff** there is a group P and a homomorphism

$$\phi : G \to P$$

such that $\ker \phi = H$.

Proof:

($\Leftarrow$) We already did: $\ker f$ is always a normal subgroup.

($\Rightarrow$) Assume H is nomral. We want to define a group P and a homomorphism $\phi : G \to P$ with $\ker \phi = H$.
Once we get ϕ, it will map $H \to \{1\} \subset P$. If $g \notin H$, then $\phi(g) \neq 1$ in P. If g' satisfies $\phi(g') = \phi(g)$, then

$$\Leftrightarrow \phi(g^{-1}g') = 1 \Leftrightarrow g^{-1}g' \in H \Leftrightarrow g' \in gH$$

Define $P = \{gH \mid g \in G\}$. This tells us what P is as a set. We define multiplication as

$$(g_1H)(g_2H) = g_1g_2H$$

we show this is well defined: say $g_1H = g_1'H, g_2H = g_2'H$, we need $g_1g_2H = g_1'g_2'H$. We need a lemma

Lemma 1.9

If H is normal, then $\forall g \in G, gH = Hg$.

Proof:

Say $gh \in H$. Suppose $gh \in Hg$. But H is normal, so $ghg^{-1} \in H$, so $gh \in Hg$. The revserse direction is similar. □

Now

$$\begin{aligned} g_1g_2H &= g_1g_2'H \\ &= g_1Hg_2' \\ &= g_1'Hg_2' \\ &= g_1'g_2'H \end{aligned}$$

It's straightforward to show that this operation makes P into a group, using the fact that G is a group.
Now, define $\phi : G \to P$ by $\phi(g) = gH$. It is a homomorphism. It is also easy to see that

$\ker \phi = H$. □

The group P is called the quotient group of G by H and is written G/H. We have $\phi : G \to H$, $\operatorname{im} \phi = \{h \in H \mid h = \phi(g)$ for some $g \in G\}$, and $\operatorname{im} \phi$ is a subgroup of G.

1.9 Universal Property of Quotients

Theorem 1.10: Universal Property of Quotients

Let G be a group. $N \subset G$ be a normal subgroup, where

$$f : G \to H \text{ a homomorphism}$$

$$q : G \to G/N \text{ the "reduce mod N" homomorphism}$$

There exists a homomorphism $\bar{f} : G/N \to H$ satisfying

$$f = \bar{f} \circ q$$

iff $N \subset \ker f$. Moreover, if $\bar{f}$ exists, then $\operatorname{im} \bar{f} = \operatorname{im} f$ and $\ker \bar{f} = q(\ker f)$.

Proof:

($\Rightarrow$) We want $N \subset \ker f$. If $n \in N$, then $f(n) = \bar{f}(q(n)) = \bar{f}(1) = 1$. ($\Leftarrow$) Say $N \subset \ker f$. Define $\bar{f}(gN) = f(g)$. To check that this is well defined, say $g_1N = g_2N$. Then

$$\bar{f}(g_1N) = f(g_1)$$

$$\bar{f}(g_2N) = f(g_2)$$

but $g_2^{-1}g_1 \in N$, so $f(g_2^{-1}g_2) = 1 \Rightarrow f(g_1) = f(g_2)$.
The facts that $\operatorname{im} \bar{f} = \operatorname{im} f$ and $\ker \bar{f} = \ker f \mod N$ follows immediately from

$$f = \bar{f} \circ q$$

and the surjectivity of q. □

Theorem 1.11: First Isomorphism Theorem

Let $f : G \to H$ be a homomorphism. Then

$$\operatorname{im} f \cong G/\ker f$$

Proof:

UPQ tells us that there is $\bar{f} : G/\ker f \to H$. The kernel of $\bar{f}$ is

$$\ker f \pmod{\ker f} = 1 \bmod \ker f$$

so $\bar{f}$ is injective. Also, $\operatorname{im} \bar{f} = \operatorname{im} f$, so $\bar{f}$ is onto $\operatorname{im} f$. Therefore, $\bar{f} : G/\ker f \to \operatorname{im} f$ is bijective, so it's an isomorphism. □

Corollary 1.12

Let $f : G \to H$ be a homomorphism with G finite. Then

$$|\ker f| \cdot |\operatorname{im} f| = |G|$$

Proof:

By the First Isomorphism Theorem, we know

$$|\operatorname{im} f| = |G/\ker f| = \frac{|G|}{|\ker f|}$$

given G is finite. □

1.10 Conjugate Class

Every group G acts on itself by conjugation

$$\phi : G \to \operatorname{Sym}(G)$$

$$\phi(g) = \{x \to gxg^{-1}\}$$

The orbit of g under this action is called the **conjugacy class** of g. Note that $\{x \to gxg^{-1}\}$ is a isomorphism $G \to G$:

$$\begin{aligned}[\phi(g)](xy) &= gxyg^{-1} = gxg^{-1}gyg^{-1} \\ &= [\phi(g)](x) \cdot [\phi(g)](y)\end{aligned}$$

so the elements of the same conjugacy class are **algebraically identical**, that is, they have the same order.

The stabilizer of x under conjugation is called **centralizer** of x. It's all the elements of G that commute with x.

Definition 1.17: Centre

The **centre** of a group G is the set

$$Z(G) = \{z \in G \mid zg = gz \forall g \in G\}$$

In particular, $Z(G)$ is a subgroup. Conjugacy in $GL_n(\mathbb{R})$ in similarity.

Example 1.6

> If G is abelian, then conjugation is trivial, so conjugacy classes all have one element.

$\phi : \mathbb{Z}/mn\mathbb{Z} \to (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$ such that

$$\phi(x \bmod mn) = (x \bmod m, x \bmod n)$$

ϕ is a homomorphism. Both sides have mn elements. ϕ is injective if $\gcd(m, n) = 1$, because if

$$x \equiv 0 \bmod m$$

$$x \equiv 0 \bmod n$$

then

$$x \equiv 0 \bmod mn$$

Thus ϕ is an isomorphism. So $\mathbb{Z}/mn\mathbb{Z} \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$.
When is $G \cong H \times K$? Well, subgroups of G would corresponde to subgroups of $H \times K$.

$$K' = \{1\} \times K \text{ and } H' = H \times \{1\}$$

are both normal subgroups of $H \times K$.

$$\begin{aligned} \pi_1 : H \times K &\to H \\ (h, k) &\to h \\ \pi_2 : H \times K &\to K \\ (h, k) &\to k \end{aligned}$$

$H' \cap K' = \{1\} = \{(1, 1)\}$ and $h'k' = k'h'$ for all $k' \in K', h' \in H'$.
For every $x \in H \times K$, there are $h' \in H'$ and $k' \in K'$ satisfying

$$h'k' = x$$

Theorem 1.13

Let G be a group, $N \notin M$ be normal subgroups G satisfying:

1. $N \cap M = \{1\}$
2. $nm = mn, \forall m \in M, n \in N$
3. $\forall g \in G, \exists m \in M, n \in N$ with $mn = g$

Then $G \cong M \times N$ via $\phi : M \times N \to G, \phi(m, n) = mn$.

Proof:

Let $\phi : M \times N \to G$, $\phi(m, n) = mn$. It is a homomorphism:

$$\begin{aligned}\phi((m_1, n_1)(m_2, n_2)) &= \phi(m_1 m_2 n_1 n_2)\\ &= m_1 m_2 n_1 n_2\\ &= m_1 n_1 m_2 n_2\\ &= \phi(m_1, n_1)\phi(m_2, n_2)\end{aligned}$$

ϕ is onto becasue of (3), $\ker \phi = \{1\}$ because if $\phi(m, n) = 1$, then $mn = 1$, $\Leftrightarrow m = n^{-1} \Leftrightarrow m = n = 1$.

□

1.11 Generators and Relations

Say $G \to D_n$, symmetries of a regular n-gon. Let $H \subset D_n$ be the subrgoup of rotations. Is there a subgroup $N \subset D_n$ such that $D_n \cong H \times N$? No because H has n elements, so if such an N existed, it would have 2 elements. But H is abelian, and every group with 2 elements is isomorphic to $\mathbb{Z}_2$, so also abelian. But D_n is not abelian, so it couldn't be isomorphic to $H \times N$.
Holder: If you understand N and G/N,then maybe you can understand G. Sadly, it's not that simple: $D_n/H \cong \mathbb{Z}_2$, $(H \times \mathbb{Z}_2)/H \times \{1\} \cong \mathbb{Z}_2$. Nevertheless, if G has non-trivial normal subgroup N, then this idea has some merit: you can use N and G/N to understand G better.

Definition 1.18: Simple Group

A group G is **simple** if its only normal subgroups are $\{1\}$ and G.

Example 1.7

$\mathbb{Z}_p$ for p prime.

Definition 1.19: Free Group

Let S be a set. The **free group** on S is the set of all equivalence classes of finite strings.

$$\{x_1,\ldots,x_r \mid r\in\mathbb{Z}_{\geq 0}, x_i = s \text{ or } s^{-1}\text{for } s\in S\}$$

where the equivalence relation is the transitive closure of

$$\{x_1\ldots x_r \sim x_1\ldots,x_m ss^{-1}x_{m+1}\ldots x_r \sim x_1\ldots x_m s^{-1}sx_{m+1}\ldots x_r\}$$

The operation is concatentaion.

Example 1.8

> $S=\phi\Rightarrow F_S=\{1\}$
> $S=\{1\}\Rightarrow F_S\cong\mathbb{Z}$ because F_1 is strings of 1's and 1^{-1}s so the homomorphism $\phi:\mathbb{Z}\to F_1$, by $\phi(n)=\begin{cases} n1 & \text{if } n>0\\ -n1^{-1} & \text{if } n<0\end{cases}$ is an isomorphism. $F_{\{a,b\}}$ is huge! It has elements like $aba^{-1}b$, $a^2b^{-1}a^{-1}b^{-1}a^{-1}$, ab, ba and they are all different.

