

RINGS

Rings

Rings, commutative, associative, zero-divisors, integral domains, ideals, maximal ideals, quotient ring, princ. ideals, prime ideals, hom, isom. thms
Euclidean rings, PID, domains, Division rings,

Rings are objects formed of a set w/
two binary operations.
We don't start w/ an example & statement
like "Groups are the study of symmetry"
because, as one expects, Rings are much more
complicated (adding a b.op. will do that...!).
Here are several ways of thinking about
the structure of rings:

Number Theory

Rings are, in essence, algebraic objects that
share the structure of the integers w/ standard
mult. & addition. In fact more general rings
than $\mathbb{Z}$ were studied to help understand $\mathbb{Z}$'s
structure.

Polynomials

If we have a ring R , then the collection

of polynomials $a_n x^n + \dots + a_1 x + a_0$ w/ $a_i \in \mathbb{R}$ also forms a ring.

The study of poly. rings introduces a very important concept of ideals, which are to rings what cosets are to groups.

Def: A semigroup is a pair $(S, \cdot)$ s.t. $\cdot$ is an associative b.o. on S & $\exists$ an identity e s.t. $s \cdot e = e \cdot s = s \ \forall s \in S$

Def: A ring is a triple $(S, +, \cdot)$ s.t. $(S, +)$ is an abelian gp & $(S, \cdot)$ is a semigrp.

The interaction between the operations is as follows:
for $a, b, c \in S$ we have

$$a \cdot (b + c) = ab + ac$$

$$(b + c) \cdot a = ba + ca$$

So rings are formed by adding a second binary operation to a group.

STRUCTURE OF RINGS FROM GROUPS

But there is a more structural way of defining rings

Defⁿ

Let $(R, +, \cdot)$ be a ring. Given a subset $T \subseteq R$, if $(T, +, \cdot)$ is also a ring it is called a subring.

Recall an endomorphism is a homomorphism $\varphi: G \rightarrow G$.

Theorem: i) Let $(R, +, \cdot)$ be a ring. Consider the set $\text{End}(R)$ of all endomorphisms $\varphi: (R, +) \rightarrow (R, +)$. Then $(\text{End}(R), +, \cdot)$ is a ring.
ii) $(R, +, \cdot)$ is isomorphic to a subring of $(\text{End}(R), +, \cdot)$.

We will talk in AA II about group actions. Think how we define symmetric groups as transformations of simplices, or even as transformations of sets (eg. sets of vertices)

In general all groups "act" on sets.
In the same way, rings "act" on abelian groups.

Homomorphisms

Of course, to discuss isomorphisms we need homomorphisms.

A homomorphism between rings R_1 & R_2 is a map $\varphi: R_1 \rightarrow R_2$ s.t.

$$\varphi(r_1 r_2) = \varphi(r_1) \cdot \varphi(r_2),$$

$$\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2),$$

$$\varphi(1_{R_1}) = 1_{R_2}$$

Why is $\varphi(1_{R_1}) = 1_{R_2}$ included?
We defined rings to contain mult identity,
& we want to study maps that preserve
ring structure.

$$\text{Remark: } \varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2) \Rightarrow \begin{cases} 0_{R_2} \in \varphi(R_1) \\ \varphi(0_{R_1}) = \varphi(0_{R_2}) \end{cases}$$

$$\text{But } \varphi(r_1 r_2) = \varphi(r_1) \varphi(r_2) \not\Rightarrow 1_{R_2} \in \varphi(R_1)$$

(See HW)

Analogue of Cayley's theorem:

Proof: i) is HW

ii) We find an injective hom: $R \rightarrow \text{End}(R)$

define $\varphi: R \rightarrow \text{End}(R): x \mapsto \lambda_x$

where λ_x is an end. of R defined by

$$\lambda_x: R \rightarrow R: y \mapsto xy \quad (\text{left mult. by } x)$$

$(R, +)$ Why is mult. okay here?