Say $G=\langle g_1,g_2\rangle$. Define $\phi:F_2\to G$ by $\phi(\text{string})=\text{same string}$. This is an homomorphism. Its image $\operatorname{im}\phi$ is $\langle g_1,g_2\rangle$. So if $G=\langle g_1,g_2\rangle$, it's onto. The kernel $\ker\phi$ of ϕ is called the relation satisfied by g_1,g_2.
$F_S=$ free group on set S. Every group is the quotient of a face group. Say $G=\langle S\rangle$, where S is some subset of G. Then we can define a homomorphism $\phi:F_S\to G$, $\phi(\text{string})=$ stribg as element of G. Then ϕ is onto because $\operatorname{im}\phi$ contains S so it contains $\langle S\rangle=G$. Sy by the UPQ, ϕ induces an isomorphism $\tilde{\phi}:F_S/\ker\phi\to G$. We usually write this as $G=\{S\mid R\}$, where R is a subset of F_S such that $\ker\phi$ is the smallest normal subgroup of F_S that contains R.

Example 1.9

> $D_n=\{x,y\mid x^2,y^n,xyxy\}$
> $x^2=y^n=1, xy=y^{-1}x$

Let's verify this. Say $G=\{x,y\mid x^2,y^2,xyxy\}$. We want an isomorphism $G\to D_n$. There is a homomorphism $\phi:F_2\to D_n$

$$\phi(x)=\text{ reflection } s$$

$$\phi(y)=\text{rotation } r \text{ of } \frac{2\pi}{n}\text{ rad}$$

This homomorphism contains x^2,y^n and $xyxy$ in its kernel. So the UPQ gives a homomorphism $\tilde{\phi}$ is onto because $\operatorname{im}\tilde{\phi}=\operatorname{im}\phi=D_n$.

We want to show that $\tilde{\phi}$ is injective. To do this, it's enough to show that F_2/N has at most $2n$ elements. An element of F_2/N is mN, where $m =$ srting of x, y, x^{-1}, y^{-1}. We will see that the relation in R to do this.
First, $x^2 = 1 \bmod N$ means that the string m mod N does not need to have consecutive x's or x^{-1}'s. Likewise for y's and y^{-1}'s.
Using $xy = y^{-1}x$, we can see that m mod N can start with a string x's and end with a string of y's. thus, mod N, the string N can be written as either:

$$y^i, i \in \{0, \dots, n-1\} \text{ or } xy^i i \in \{0, \dots, n-1\}$$

So F_2/N has at most $2n$ elements.
Since ϕ surjects onto the $2n$-element group D_n, we see $\tilde{\phi}$ is an isomorphism. □

S_n acts on $\mathbb{R}^n$ by permuting coordinates.

Example 1.10

> (12) permutes (a, b) via (b, a).

$$\phi : S_n \to \text{Sym}(\mathbb{R}^n)$$

In fact, we get $\phi : S_n \to GL_n(\mathbb{R})$. We can compose with det to get a homomorphism.

$$\text{sgn}(\sigma) = \det(\phi(\sigma))$$

Clearly, $\text{sgn}(\sigma) = 1$ or -1. Not always -1. Also, not always 1. $\text{sgn}((12)) = -1$. So $\text{sgn} : S_n \to \{\pm 1\}$ is a homomorphism whose kernel has $\frac{n!}{2}$ elements.

$$(\#\ker(\text{sgn}))\underbrace{(\#\,\text{im}(\text{sgn}))}_{2} = \#\underbrace{S_n}_{n!}$$

The subgroup of $\ker(\text{sgn}) \subset S_n$ is called A_n, the alternating group on n letters. Elements of A_n are even permutations. Other elements of S_n are odd permutations.

Example 1.11

> 1. The identity (1) is even.
>
> 2. Every 2-cycle is odd.
>
> 3. A 3-cycle $(xyz) = (xz)(xy)$.

Fact: n is odd $\Rightarrow$ $n-$cycle is even. n is even $\Rightarrow$ n-cycle is odd.

Proof: $(a_1 \dots a_m) = \underbrace{(a_m a_{m-1}) \dots (a_2 a_1)}_{m-1 \text{ of these, all odd}}$.

So the 2-cycles generate S_n, any subgroup of S_n that contains all the 2-cycles is S_n.

1.12 Orbit-Stabilizer Theorem

Theorem 1.14: Orbit-Stabilizer

Let G be finite group acting on a set X. X is a G-set. Let $x \in X$. Then,

$$|O_x| \cdot |\operatorname{Stab}(x)| = |G|$$

Proof:

> $\exists$ a homomorphism $\phi : G \to \operatorname{Sym}(X)$. There is a function $\varphi : G \to O_x$, given by $g \to [\phi(g)](x)$. The set $\varphi^{-1}(x) = \operatorname{Stab}(x) = \{g \in G \mid \varphi(g) \in \{x\}\}$ For any $y \in O_x$, there is some g such that $g(x) = y$. If $g'(x) = y$, then
>
> $$(g^{-1}g')(x) = g^{-1}(y) = x, \text{ so } g^{-1}g \in \operatorname{Stab}(x)$$
>
> Conversely, if $g^{-1}g \in \operatorname{Stab} x$, then $(g^{-1}g')(x) = x \Rightarrow g^{-1}(g'(x)) = x$, so $g'(x) = y$.
> So $g'(x) = y$ iff $g^{-1}g \in \operatorname{Stab}(x) \Leftrightarrow g' \in g \operatorname{Stab}(x)$.
> Thus, for each element of O_x, there are $\operatorname{Stab}(x)$ elements of G satisfying $g(x) = y$. Therefore, $|G| = |O_x| \cdot |\operatorname{Stab}(x)|$ □

Let G act on itself by conjugation. If $x \in G$, then for this action, $O_x =$ conjugacy classes of x and $\operatorname{Stab}(x) =$ centralizer of x. So $|\text{conjugacy class}| \cdot |\text{cent}(x)| = |G|$.
$G =$ disjoint union of conjugacy classes. Say conjugacy classes are $K_1, \dots, K_r$. Choose $g_i \in K_i$. Then

$$|G| = \sum_{i=1}^{r} |K_i| - \sum_{i=1}^{r} \frac{|G|}{|\operatorname{Cent}(g_i)|} = |Z(G)| + \sum_{i=j+1}^{r} \frac{|G|}{\operatorname{Cent}(g_i)}$$

where $Z(G) =$ centre of $K_1, \dots, K_j$ are the conjugacy classes of eleemnts of $Z(G)$.
Say $\tau \in S_n$. Then $\tau(a_1 \dots, a_r)\tau^{-1} = (\tau(a_1)\tau(a_2)\tau(a_3) \dots \tau(a_r))$. More generally, conjugating σ by τ yields the same permutation only with a_i by $\tau(a_i)$. So conjugacy classes in S_n are the sets of permutation with the same disjoint cycle notation shape.

Example 1.12

> $S_3 = \{(1)\}, \{(12), (13), (23)\}, \{(123), (132)\}$.
> $S_5 = \underset{1}{\{(1)\}}, \underset{10}{\{(ab)\}}, \underset{20}{\{(abc)\}}, \underset{30}{\{(abcd)\}}, \underset{24}{\{(abcde)\}}, \underset{15}{\{(ab)(cd)\}}, \underset{20}{\{(abc)(de)\}}$.

1.13 Even Permutations

$A_5 =$ even permutations in S_5. These are

$$\begin{aligned}\{(1)\} &- 1 \text{ element}\\ \{(abc)\} &- 20 \text{ elements}\\ \{(abcde)\} &- 24 \text{ elements}\\ \{(ab)(cd)\} &- 15 \text{ elements}\end{aligned}$$

We will use this list to show that A_5 is simple. Show the only subgroups of A_5 are $\{1\}$ and A_5.
What are the conjugacy classes of A_5? Any normal subgroups of A_5 is a union of conjugacy classes. So

$$|\text{conjugacy class}| \cdot |\text{centralizer}| = |G|$$

In S_5, the centralizers are

$$\begin{aligned} &\qquad\text{Centralizer}\\ \{1\} &\leftrightarrow \quad S_5\\ \{(abc)\} &\leftrightarrow 6 \text{ element subgroup}\\ \{(abcde)\} &\leftrightarrow 5 \text{ elements} = \langle(abcde)\rangle\\ \{(ab)(cd)\} &\leftrightarrow 8 \text{ element subgroup}\end{aligned}$$

Every conjugacy class in A_5 is contained in some conjugacy class of S_5, $\forall\sigma \in A_5$, $\text{Cent}_{A_5}(\sigma) \subset \text{Cent}_{S_5}(\sigma)$. In fact, $\text{Cent}_{A_5}(\sigma) = \text{Cent}_{S_5}(\sigma) \cap A_5$.
$\text{sgn}(\text{Cent}_{S_5}(\sigma)) = \{\pm 1\}$ or $\{1\}$. If it's $\{1\}$, then the $\text{Cent}_{S_5}(\sigma) \subset A_5$ so $\text{Cent}_{A_5}(\sigma) = \text{Cent}_{S_5}(\sigma)$. If it's $\{\pm 1\}$, then $\text{Cent}_{A_5}(\sigma)$ has index 2 in $\text{Cent}_{S_5}(\sigma)$. So it's half the size.
$\{1\} - \text{Cent}_{S_5}(\sigma)$ has size 120 so $\text{Cent}_{A_5}(\sigma)$ has size 60, so its A_5. So $\{1\}$ is a conjugacy class of A_5.
$\{(abc)\}-$ this commutes with the odd 2-cycle (de) where $\phi = \{d, e\} \cap \{a, b, c\}$. So $\text{Cent}_{A_5}(abc) = 6/2 = 3$. So, $\text{Cent}_{S_5}(abc) \not\subset A_5$, So, conjugacy class of (abc) has size $60/3 = 20$. Thus, the set $\{(abc)\}$ is a single conjugacy class of A_5.
The centralizer of $(abcde)$ is$\langle(abcde)\rangle \subset A_5$. So the conjugacy class of $(abcde)$ has size $60/5 = 12$. So the S_5 conjugacy class of $\{abcde\}$ splits into 2 conjugacy classes of size 12 in A_5.

Why is A_5 simple? Why are there no interesting homomorphism from A_5 to anywhere else? Notices that a normal subgroup is a union of conjugacy classes. We will compute all the conjugacy classes of A_5 and then show that no non-stupid union of them is a subgroup. Conjugacy classes of A_5:

$$\begin{aligned} \{1\} &- 1 \text{ elment} \\ \{(abc)\} &- 20 \text{ elements} \\ \{(abcde)\} &- 12 \text{ elements, } 12 \text{ elements} \\ \{(ab)(cd)\} &- 15 \text{ elements} \end{aligned}$$

$|\text{conjugacy classes}| \cdot |\operatorname{Cent}| = |G|$
In S_5, have 15 elements of the conjugacy class. So $|\operatorname{Cent} = \frac{120}{15} = 8|$ in A_5.

$$\begin{array}{lll} \operatorname{Cent}_{S_5}[(12)(34)]: & (1) \text{ even} & (34) \text{ odd} \\ & (12) \text{ odd} & (14)(23) \text{ even} \\ & (12)(34) \text{ even} & \dots \end{array}$$

So, $|\text{conjugacy class}| \cdot 4 = 60 \implies |\text{conjugacy class}| = 15$.

Can we make a subgroup out of these?
Let H be a subgroup union of conjugacy classes. Then $1 \in H$ and $|H| \mid 60$. So if $H \neq \{(1)\}$, then we must have $\{(ab)(cd)\}$ in H too or else $|H|$ divides 15, which is impossible. This means $|H| \geq 16$, so $|H| = 20, 30$ or 60. Of these, only 60 is possible.
We will show A_n is simple for $n \geq 5$. Say $H \subset A_n$ is a normal subgroup. $H \neq \{(1)\}$. We will show that $H = A_n$. Pick $\sigma \in H$, $\sigma \neq (1)$. Let $\tau \in A_n$. Since H is normal, $\tau\sigma\tau^{-1} \in H$. Then $\tau\sigma\tau^{-1}\sigma^{-1}$ is a product of 2 3-cycles, so it moves at most 6 things.
Choose τ carefully, we can ensure that $\alpha = \tau\sigma\tau^{-1}\sigma^{-1}$ moves between 2 and 5 things. So, H contains an element that moves between 2 and 5 things. If $\{a, b, c, d, e\}$ is a set that contains all the numbers that α moves, then the subgroup B of A_n that permutes just $\{a, b, c, d, e\}$ is isomorphic to A_5.
But $H \cap B$ is normal in B. So $H \cap B = B$ (since $\alpha \in H \cap B$ and B is simple). So $B \subset H$, so H contains a 3-cycle. This means H contains all 3-cycles because they are all conjugate in S_n, and the class doesn't split in A_n because any 3-cycle commute with any (odd) disjoint 2-cycle. So it is enough to show that A_n is generated by its 3-cycles.

1.14 Sylow's Theorem

Show that A_n is simple for $n \geq 5$. It is enought to show that for $n \geq 5$, the 3-cycles generated A_n. That is, the only subgroup of A_n that contains all 3-cycles is A_n.

Theorem 1.15

The 2-cycles generate S_n, for any $n \geq 1$.

Proof:

We will write $\sigma \in S_n$ as a product of 2-cycles.

$$\sigma = (a_1 \dots a_r)(b_1 \dots b_s)(x_1 \dots, x_x)$$

Disjoint cycle notation works so it's enough to show that any k-cycle is a product of 2-cycles.

$$(a_1 \dots a_m) = (a_1 a_2) \dots (a_{m-2} a_{m-1})(a_{m-1} a_m)$$

To show that every even permutation is a product of 3-cycles. write $\sigma = t_1 \dots t_r$, where t_i is a 2-cycle. The r must be even because σ is even. It's enough to show that the product of any 2 2-cycles is a product 3-cycles.
If $t_1 = t_2$, then $t_1 t_2 = (1)$ is a product of 3-cycles.
If $t_1 \neq t_2$ moves the same number b, then say

$$t_1 = (ab) \text{ and } t_2 = (bc)$$

then

$$t_1 t_2 = (ab)(bc) = (abc)$$

which is a product of 3-cycles. Otherwise, write $t_1 = (ab)$, and $t_2 = (cd)$ for distinct a, b, c, d. Then $(ab)(cd) = (abc)(bcd)$, which is a product of 3-cycles.
This means that A_n is simple for $n \geq 5$. □

What about A_n for $n < 5$?

1. $A_1 : \{(1)\}-$ simple
2. $A_2 : \{(1)\}-$ simple
3. $A_3 : \{(1), (123), (132)\}-$ simple
4. A_4 : has order 12. – NOT simple.
   Consider conjugacy class in S_n:

   $\{(1)\}$ congacy class in A_4

   $\{(abcd)\}$ not in A_4

   $\{(ab)\}$not in A_4

$$\{(ab)(cd)\} - 3 \text{ elements conjugacy class of } A_4 \text{ because } 3/2 \notin \mathbb{Z}$$

$$\{(abc)\} - 8 \text{ elements: cent has order 3 conjugacy class of } A_4$$

Any union of conjugacy class of A_4 that is a subgroup must contain $\{(1)\}$. Possible orders are: $\underset{\checkmark}{1}, \underset{x}{2}, \underset{x}{3}, \underset{?}{4}, \underset{x}{6}, \underset{\checkmark}{12}$.
We say that $H = \{(1), (12)(34), (13)(24), (14)(23)\}$ is a subgroup of A_4. Since it's a union of conjugacy classes, it's a normal subgroup.

Definition 1.20: P-Group

A **p-group** is a group whose order is a power of prime p.

Definition 1.21: P-Sylow Subgroup

Let G be finite group of $p^a m$, where $p \nmid m$. A p-sylow subgroup of G is a subgroup with p^a elements.

Theorem 1.16: Sylow's Theorem

Let G be a group with $p^a m$ elements where $p \nmid m$.

1. G has a p-sylow subrgoup.
2. Any p-subgroup of G is contained in a p-sylow subgroup and any 2 p-sylow subgroups are conjugate.
3. The number N of p-sylow subgroups of G satisfies
   (a) $N \equiv 1 \bmod p$, $N = \#$ of p-sylows
   (b) $N = [G : N(p)]$ divides $|G|$ where $N(p) =$ normalizer of any p-sylow subgroup.

Definition 1.22: Normalizer

Let $S \subset G$ be a subset of G. The **normalizer** of S in G is $N_G(S) = N(S) = \{g \in G \mid gsg^{-1} \in S, \forall s \in S\} = \{g \in G \mid gsg^{-1} = s\}$

In particular, if S is a subgroup, then S is normal in $N(S)$, and any subgroup H of which S is a normal subrgoup satisfies $H \subset N_G(S)$.

Example 1.13

> Let G be a group of order 15. Let H be a 3-sylow subgroup. Then $|H| = 3$. Let K be a 5-sylow subgroup. Then $|K| = 5$. The number of conjugates of $H \equiv 1 \bmod 3$ and divides 15. So H has one conjugate. So H is normal. Similarly, K is normal. Since $\gcd(|H|, |K|) = 1$, we have $H \cap K = 1$.
> Consider $HK = \{hk \mid h \in H, k \in K\}$. If $h_1k_1 = h_2k_2$, then $H \ni h_2^{-1}k_1 = k_2k^{-1} \in K \implies h_2^{-1}h_1 = k_2k_1^{-1} = 1 \implies h_1 = h_2$ and $k_1 = k_2$.

1.15 Isomorphisms of Finite Group

$|G| = 1 \implies G = \{1\}$.
$|G| = 2 \implies G = \langle x \rangle$, for $x \in G$, $x \neq 1$, $\implies G \cong \mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z}$.
$|G| = 3 \implies G$ is abelian $(4 = 2^2)$
If G has an element of x of order 4, then $G = \langle x \rangle \cong \mathbb{Z}/4\mathbb{Z}$. If not, then G has 3 elements of order 2. Let x, y be 2 of them. Then $G = \langle x, y \rangle = \langle x \rangle \langle y \rangle$ and $\langle x \rangle \cap \langle y \rangle = \{1\}$. So $G \cong \langle x \rangle \cap \langle y \rangle \cong \langle x \rangle \times \langle y \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

$|G| = 5 \implies G \cong \mathbb{Z}/5\mathbb{Z}$.
$|G| = 6 \implies$ there is a 2-sylow P_2 and a 3-sylow P_3. The subgroups P_3 is normal because 1 is the only positive intger $\equiv 1 \bmod 3$ that counts at set of order 3 subgroups that fits into a 6-element group. If P_2 is normal. then $G \cong P_2 \times P_3 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}$. If not, then there are 3 conjugates of P_2. Call them A, B, C. Then, G acts on $\{A, B, C\}$ transitively by conjugation, so there is a homomorphism $\phi : G \to S_3$. $\ker\phi$ is the set $\{g \in G \mid gAg^{-1} = A, gBg^{-1} = B, gCg^{-1} = C\}$. The G-orbit has size 3 so stabilizer has size 2. Since $A \subset \mathrm{Stab}(A)$, we gte $A = \mathrm{Stab}(A)$. So $\mathrm{Stab}(A) \cap \mathrm{Stab}(B) = A \cap B = \{1\}$. Thus $\ker\phi = \{1\}$. Thus ϕ is isomorphism and $G \cong S_3$.

$|G| = 7 : G \cong \mathbb{Z}_7$
$|G| = 8$: If G has an element of order 8, then $G = \langle x \rangle$ and $G \cong \mathbb{Z}_8$. If every nontrivial element of G has order 2 then $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.
Say $a, b \in G$, $a \neq 1, b \neq 1$. then $(ab)^2 = 1 \implies abab = 1 \implies aba = b \implies ba = ab$, So G is abelian. So 3 elements a, b, c with $a \neq b \neq c$, $abc \neq 1$ generate subgroups satisfying $G \cong \langle a \rangle \times \langle b \rangle \times \langle c \rangle$.
Now ,say $x \in G$ has order 4. Then $\langle x \rangle$ has index 2 and it's normal.

Theorem 1.17

Let $H \subset G$ be a subgroup of index 2. Then H is normal.

Proof:

> Define $\phi : G \to \{\pm 1\}$ by $\phi(g) = \begin{cases} 1 & \text{if } g \in H \\ 1 & \text{if } g \notin H \end{cases}$. It's easy to check that $\phi(g_1g_2) = \phi(g_1)\phi(g_2)$ if g_1 or g_2 lies in H. If $g_1, g_2 \notin H$, then $g_1g_2 \in H$ because the stabilizer of H under the G-action by left-multiplication is H. Similarly, for $G - H$, so $g_1g_2 \in H$. $g_1(g_2H) = g_1(G - H) - H$. So, $g_1g_2 \in \operatorname{Stab}(H) = H$. So $H = \ker\phi$ is normal. □

So $|\langle 4\rangle|$ and $\langle x\rangle$ is normal. Say $y \notin \langle 4\rangle$. Then $yxy^{-1} = x^a$. So x^a has order 4. That means $a = 1$ or $a = -1$.
If $a = -1$, so $yx = x^{-1}y$. If y has order 2, then $G = \{x, y \mid x^4 = y^2 = 1, yx = x^{-1}y\} \cong D_4$. The only other possibility is that every element of $G - \langle x\rangle$ has order 4. So

$$G = \{\underset{\text{order 1}}{1}, \underset{\text{order 2}}{-1}, \underbrace{x, x^{-1}, y, y^{-1}, z, z^{-1}}_{\text{order 4}}\}$$

Note $-1 = x^2 = y^2 = z^2$, so -1 commutes with every element of G. This is exactly the table for the quaternion group with $x \leftrightarrow i$, $y \leftrightarrow j$, $z \leftrightarrow k$.