Let's check: Since $(R, +, \cdot)$ is a ring, $xy \in R$

$\forall x, y$. So λ_x is a map between $(R, +)$ & $(R, +)$.

hom? $\lambda_x(y+z) = x(y+z) = xy + xz = \lambda_x(y) + \lambda_x(z)$

Let's show now that φ is hom. (of rings)

$$\varphi(1) = \lambda_1 \quad \& \quad \lambda_1(\lambda_x(y)) = 1 \cdot \lambda_x(y) = \lambda_x(y)$$

$$\lambda_x(\lambda_1(y)) = \lambda_x(1 \cdot y) = \lambda_x(y)$$

So mult. id. preserved.

$$\begin{aligned} \varphi(a+b) &= \lambda_{a+b} & \lambda_{a+b}(y) &= (a+b)(y) = ay + by = \lambda_a(y) + \lambda_b(y) \\ &= \lambda_a + \lambda_b & &= (\lambda_a + \lambda_b)(y) \end{aligned}$$

$$\begin{aligned} \varphi(a \cdot b) &= \lambda_{ab} & \lambda_{ab}(y) &= (ab)y = a \cdot (by) = a \cdot \lambda_b(y) = \lambda_a(\lambda_b(y)) \\ &= \lambda_a \circ \lambda_b \end{aligned}$$

So φ is hom.

Finally check φ is injective

$$\varphi(a) = \varphi(b) \Leftrightarrow \lambda_a = \lambda_b$$

$$\Leftrightarrow ax = bx \quad \forall x \in R$$

$$\Leftrightarrow a = b$$

So φ injective. $\square$

To finish we will state analogues of the isomorphism theorems for rings.



IDEALS

Remember the story from groups:
Groups are the algebraic structure of symmetry

- We studied structure preserving maps between groups (homomorphisms)
- We saw kernels as determining structure particularly normality, from which we define
- Quotients, which are defined by normal subgroups

We have a very similar story for rings. Instead of normal subgroups we have ideals.

Def¹ In a ring $(R, +, \cdot)$, a subset $H \subset R$ is called a subring if $(H, +, \cdot)$ is a ring.

Recall a normal subgroup $N \trianglelefteq G$ has
 $gN = Ng \quad \forall g \in G$.

Normal subgroups partition groups into subsets that themselves have a group structure (quotient groups)

We follow the same path for partitioning rings. We start with... Normal subgroups!

Defⁿ: Let $(R, +, \cdot)$ be a ring. Let $I \subset R$ s.t. $(I, +)$ is a subgroup of $(R, +)$ & I is closed under multiplication, i.e.

$$gI = \{gi \mid i \in I\} \subseteq I \quad \forall g \in R.$$

Then I is called a left ideal in R .

A similar definition exists for right ideals.
Henceforth we only consider commutative rings.
So every left ideal is a right ideal.

Example: (commutative algebra compared to a countable set)
(non-commutative algebra compared to an uncountable set)

Consider subsets $\mathbb{Z}, 2\mathbb{Z}, 3\mathbb{Z}$, of $\mathbb{Z}$

take $3\mathbb{Z} = \{3z \mid z \in \mathbb{Z}\} = \{\dots, -6, -3, 0, 3, 6, \dots\}$.

then $g \cdot (3\mathbb{Z}) = \{3gz \mid z \in \mathbb{Z}\} = \{\dots, -6g, -3g, 0, 3g, 6g, \dots\}$

$\subseteq 3\mathbb{Z} \quad \forall g$. So $3\mathbb{Z}$ is an ideal in $\mathbb{Z}$.

Remark: Note $(\mathbb{R}, +)$ is an abelian gp,
so all subgroups are normal. Hence ideals
are normal additive subgps.
However, not all normal subgps are ideals.

Example: $(\mathbb{Q}, +, \cdot)$ and consider

$(\mathbb{Z}, +) \triangleleft (\mathbb{Q}, +)$. But $\frac{1}{2} \cdot \mathbb{Z} \not\subseteq \mathbb{Z}$, so

$\mathbb{Z}$ is not an ideal in $\mathbb{Q}$.

Ideal Structure

Let $I \subset R$ be an ideal.