$|G| = 9 = 3^2$: Abelian, so $\mathbb{Z}_9$ or $\mathbb{Z}_3 \times \mathbb{Z}_3$. $|G| = 10 : G \cong \mathbb{Z}_{10}$ or $G \cong D_5$.
$|G| = 11 : G \cong \mathbb{Z}_{11}$.
$|G| = 12$: Let $P_2 = 2-$Sylow, $P_3 = 3-$Sylow. If P_2, P_3 both normal $\implies G \cong P_2 \times P_3$, so G is abelian and $G \cong \mathbb{Z}_{12}$ or $\mathbb{Z}_2 \times \mathbb{Z}_6$.
So let's say one of P_2 or P_3 is not normal. If P_3 is not normal, then it has four conjugates. And G acts transitively on the set of 4 conjugates of P_3. So we get a homomorphism $\phi : G \to S_4$. The stabilizer of p_3 is P_3, because

$$|\text{orbit}| \cdot |\operatorname{Stab}| = |G| = 12 \implies 4 \times |\operatorname{Stab}| = 12 \implies |\operatorname{Stab}| = 3$$

Since $P_3 \subset \operatorname{Stab}(P_3)$, we get $P_3 = \operatorname{Stab}(P_3)$. The same is true for each of the conjugates of P_3, namely A, B, C. So

$$\ker\phi = P_3 \cap A \cap B \cap C = \{1\}$$

So, ϕ is injective. Thus $\phi(G)$ is a 12-element subgrop of S_4. Any 12-element subgroup of S_4 has index 2, so it's normal. But we know the normal subgroups of S_4:

$$\{(1)\}, \{(1), (ab)(cd), \underset{\text{only one of order 12}}{A_4}, S_4\}$$

If P_3 is normal, but P_2 isn't, then if $P_2 \cong \mathbb{Z}_4$, then write $P_2 = \langle y\rangle$ and $P_3 = \langle x\rangle$. Since P_3 is normal, $yxy^{-1} = x^a$ for some x. Either $a = 1$, or $a = -1$. If $a = 1$, then $xy = yx$ and G is abelian. So we may assume that $yx = x^{-1}y$. So $G \cong \{x, y \mid x^3 = y^4 = 1, yx = x^{-1}y\}$. To see this, write $\phi : F_2 \to G$ by $\phi(x) = x$, $\phi(y) = y$. If $N \subset F_2$ is the normal subgroup generated by $x^3, y^4, yxy^{-1}x$, then $N \subset \ker\phi$. So ϕ induces $(\tilde{\phi} : F_2/N \to G)$. We want to show that $(\tilde{\phi})$ is an isomorphism. It's clearly onto because $G = \langle x, y\rangle$, It's 1-1 because F_2/N has at most 12 elements. Using $x^3 = y^4 = 1$ and $yx = x^{-1}y$, we can represent any element of F_2/N by $x^a y^b$ for $a \in \{0, 1, 2\}$, and $b \in \{0, 1, 2, 3\}$.

Finally, say P_3 is normal and $P_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Write $P_2 = \{1, a, b, c\}$, where a, b, c have order 2 and $c = ab$, Write $P_3 = \langle x\rangle$. So $axa^{-1} = axa = x^k$ for $k \in \{-1, 1\}$. If $k = 1$, then the group $\langle a, x\rangle$ is abelian with 6 elements, so it's isomorphic to $\mathbb{Z}_6$. So $\langle a, x\rangle = \langle z\rangle$ for some $z \in \langle a, x\rangle$. Now $bzb^{-1} = z^l$, where $l \in \{-1, 1\}$. if $l = 1$, then G is abelian. If $l = -1$, then $G \cong D_6$ because $G \cong \{b, z \mid b^2 = z^6 = 1, bz = z^{-1}b\}$.

If $k = -1$, consider $bzb^{-1} = z^l$. If $l = 1$, the previous argument shows $G \cong D_6$.

If $l = -1$, then $bzb^{-1} = z^{-1}$. So, $czc^{-1} = abzb^{-1}a^{-1} = az^{-1}a^{-1} = z$. So, $G \cong D_6$ by the previous argument.

$|G| = 13 \implies G \cong \mathbb{Z}_{13}$.
$|G| = 14 \implies G \cong \mathbb{Z}_{14}$ or D_4.
$|G| = 15 \implies G \cong \mathbb{Z}_{15}$.

2 Introduction to Rings

2.1 Basic Axioms and Definitions

A **ring** is a bunch of things your can add, subtract, and multiply.

Example 2.0

> - $\mathbb{Z}$: Integers, $\mathbb{R}$: Real numbers, $\mathbb{Q}$: rationals, $\mathbb{C}$: complex numbers.
> - $\mathbb{R}[x, y]$: polynomials in x, y with real coefficients
> - $M_n(\mathbb{R})$: $n \times n$ matices with real entries (not commutative)
> - $\mathbb{Z}/n\mathbb{Z}$: integers mod n.

Definition 2.1: Ring

A ring is a set R with two operations $+ : R \times R \to R$, $\cdot : R \times R \to R$ satisfying for all $a, b, c \in R$,

1. $(a + b) + c = a + (b + c)$.
2. $a + b = b + a$.
3. There exists $0 \in R$ such that $0 + a = a$.
4. There is a $-a \in R$ such that $a + (-a) = 0$.
5. $(ab) \cdot c = a \cdot (bc)$,
6. There exists $1 \in R$ such that $a \cdot 1 = 1 \cdot a = a$.
7. $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$.

Before we prove the subring theorem, here are a couple more defnitions of rings:

Definition 2.2: Commutative Rings

A ring R is commutative **iff** $ab = ba$ for all $a, b \in R$

Definition 2.3: Division Rings

A ring R is a **division ring** iff for all $a \in R, a \neq 0$, there is $a^{-1} \in R$ with $aa^{-1} = a^{-1}a = 1$.

Definition 2.4: Fields

A **field** is a commutative division ring.

Definition 2.5: Unit

An element $a \in R$ is a **unit** iff there is $a^{-1} \in R$ such that $aa^{-1} = a^{-1}a = 1$.

Definition 2.6: Zero Divisor

An element $a \in R$ is a **zero divisor** iff $a \neq 0$ and there is some $b \in R, b \neq 0$, with $ab = 0$ or $ba = 0$.

Definition 2.7: Integral Domain

An integral domain, or **domain** is a ring with **no zero divisors**.

$\mathbb{Z}/6\mathbb{Z}$ is not a domain because

$$2 \neq 0, 3 \neq 0, \text{ but}$$

$$2 \cdot 3 = 6 = 0$$

Now we have a theorem:

Theorem 2.1

Every unit is not a zero divisor.

Proof:

> Say $a \in R$ is a unit. If $ab = 0$, then $b = a^{-1} \cdot 0 = 0$. If $ba = 0$, then $b = 0 \cdot a^{-1} = 0$. So a is not a zero divisor. □

We give some examples of units/zero divisors of rings. Consider

- $\mathbb{Z}$: units are $\{1, -1\}$
- $\mathbb{Q}$ is a field, and so are $\mathbb{R}, \mathbb{C}$.
- $M_n(\mathbb{R})$: if $n \geq 2$, $\begin{pmatrix} 0 & \cdots & 0 & 1 \\ 0 & \cdots & 0 & \vdots \\ 0 & \cdots & 0 & 0 \end{pmatrix}^2 = 0$. Units are $GL_n(\mathbb{R})$.
- $\mathbb{R}[x]$: no zero divisors. Units are nonezero constants.

2.2 Subring Theorem

Next, we proceed to the subring theorem so that we don't need to check all axioms of rings.

Definition 2.8: Subring

A **subring** of a ring R is a subset $S \subset R$ that is a ring using the same $+, \cdot$, and 1 as R.

Theorem 2.2: Subring Theorem

A subset $S \subset R$ of a ring R is a subring iff

1. $1 \in S$
2. S is closed under subtraction $-$, that is, $a, b \in S \implies a - b \in S$
3. S is closed under multiplication $\cdot$, that is, $a, b \in S \implies ab \in S$

Proof:

($\Rightarrow$) If S is a subring, then $(1), (2), (3)$ are trivially satisfied.

($\Leftarrow$) So assume S satisfies (1), (2), and (3).
First, note that $\cdot : S \times S \to S$ is well defined by (3).
Since $1 \in S$, by (2), we get $0 = 1 - 1 \in S$, so $-1 = 0 - 1 \in S$.
So if $a, b \in S$, then $-b \in S$ by (3), so $a + b = a - (-b) \in S$, and hence we also have $+ : S \times S \to S$.
Associativity of $+$ and $\cdot$ and commutativity of $+$ are immediately true for S.
Same for distributivity. Existence of 0, additive inverse, and 1 in S follows from (1) and previous discussion.

□

Example: Let $R = \mathbb{C}$, let S be:

$$S = \{a + b\gamma + c\gamma^2 + d\gamma^3 + e\gamma^4 \mid a, b, c, d, e \in \mathbb{Z}, \gamma = e^{\frac{2\pi i}{5}}\}$$

We have $\gamma^5 = 1, \gamma \neq 1$ (We usually write $S = \mathbb{Z}[]$).
By Subring Theorem:

1. $1 \in S$, becasue you can pick $a = 1$, $b, c, d, e = 0$
2. trivial

3. say $x, y \in S$,

$$x = a + b\gamma + c\gamma^2 + d\gamma^3 + e\gamma^4$$

$$y = a' + b'\gamma + c'\gamma^2 + d'\gamma^3 + e'\gamma^4$$

   xy = sum of terms of the form (integers)$\cdot\gamma^n$ for some $n \in \mathbb{Z}_{\geq 0}$. Since $\gamma^5 = 1$, (integer)$\cdot\gamma^n$ can always be written with $n \in \{0, 1, 2, 3, 4\}$.

So S is a subring of $\mathbb{C}$.

2.3 Homomorhisms

Definition 2.9: Homomorphism of Ring

A **homomorphism of rings** is a function $f : R \to T$ such that

1. f(1) = 1
2. $f(ab) = f(a)(b)$
3. $f(a + b) = f(a) + f(b)$

Note: (1) is a must: consider $f(n) = (n, 0)$, we have $f(1)^2 = f(1)$, so it can't be derive with (2).

Definition 2.10: Isomorphism

An **isomorphism** is a homomorphism with an inverse homomorphism.

Theorem 2.3

A homomorphism of rings is an isomorphism **iff** it's a bijection.

Examples of homomorphism:

1. $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $f(a, b) = a$
2. $f : \mathbb{R}[x] \to \mathbb{C}$, where

$$f(p(x)) = p(i)$$

$$f(x^2 + 1) = i^2 + 1 = 0$$

$$f(x^3 + 3x^2 + x - 7) = i^3 + 3i^3 + i - 7 = -10$$

   This is a homomorphism, and it's onto.
   In fact, plugging stuff in for the variables is always a hom. from a polynomial ring.

Definition 2.11: Image, Kernel

The **image** of a hom. $\phi : R \to T$ is

$$im(\phi) = \{t \in T \mid t = \phi(r) \text{ for some } r \in R\}$$

The **kernel** of ϕ is

$$ker\phi = \{r \in R \mid \phi(r) = 0\}$$

Theorem 2.4

$im\phi$ is a subring of T. $ker\phi$ is not a subring of R.

Proof:

$1 \in Im\phi$ because $1 = \phi(1)$. If $a, b \in Im(\phi)$, then

$$a = \phi(r_1), b = \phi(r_2)$$

so $a - b = \phi(r_1 - r_2) \in Im\phi$ and $ab = \phi(r_1, r_2) \in Im\phi$.
So $Im\phi$ is a subring.
However, if $1 \in ker\phi$, then

$$\phi(1) = 0 \implies \phi(a) = \phi(a)\phi(1) = 0$$

for all $a \in R$, and $\phi(1) = 1$, so $0 = 1$, which is not allowed. So $ker\phi$ is not a subring of R.

□

2.4 R-module

An R-module is a bunch of things you can add, subtract, and multiply by elements of R. Although $ker\phi$ is not a subring of R, it is an **R-module**.

Definition 2.12: R-module

Let R be a ring. An R-module is an abelian group M with a function $\cdot : R \times M \to M$ satisfying:

1. $(r_1 + r_2)m = r_1 m + r_2 m$
2. $r \cdot (m_1 + m_2) = (r \cdot m_1 + r \cdot m_2)$
3. $r_1 \cdot (r_2 \cdot m) = (r_1 r_2) \cdot m$

From now on, every ring we deal with will be commutative.

Example 2.1

- If $R = \mathbb{R}$, then an R-module is exactly the same thing as an $\mathbb{R}$-vector space. In fact, if R is a field, then R-module is exactly the same thing as an R-vector space.
- $2\mathbb{Z} = \{\text{even integers}\}$ is a $\mathbb{Z}$-module.
- $\mathbb{Z}/6\mathbb{Z}$ is a $\mathbb{Z}$-module.

Theorem 2.5: Submodule Theorem

A subset of S of an R-module M is an R-submodule of M iff

1. $0 \in S$
2. S is closed under $-$
3. S is closed under $\cdot$

Proof:

Same as other subxx theorems. □

Definition 2.13: Submodule

A **submodule** of an R-module M is a subset $S \subset M$ that is an R-module using the same operations $+, -, \cdot$ as M.

2.5 Properties of Ideals

Definition 2.14: Ideal

An **ideal** of R is an R-submodule of R.

For example, $2\mathbb{Z}$ is an ideal of $\mathbb{Z}$. We showed last time that if $\phi : R \to T$ is an homomorphism, then $ker\phi$ is an ideal of R. Is is true that every ideal of R is the kernel of some homomorphism.

Answer: YES. Take the quotient. Let's say $I \subset R$ is an ideal. We want to find homomorphism $\phi : R \to T$ with $ker\phi = I$. If we had such a ϕ and such a T, then

$$\phi^{-1}(0) = I$$

$$\phi^{-1}(1) = 1 + I$$

$$\phi^{-1}(t) = r + I$$

where $\phi(r) = t$. So defind R/I to be

$$\{r + I \mid r \in R\}$$

with

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

$$(r_1 + I)(r_2 + I) = r_1r_2 + I$$

and $1 + I$ is the mult. identity. It is proven in the textbook that R/I is a ring. R/I is not a subring of R.

Theorem 2.6: Universal Property of Quotients

Let $\phi : R \to T$ be a homomorphism, $I \subset R$ an ideal. Then

$$\begin{tikzcd} R \arrow[r, "\phi"] \arrow[d, "q"'] & T \\ R/I \arrow[ur, dashed, "\tilde{\phi}"'] & \end{tikzcd}$$

there exists a homomorphism $\hat{\phi} : R/I \to T$ statisfying $\phi = \hat{\phi} \circ q$ iff $I \subset ker\phi$.
$q : R \to R/I$ is the reduce mod I homomorphism. Furthermore, $im\hat{\phi} = im\phi$ and $ker\hat{\phi} = q(ker\phi) = ker\phi$ "mod I"

Example 2.2

> $\mathbb{R}[x] = \{\text{polys in } x \text{ with real coefficients}\}$
> $I = \{p(x)|p(1) = 0\}$ is an ideal.
> What does $\mathbb{R}[x]/I$ look like?
> Define $\phi : \mathbb{R}[x] \to R$
>
> $$\phi(p(x)) = p(1)$$
>
> so $\phi(x^2 + 1) = 1^2 + 1 = 2$ and $\phi(2x - 7) = 2 - 7 = -5$.
> It is easy to see that $ker\phi = I$. Therefore, by the UPQ, $\hat{\phi} : \mathbb{R}[x]/I \to R$ has image $\mathbb{R}$ and kernel 0 mod I. So $\hat{\phi}$ is $1 - 1$ and onto, so it's an isomorphism. (A ring hom. ϕ is one-to-one iff $ker\phi = \{0\}$).

Theorem 2.7

A ring homomorphism is $1-1$ **iff** its kernel is 0.

Proof:

If $\phi : R \to T$ is injective, then $ker\phi = \{0\}$, trivially. So assume $ker\phi = \{0\}$. Say $\phi(a) = \phi(b)$, We want to show $a = b$. Well, $\phi(a-b) = 0$. so $a - b \in ker\phi \Rightarrow a = b$. □

Definition 2.15: Maximal Ideal

An ideal $I \subset R$ is maximal iff $I \neq R$ and if $J \subset R$ is an ideal with $I \subset J \subset R$, then either $J = I$ or $J = R$.

Example 2.3

Let $R = \mathbb{Z}$. What are the ideals of R?

Say $I \subset \mathbb{Z}$ is an ideal. If $I \neq (0)$, then there is some $n \in I, n \neq 0$. Let's choose the smallest positive $n \in I$.

Claim: $I = n\mathbb{Z}$.

Proof of claim: Certainly $n\mathbb{Z}$ is contained in I. We just need to show $I \subset n\mathbb{Z}$. Say $x \in I$. Write

$$x = qn + r$$

where $r, q \in \mathbb{Z}$, $0 \leq r < n$. Then $r = x - qn \in I$. Since $r < n$, we have $r \leq 0$, so $r = 0$. So $x = qn \in n\mathbb{Z}$.

So every ideal of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for some $n \in \mathbb{Z}$. And $n\mathbb{Z} \subset k\mathbb{Z}$ iff $k \mid n$. So $n\mathbb{Z} \subset \mathbb{Z}$ is maximal iff n is prime.

Definition 2.16: Generated Ideal

Let R be a ring, $S \subset R$ be any subset. The **ideal generated** by S the intersection of all ideals that contains S. It's written as (S).

More concretely,

$$(S) = \{r_1 s_1 + \ldots + r_n s_n \mid r_i \in R, s_i \in S\}$$

When $S = \{x\}$, then

$$(x) = \{rx \mid r \in R\}$$

Example 2.4

1. $(1) = R$

2. $(6, 8) \subset \mathbb{Z}$.

$$(6, 8) = \{a6 + b8 \mid a, b \in \mathbb{Z}\}$$

We know this is (n) for some $n \in \mathbb{Z}$. Since $2 = 8 - 6 \in (6, 8)$ we have $(2) \subset (6, 8)$. But $6, 8 \in (2)$, so $(6, 8) \subset (2)$, so $(6, 8) = (2)$.

Theorem 2.8

An ideal $I \subset R$ is maximal **iff** R/I is a field.

Proof:

We'll start by proving

Lemma 2.9

The ideals of R/I are precisely the reductions mod I of ideals of R that contain I.

Proof:

Say $J \subset R$ is an ideal with $I \subset J$. Then if $q : R \to R/I$ is the quotient homomorphism, $q(J)$ is an ideal of R/I because homs. map ideals to ideals.
Conversely, if $\bar{J}$ is an ideal of R/I, define

$$J = \{r \in R \mid q(r) \in J\} = q^{-1}(J)$$

This is an ideal: $0 \in J$ since $q(0) = 0 \in \bar{J}$.
If $x, y \in J$, then

$$q(x - y) = q(x) - q(y) \in \bar{J}$$

so $x - y \in J$.
If $r \in R$ and $x \in J$, then we want $rx \in J$. But $q(rx) = q(r)q(x) \in \bar{J}$, so $rx \in J$.
Finallly, note that if $x \in I$, then $q(x) = 0 \in \bar{J}$, so $x \in J$.
Moreover, if $\bar{J}_1 \neq \bar{J}_2$, then $J_1 \neq J_2$ because q is onto. □

(⇒) R/I is a field. We want to show that $I \subset R$ is maximal. First, note that any ideal that contains a unit must be the whole ring. Any nonzero ideal of R/I contains a unit, so it's R/I. (If $a \in I$ is a unit, then $\frac{1}{a}(a) \in I$, so $1 \in I$, so $r \cdot 1 \in I$ for all $r \in R$). So R/I has 2 ideals, R/I and (0). So by the lemma, the only ideals of R that contains I are I and R. So I is maximal.

(⇐) Conversely, assume I is maximal. We want to show that R/I is a field. By the lemma, R/I has exactly 2 ideals, (0) and R/I. Let $x \in R/I$ be any nonzero element. Then $(x) = R/I$, so $1 = rx$ for some $r \in R/I$. So x is a unit, and R/I is field. □

The maximal ideals of $\mathbb{Z}$ are the ideals (p) for p prime. So $\mathbb{Z}/n\mathbb{Z}$ is a field **iff** n is prime.

Example 2.5

> Say F is a field. What are the maximal ideals of $F[x]$? First, say $I \subset F[x]$ is an ideal. We could have $I = (0)$. If not, then there is some $p(x) \in I$ for $p(x) \neq 0$. Let $p(x) \in I$ for $p(x) \neq 0$. Let $p(x)$ be a nonzero polynomial of minimal degree. We'll show $I = (p(x))$. Say $q(x) \in I$, we want to show $q(x) = t(x)p(x)$ for some $t(x) \in F[x]$.
>
> $$q(x) = t(x)p(x) + r(x)$$
>
> where $deg(r(x)) < deg(p(x))$. But $r(x) = q(x) - t(x)p(x) \in I$, so by minimality of $deg(p)$, we have $r(x) = 0$ and
>
> $$q(x) = t(x)p(x)$$
>
> so $I = (p(x))$.

We proved R/I is a field **iff** I is a maximal ideal **iff** R/I has only two ideals (0) and (1).

Theorem 2.10

Let $\phi : F \to T$ be a homomorphism, where F is a field. Then ϕ is injective.

Proof:

> $ker\phi$ is an ideal of F. So $ker\phi = (0)$ or (1). But $\phi(1) = 1 \neq 0$. So $ker\phi = (0)$. □

Reminder: A domain is a ring with no zero divisors; that is, if $ab = 0$, then $a = 0$ or $b = 0$. So R/I is a domain iff $ab \equiv 0 \bmod I \implies a \equiv 0 \bmod I$ or $b \equiv 0 \bmod I$ iff $ab \in I \implies a \in I$ or $b \in I$.

Definition 2.17: Prime Ideal

An ideal $I \subset R$ is prime iff for all $a, b \in R$ with $ab \in I$, either $a \in I$ or $b \in I$.

Theorem 2.11

R/I is a domain iff I is a prime ideal.

Proof:

> We just did it. □

Example 2.6

> What are the prime ideals of $\mathbb{Z}$? $n\mathbb{Z} = (n)$ is maximal iff n is prime. $n\mathbb{Z}$ is prime iff n is prime or $n = 0$.

2.6 Principal Ideal Domain

Definition 2.18: Principal Ideal Domain

A principle ideal domain is a domain D such that every ideal of D can be generated by one element.

Example 2.7

> 1. $\mathbb{Z}$ is a PID.
>
> 2. $F[x]$, F is a field, x a variable, is a PID.

Let R be any ring. There is a unique hom. $\phi : \mathbb{Z} \to R$, called the characteristic homomorphism, defined by

$$\phi(n) = \begin{cases} \underbrace{1+1+\ldots+1}_{\times n} & n \geq 0 \\ \underbrace{-(1+1+\ldots+1)}_{\times -n} & n < 0 \end{cases}$$

The kernel of ϕ is $n\mathbb{Z}$ for some $n \in \mathbb{Z}$, we might as well assume $n \geq 0$, because $n\mathbb{Z} = -n\mathbb{Z}$. The value of n is called the characteristic of R.

Example 2.8

> 1. If $R = \mathbb{Z}$, then char$\mathbb{Z} = 0$, because the characteristic hom. is the identity hom. which is $1-1$.
>
> 2. If $R = \mathbb{Q}$, char$\mathbb{Q} = 0$
>
> 3. $\mathbb{Z}/n\mathbb{Z}$ has characteristic n.
>
> 4. $\mathbb{Z}/3\mathbb{Z}[x]$ has characteristic

facts: If D is a domain then $im\phi$ is also a domain. So $ker\phi$ is a prime ideal of $\mathbb{Z}$, so char$D = 0$ or prime (converse if not true!).

Let's say R is a ring, T a ring that contains R, $\alpha \in T$ some element. Then

$$R[\alpha] = \{a_n\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_0 \mid a_i \in R, n \in \mathbb{Z}\}$$

Example 2.9

1. $\mathbb{Z}[\zeta_5], \zeta_5 = e^{\frac{2\pi i}{5}}$.

$$\begin{aligned}\mathbb{Z}[\zeta_5] &= \{a_n\zeta_5^n + \ldots + a_0 \mid a_i \in \mathbb{Z}\}\\ &= \{a_0 + a_1\zeta_5 + a_2\zeta_5^2 + a_3\zeta_5^3 + a_4\zeta_5^4 + a_5\zeta_5^5 \mid a_i \in \mathbb{Z}\}\end{aligned}$$

$$x_5 + 1 \to 2(x = \zeta_5)$$

$$x + 1 \to 1 + \zeta_5(x = \zeta_5)$$

2. $\mathbb{Z}[i]$

$$\begin{aligned}\mathbb{Z}[i] &= \{a_n i^n + \ldots + a_0 \mid a_i \in \mathbb{Z}\}\\ &= \{a_1 i + a_0 \mid a_1 \in \mathbb{Z}\}\end{aligned}$$

3. $\mathbb{Z}[\sqrt{2}, \sqrt{3}]$.

$$\begin{aligned}\mathbb{Z}[\sqrt{2}, \sqrt{3}] &= \{p(\sqrt{2}, \sqrt{3}) \mid p(x, y) \text{ polynomials with coefficients in } \mathbb{Z}\}\\ &= \{a_0 + a_{10}\sqrt{2} + a_{01}\sqrt{3} + a_{11}\sqrt{6}\}\end{aligned}$$

Quiz 8:
The ideal of $(p(x))$ is maximal iff there are no ideals T with $p(1) \subsetneq J \subsetneq F[x]$. But $(p(x)) \subset (q(x))$ iff $q(x) \mid p(x)$, so $(p(x))$ is maximal iff $p(x)$ has no nontrivial factors in $F[x]$.

Definition 2.19: Irreducible

A polynomial $p(x) \in F[x]$ is irreducible iff $p(x)$ is not constant and has no nontrivial factors.

so $(p(x))$ is maximal iff $(p(x))$ is irreducible. $(p(x))$ is prime iff $p(x)$ is irreducible or 0.
Note: Two different polynomials can represent the same function. x^3 and x represents the same function in $\mathbb{F}_3[x]$, but they are different polynomial ($\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$).

2.7 Properties of R-modules

If F is a field, then an F-module is an F-vector space.

Definition 2.20: R-module Homomorhisms

An R-module **homomorphism** is a function $\phi : M \to N$, where M, N are R-modules satisfying

1. $\phi(rm) = r\phi(m)$
2. $\phi(m_1 + m_2) = \phi(m_1) + \phi(m_2)$

Example 2.10

1. An F-module homomorphism is an F-linear transformation if F is a field.
2. $R = \mathbb{Z}$, $\phi : \mathbb{Z}_{12} \to \mathbb{Z}_3$ such that
$$\phi(n) = n \mod 3$$
3. $\phi : \mathbb{Z}^2 \to \mathbb{Z}^2$ such that
$$\phi(a, b) = (a + b, a - b)$$
This is a $\mathbb{Z}$-module homomorphism. It's 1-1 but not onto.

Theorem 2.12

If $\phi : M \to N$ is an R-module homomorphism, then $\ker \phi$ is an R-submodule of M and $\operatorname{im} \phi$ is an R-submodule of N.

Proof:

We want to show that $\ker \phi$ is closed under $+, -$ and $\cdot$, and isn't empty.

$$\phi(0) = 0 \Rightarrow 0 \in \ker \phi$$

Say $m_1, m_2 \in \ker \phi$. Then

$$\phi(m_1 \pm m_2) = \phi(m_1) \pm \phi(m_2) = 0$$

so $m_1 + m_2 \in \ker \phi$. And $m \in \ker \phi$, $r \in R \implies \phi(rm) = r\phi(m) = 0$ so $rm \in \ker \phi$. Similarly, we have $\phi(0) = 0$ so $0 \in \operatorname{im} \phi$. If $n_1, n_2 \in \operatorname{im} \phi$, then $n_1 = \phi(m_1)$, $n_2 = \phi(m_2)$ for some $m_1, m_2 \in M$, so
$$n_1 \pm n_2 = \phi(m_1 \pm m_2)$$
and if $r \in R$, $n \in \operatorname{im} \phi$, $n = \phi(m)$, so $rn = \operatorname{im} \phi(rm)$. □

Question: Is every R-submodule of M the kernel of a homomorphism?
Answer: Yes! This involves quotients, again. Say $N \subset M$ is an R-submodule. We want to define M/N as an R-module. First define the set M/N and the $+, -$ using the quotient of abelian groups.
The last step is to define multiplication by elements of R. Let's try

$$r(m+N) = rm + N$$

If $m + N = m' + N$, then

$$rm - rm' = r(\underbrace{m - m'}_{\in N})$$

because N is an R-module. So $rm + N = rm' + N$. Thus our multiplication is well defined. It is now straightforward to show that M/N is an R-module with this multiplication (M/N is NOT an R-submodule of M).

Theorem 2.13: Universal Property of Quotients

There exists $\tilde{\phi} : M/N \to L$ such that $\phi = \tilde{\phi} \circ q$ **iff** $N \subset \ker \phi$.

$$\begin{tikzcd} M \arrow[r, "\phi"] \arrow[d, "q"] & L \\ M/N \arrow[ur, "\tilde{\phi}"] & \end{tikzcd}$$

Moreover, $\operatorname{im} \tilde{\phi} = \operatorname{im} \phi$, $\ker \tilde{\phi} = \ker \phi + N$.

Proof:

($\Rightarrow$) Trivial, if $\tilde{\phi}$ exists and $\phi = \tilde{\phi} \circ q$, then $N = \ker q \subset \ker \phi$.

($\Leftarrow$) Define $\tilde{\phi} : M/N \to L$ by $\tilde{\phi}(m + N) = \phi(m)$.
Check well defined: if $m + N = m' + N$

$$\tilde{\phi}(m+N) = \phi(m)$$
$$\tilde{\phi}(m'+N) = \phi(m')$$

and $m - m' \in N \subset \ker \phi \Rightarrow \phi(m - m') = 0 \Rightarrow \phi(m) = \phi(m')$. It is now straightforward to see that $\tilde{\phi}$ is a homomorphism with $\phi = \tilde{\phi} \circ q$. Since q is onto, $\operatorname{im} \phi = \operatorname{im} \tilde{\phi}$. Moreover, $m \in \ker \phi$ iff $\phi(m) = 0$ iff $\tilde{\phi}(q(m)) = 0$ iff $q(m) \in \ker \tilde{\phi}$. □

Note that ring homomorphism and R-module homomorphism are not the same thing:
Ring hom:

$$\phi(a \pm b) = \phi(a) \pm \phi(b)$$

$$\phi(1) = 1$$

$$\phi(ab) = \phi(a)\phi(b)$$

R-module homomorphism:

$$\phi(a \pm b) = \phi(a) + \phi(b)$$

$$\phi(rm) = r\phi(m)$$

Example 2.11

> $\mathbb{C}$ is a $\mathbb{C}$-module and a ring.
>
> $$\phi(a + bi) = a - bi$$
>
> This is a ring homomorphism, but not a $\mathbb{C}$-module homomorphism.

Definition 2.21

Let M be an R-module, $S \subset M$ a subset. The R-module generated by S is

$$\{r_1 s_1 + \cdots + r_n s_n \mid s_i \in S, r_i \in R\}$$

Also somtimes called the R-span of S.

Example 2.12

> 1. If R is a field, then the module generated by S is literally the span of S.
> 2. $R = \mathbb{Z}$, $M = \mathbb{Z}/20\mathbb{Z}$, $S = \{4, 5\}$. Then the submodule generated by S is
>
> $$\{4a + 5b \mid a, b \in \mathbb{Z}\} \subset \mathbb{Z}/20\mathbb{Z} = \mathbb{Z}/20\mathbb{Z}$$
>
>   because any element of $\mathbb{Z}/20\mathbb{Z}$ is of the form $4a + 5b$.
> 3. If $M \subset R$, then M is an ideal of R, and the R-submodule generated by S is just the ideal generated by S.

If $S = \{s_1, \ldots, s_r\}$ is finite, then the R-module generated by S is written

$$Rs_1 + Rs_2 + \ldots + Rs_r$$

Definition 2.22: Free R-module

Let S be a set. The free R-module on S is the set

$$\{r_1 s_2 + \cdots + r_n s_n \mid r_i \in R, s_i \in S\}$$

with

1. $(r_1 s_1 + \cdots r_n s_n) + (r_1' s_1' + \cdots + r_m' s_m') = r_1 s_1 + \cdots + r_1' s_1' + \cdots + r_m' s_m'$
2. $(r_1 s_2 + \cdots + r_n s_n) - (r_1' s_1' + \cdots + r_m' s_m') = (r_1 s_2 + \cdots + r_n s_n) + (-r_1') s_1' + \cdots + (-r_m') s_m'$
3. $r(r_1 s_1 + \cdots + r_n s_n) = (r r_1) s_1 + \cdots (r r_n) s_n$

Example 2.13

> The free $\mathbb{Z}$-module on
>
> $$\{\text{John, Paul, George, Ringo}\}$$
>
> is
>
> $$\{a(\text{John}) + b(\text{Paul}) + c(\text{George}) + d(\text{Ringo}) \mid a, b, c, d \in \mathbb{Z}\}$$

Say M is an R-module, say M is generated by S. Let F be the free R-module on S. There exists a homomorphism $\phi : F \to M$ given by

$$\phi(r_1 s_2 + \cdots r_n s_n) = r_1 s_1 + \cdots + r_n s_n \in M$$

because S generates M, ϕ is onto. Thus ϕ induces an isomorphism $\tilde{\phi} : F / \ker \phi \to M$.

Example 2.14

> If $M = \mathbb{Z}/20\mathbb{Z}$, $R = \mathbb{Z}$, $S = \{4, 5\}$.
>
> $$F = \{a(4) + b(5) \mid a, b \in \mathbb{Z}\} \cong \mathbb{Z}^2 \cong \{a(\text{four}) + b(\text{five}) \mid a, b \in \mathbb{Z}\}$$
>
> $\phi(a(4) + b(5)) = 4a + 5b \bmod 20$. ϕ is onto – what is $\ker \phi$?
>
> $$-5(4) + 4(5) \in \ker \phi$$
>
> $$5(4) \in \ker \phi$$
>
> so $\ker \phi$ contains $5(4), 4(5)$. We claim $\ker \phi$ is generated by these two elements.
> Let $N = \mathbb{Z}[5(4)] + \mathbb{Z}[4(5)]$. Then mod N, every element of F is congruent to $x(4) + y(5)$ for $x \in \{0, 1, 2, 3, 4\}$, $y \in \{0, 1, 2, 3\}$. So F/N has at most 20 elements. And F/N surjects

onto $\mathbb{Z}/20\mathbb{Z}$, so it has at least 20 elements, so $|F/N| = 20$, and so $N = \ker\phi$.

$\mathbb{Z}[\zeta_5]$ is the free $\mathbb{Z}$-module on $\{1, \zeta_5, \zeta_5^2, \zeta_5^3, \zeta_5^4\}$, but as a ring, $\mathbb{Z}[\zeta_5]$ is generated by ζ_5.

2.8 Fundamental Theorem of Finitely Generated Abelian Group

Recall that R-module generated by $m_1, \dots, m_r$ is

$$M = Rm_1 + Rm_2 + \cdots + Rm_r = \{r_1 m_1 + \cdots + r_r m_r \mid r_i \in R, m_i \in M\}$$

What do abelian groups look like if they are finitely generated? That is, if A is an abelian group with $A = \langle g_1, \dots, g_n \rangle$. What is A like? We will find a list of abelian groups such that every group is isomorphic to exactly one of the groups on the list.

Fact: Every abelian group is a $\mathbb{Z}$-module, and vice versa.
What is $\mathbb{Z}^2/X$?

$$X = \text{span}\left\{\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix}\right\}$$

Could choose

$$\left\{\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}\right\} = B$$

as a basis of $\mathbb{Z}^2$. Then

$$X = \text{span}\left\{\begin{pmatrix} 1 \\ 0 \end{pmatrix}_B, \begin{pmatrix} -1 \\ 2 \end{pmatrix}_B\right\}$$

and

$$X = \text{span}\left\{\begin{pmatrix} 1 \\ 0 \end{pmatrix}_B, \begin{pmatrix} 0 \\ 2 \end{pmatrix}_B\right\}$$

So

$$\mathbb{Z}^2/X \cong (\mathbb{Z}/2\mathbb{Z})$$

The trick was simply to find the bases of $\mathbb{Z}^2$ and of X

$$\mathbb{Z}^2 = \{(a, b)\}$$

$$X = \{(a, 2b)\}$$

Theorem 2.14: Fundamental Theorem of Finitely Generated Abelian Group

Let A be a finitely generated abelian group, r the rank of A. Then

$$A \cong \mathbb{Z}^r \times (\mathbb{Z}/p_1^{a_1}\mathbb{Z}) \times (\mathbb{Z}/p_2^{a_2}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_m^{a_m}\mathbb{Z})$$

where the p_i are prime, $a_1, \ldots, a_m, r \in \mathbb{Z}_{\geq 0}, a_1, \ldots, a_m > 0$. Moreover, this expression is unique up to permutation of $p_i^{a_i}$.

Proof:

Say $A = \langle g_1, \ldots, g_m \rangle$. Then there is a homomorphism $\phi : \mathbb{Z}^m \to A$ given by $\phi(x_1, \ldots, x_m) = x_1 g_1 + \cdots + x_m g_m$. ϕ is onto because $A = \langle g_1, \ldots, g_m \rangle$. So $A \cong \mathbb{Z}^m / \ker \phi$ by the First Isomorphism Theorem (or UPQ). So let's understand this quotient.

Lemma: Let $N \subset \mathbb{Z}^r$ be a subgroup. Then $N \cong \mathbb{Z}^k$ for some $k \geq 0$.

Proof:

We proceed by induction on k. $k = 0$ is trivial, and $k = 1$ we already did.
Let $M = N \cap (\mathbb{Z} \times \{\vec{0}\}) = \{(*, 0, \ldots, 0) \in N\}$. Then $M = l\mathbb{Z} \times \vec{0}$ for some $l \in \mathbb{Z}$.
Let $\phi : \mathbb{Z}^r \to \mathbb{Z}^{r-1}$ be $\phi(a_1, \ldots, a_r) = (a_2, \ldots, a_r)$. Then $\phi(N) \subset \mathbb{Z}^{r-1}$. By induction, $\phi(N) \cong \mathbb{Z}^t$ for some t. So $\phi(N) = \sum z_i \vec{y_i}$ (lattice combination) for $z_i \in \mathbb{Z}$ for some $\vec{y_i} \in \mathbb{Z}^{r-1}$ with $\{\vec{y_i}\}$ linearly indenpendent.
For each i, choose $\vec{z_i} \in N$ such that $\phi(\vec{z_i}) = \vec{y_i}$, so $\vec{z_i} = (*, \vec{y_i})$. For any $\vec{v} \in N$, we can write $\vec{v}$ as a $\mathbb{Z}$-linear combination of the $\vec{z_i}$, except maybe the first coordinate is wrong. In other words, there are $a_1, \ldots, a_t$ in $\mathbb{Z}$ such that

$$\begin{aligned} \vec{v} - (a_1 \vec{z_1} + \ldots a_t \vec{z_t}) &= (*, 0, \ldots, 0) \in N \in M \\ &= n(l, 0, \ldots, 0) \text{ for some } n \in \mathbb{Z} \\ &= n\vec{z}_{t+1} \end{aligned}$$

If $l = 0$, then this shows that $\{\vec{z_1}, \ldots, \vec{z_t}\}$ is a basis of N.
If $l \neq 0$, then set $\vec{z}_{t+1} = (l, 0, \ldots, 0)$. We get a basis $\{\vec{z_1}, \ldots, \vec{z}_{t+1}\}$ of N.
So N has a $\mathbb{Z}$-basis, and is therefore isomorphic to $\mathbb{Z}^t$ or $\mathbb{Z}^{t-1}$ depending on if l is 0 or not. □

by the lemma, $\ker \phi$ has basis $\{\vec{y}_1, \ldots, \vec{y}_t\}$. Consider the matrix

$$\begin{pmatrix} \vec{y}_1 & \cdots & \vec{y}_t \end{pmatrix} = Y$$

Row operations on Y will rewrite the columns in a different baiss of $\mathbb{Z}^m$. Column operations will change the basis of $\ker \phi$ to a different basis of $\ker \phi$. So performing row and column

operations on Y will not change the isomorphism type of A. So permute to row 1 the row with the with the smallest nonzero entry in col 1 (in absolute value). Use row operations to reduce all the other entries in col 1 to less than the top entry. Keep doing this until all entries in col 1 are zero except the first one. Then use column operations to do the same for col 1. We want the upper left entry to be the only nonzero entry in the first row. If necessary, go back and fix col 1 again. Repeat until all of row 1 and rol 1 are 0 except the upper left. This process ends because the upper left alwats goes down (in abs value) with each iteration and it's an integer.
Now repeat on the smaller matrix B_i. Eventually, you get

$$\begin{pmatrix} d_1 & & & \\ & d_2 & & \\ & & \ddots & \\ & & & d_t \end{pmatrix}$$

where the d_i are integersm so now

$$A \cong (\mathbb{Z}/d_1\mathbb{Z}) \times \ldots \times (\mathbb{Z}/d_t Z)$$

If $d_i = 0$, then $\mathbb{Z}/d_i\mathbb{Z} = \mathbb{Z}$, so $A \cong \mathbb{Z}^r \times (\mathbb{Z}/e_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/e_k\mathbb{Z}) \cong \mathbb{Z}^r \times (\mathbb{Z}/p_1^{a_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_n^{a_n}\mathbb{Z})$ by the Chinese Remainder Theorem.
To show the uniqueness of representation, define $T \subset A$ by

$$T = \{a \in A \mid na = 0 \text{ for some } n > 0\}$$

If $A \cong A'$, then $A/T \cong A'/T$. Write $A \cong \mathbb{Z}^r \times T$, $A' \cong \mathbb{Z}^{r'} \times T \Rightarrow \mathbb{Z}^r \cong A/T \cong A'/T \cong \mathbb{Z}^{r'} \Rightarrow r = r'$.
All that's left of the proof of the Fundamental Thoerme of F.G. Abelian Groups is to show that if $(\mathbb{Z}/p_1^{a_1}\mathbb{Z} \times \cdots \times (\mathbb{Z}/p_r^{a_r}\mathbb{Z}))$ is isomorphic to $(\mathbb{Z}/p_1'^{a_1'}\mathbb{Z} \times \cdots \times (\mathbb{Z}/p_r'^{a_r'}\mathbb{Z}))$, then the multisets

$$\{p_1^{a_1}, \ldots, p_r^{a_r}\} = \{p_1'^{a_1'}, \ldots, p_r'^{a_r'}\}$$

are equal.
Define $T_p = \{g \in A \mid g \text{ has order } p^n \text{ for some } n\}$. Define similarly for A'. It is enough to show $T_p \cong T_p'$,

$$\underbrace{(\mathbb{Z}/9\mathbb{Z})}_{T_3} \times \underbrace{(\mathbb{Z}/7\mathbb{Z}) \times (\mathbb{Z}/49\mathbb{Z})}_{T_7}$$

because $T \cong \Pi_p T_p$. Let $n_k = \#$ of (elements of A where order divides p^k), $n_k' =$ same for A', $n_1 = p^r$, where $r = \#$ of factors, $n_1' = p_r'$, where $r' = \#$ of factors. Since $T_p \cong T_p'$, we

have $p^r = p^{r'} \implies r = r'$. $n_2 = (p^2)^{r_2} p^{r-r_2}$ where $r_2 = \#$ of factors where $p^2 \mid p_i^{a_i} \implies r_2 + r = r_2' + r \implies r_2 = r_2'$.
$n_k = (p^k)^{r_k} P_{k-1} = (p^k)^{r_k'} P_{k-1}$ where $P_{k-1} =$ product of terms from $k-1$ step, so $r_k = r_k'$, and thus two representations are identical. □

Say D is a domain. Then if $ab = cb$, $b \neq 0 \implies a = c$, because $b(a-c) = 0 \implies a - c = 0$. Let's develop the technology to just divide both sides by b. Let $D' = D[x]/(bx-1)$. Then, in D', $bx = 1$, so b is a unit. We will see later that D' is a domain that contains D. Alternatively, you could do this. Let $K(D) = \{\frac{a}{b} \mid a, b \in D, b \neq 0\}/\sim$, where $\frac{a}{b} \sim \frac{c}{d}$ iff $ad = bc$. $\frac{a}{b} \pm \frac{c}{d} = \frac{ad \pm bc}{bd}$, and $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$. These operations make $K(D)$ into a ring, called the fraction field of D. The multiplicative identity is $\frac{1}{1}$. Also ,there is an injective homomorphism $\phi : D \to K(D)$

$$\phi(d) = \frac{d}{1}$$

Often we write d instead of $\frac{d}{1}$.

Example 2.15

$K(\mathbb{Z}) = \mathbb{Q}$.

Example 2.16

$K(\mathbb{R}[x]) = \{\frac{p(x)}{q(x)} \mid q(x) \neq 0\} =$ rational functions in $x = \mathbb{R}(x)$.

Example 2.17

$K(\mathbb{C}[x, y, z]) = \{\frac{p(x,y,z)}{q(x,y,z)} \mid q \neq 0\} = \mathbb{C}(x, y, z)$.

Theorem 2.15

$K(D)$ is a field.

Proof:

The inverse of $\frac{a}{b}$ is $\frac{b}{a}$, as long as $a \neq 0$. □

Theorem 2.16

Say $\phi : D \to F$ is an injective homomorphism where D is a domain and F is a field. Then there is an injective homomorphism $\psi : K(D) \to F$ satisfying

$$\begin{tikzcd}
D \arrow[r, "\phi"] \arrow[d, "i"'] & F \\
K(D) \arrow[ur, "\psi"] &
\end{tikzcd}$$

$\phi = \psi \circ i$, where $i(d) = \frac{d}{1}$ and $K(D) =$ the fraction field of D.

Proof:

Define $\psi : K(D) \to F$ by $\psi(\frac{a}{b}) = \frac{\phi(a)}{\phi(b)}$. If $\frac{a}{b} = \frac{c}{d}$, then $ad = bc$, so $\phi(a)\phi(d) = \phi(b)\phi(c)$ so

$$\frac{\phi(a)}{\phi(b)} = \frac{\phi(c)}{\phi(d)}$$

Moreover, $\phi(b) = 0$ only happens where $b = 0$, because ϕ is 1-1. So ψ is well defined. ψ is also a homomorphism since $\psi(1) = 1$, $\psi(\frac{a}{b} + \frac{c}{d}) = \psi(\frac{a}{b}) + \psi(\frac{c}{d})$, $\psi(\frac{a}{b} \cdot \frac{c}{d}) = \psi(\frac{a}{b})\psi(\frac{c}{d})$, and ψ is injective because $K(D)$ is a field. Finally, $(\psi \circ i)(d) = \psi(\frac{d}{1}) = \frac{\phi(d)}{\phi(1)} = \phi(d)$. □

If D is a domain, $b \in D$ any element, then $D[\frac{1}{b}] \subseteq K(D)$ is a ring (domain) in which b is a unit. In fact, you can do this for arbitrary subsets of $D - \{0\}$.

Definition 2.23: Multiplicative Subset

Let D be a domain. A **multiplicative subset** of D is a subset $S \subset D - \{0\}$ that is closed under multiplcation.

Definition 2.24: Localization

The **localization** of D at S is

$$D_s = \{\frac{a}{b} \mid a \in D, b \in S\}$$

D_s is a subring of $K(D)$.

Let D be a domain, $P \subset D$ a prime ideal. The localization of D at P is

$$D_p = \{\frac{a}{b} \mid a, b \in D, b \notin P\}$$

This is actually the localization of D at $D - P$, but no one ever says that. You need P to be prime because $a, b \notin P \Rightarrow ab \notin P$ only works for prime ideals.

2.9 Chinese Remainder Theorem

Definition 2.25

1. $I + J = \{a + b \mid a \in I, b \in J\}$
2. IJ is the ideal generated by $\{ab \mid a \in I, b \in J\}$
3. $IJ = \{a_1 b_1 + \cdots + a_n b_n \mid a_i \in I, b_i \in J\}$
4. $I = (a_1, \ldots, a_r), J = (b_1, \ldots, b_t) \Rightarrow IJ = (a_1 b_1, \ldots, a_r b_t)$ (every possible pair).

Theorem 2.17: Chinese Remainder Theorem

Let R be a ring, $I, J \subset R$ ideals with $I + J = R$. Then

$$R/IJ \cong (R/I) \times (R/J)$$

Proof:

Define $\phi : R \to (R/I) \times (R/J)$ by

$$\phi(r) = (r + I, r + J)$$

The kernel of ϕ is $\ker \phi = I \cap J$, since $IJ \subset I \cap J$,we get a homomorphism $\tilde{\phi} : R/IJ \to (R/I) \times (R/J)$. $\tilde{\phi}$ is onto because $I + J = R \Rightarrow$ there are $a \in I.b \in J$ with $a + b = 1$. So for any $(x, y) \in (R/I) \times (R/J)$, $\phi(bx + ay) = (x, y)$. The kernel of $\tilde{\phi}$ is $\ker \phi = I \cap J$ reduced mod IJ. And:

$$I \cap J = (I \cap J)R = (I \cap J)(I + J) = (I \cap J)I = (I \cap J)J \subset JI + IJ = IJ$$

so $I \cap J \subset IJ$. Since we already know $IJ \subset I \cap J$, we get $I \cap J = IJ$, so

$$\tilde{\phi} : R/(IJ) \to (R/I) \times (R/J)$$

is an isomorphism. □

Example 2.18

$$\begin{aligned}\mathbb{R}[x]/(x^2+3x+2) &= \mathbb{R}[x]/(x+1)(x+2)\\ &= \mathbb{R}[x]/(x+1)\times\mathbb{R}[x]/(x+2)\\ &= \mathbb{R}\times\mathbb{R}\end{aligned}$$

2.10 Final Exam

6 questions. Topics include:

- Group Actions
- Quotients
- Conjugacy Classes
- Disjoint Cycle Notation
- Sylow's Theorem
- Free Groups
- Ring Homomorphisms
- Ideals
- Modules
- etc...