Then $rI \subset I \quad \forall r \in R$.

What about $r + I = \{r + i \mid i \in I\}$?

Let $r_0 \in I$. Then $r_0 + I = I$, as $(I, +)$ is a group.

Let $r_1 \in R \setminus I$. Then $r_1 + I = \{r_1 + i \mid i \in I\}$

Lemma: $(r + I) \cap I = \begin{cases} \emptyset, & r \notin I \\ I, & r \in I \end{cases}$

Proof: if $r \in I$ then $(r + I) \cap I = I \cap I = I$

if $r \notin I$ then $r + i \in I \Leftrightarrow$
 $r + i - i \in I \Leftrightarrow$ ($\neq$ group would imply $-i \in I$)
 $r \in I \Rightarrow \square$

Lemma: If $r_1 \in r_2 + I$ then $r_1 + I = r_2 + I$.

Proof: $r_1 = r_2 + i_2$, some $i_2 \in I$. Let $\bar{i} \in I$. Then

$r_1 + \bar{i} = r_2 + i_2 + \bar{i} \in r_2 + I$. So $r_1 + I \subseteq r_2 + I$

Also $r_1 - \bar{i}_2 = r_2$, so $r_2 \in r_1 + I$. Hence

$r_2 + \bar{i} = r_1 + \bar{i} - \bar{i}_2 \in r_1 + I$. So $r_2 + I \subseteq r_1 + I$

Hence $r_1 + I = r_2 + I$.

Lemma: if $r_1 \notin r_2 + I$ then $(r_1 + I) \cap (r_2 + I) = \emptyset$

$r_1 + i \in r_2 + I$ iff $r_1 + i = r_2 + j$, some $j \in I$.

iff $r_1 = r_2 + j - i \in r_2 + I \Rightarrow \square$

So no element of $(r_1 + I)$ is in $(r_2 + I)$ $\square$

Lemma: The union of all cosets of an ideal is the ring itself. $\square$ (H.W.)

Corollary: An ideal I of R partitions the ring into distinct subsets $r+I$.

Remark: Restricted to groups this is precisely the construction of Lagrange's Theorem.

This partitioning retains ring structure!

Defn Let $I \subset R$ be an ideal. The collection of cosets $\{I, r_1+I, r_2+I, \dots\}$ is called the quotient ring of R by I , denoted R/I .

R/I is a ring with i in $\swarrow$ non-comm. rings R/I & I/R may be different.

$$\bullet (r_1+I, r_2+I) = r_1 r_2 + I$$

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

HW: Prove R/I is a ring

FIELDS

Fields

There are many properties a ring may have: commutativity, division, factorisation, etc. We focus on two, one necessary for the other.

zero-divisors: an element $z \in R$ is called a zero-divisor if $\exists$ some $r \in R \setminus \{0\}$ s.t.
 $z \cdot r = 0$

eg. Consider $\mathbb{Z}_{12} = \{0, 1, 2, \dots, 11\}$

$$\text{Then } 3 \cdot 4 = 12 \equiv 0$$

3 & 4 are zero divisors... they always come in pairs!

Note (HW): Any elt. of a finite ring is either a zero-divisor or invertible. Invertible elements are called units.

Defn A ring with no zero divisors is called an integral domain

Ex. As the name suggests, $(\mathbb{Z}, +, \cdot)$ is an integral domain.

A field is a ring in which $(R, +)$ is an abelian group, i.e. we have addition, subtraction, multiplication, & division (with exception of 0)

Rings capture the structure of $(\mathbb{Z}, +, \cdot)$
Fields capture the structure of $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

There is a strong connection between ideals and division:

Defⁿ: Let I be an ideal in R s.t. the only ideal containing I is R itself. Then I is called a maximal ideal

Example: in $\mathbb{Z}$, $n\mathbb{Z}$ is an ideal

Note $4\mathbb{Z} = \{-4, 0, 4, \dots\} \subseteq \{-4, -2, 0, 2, 4, \dots\} = 2\mathbb{Z}$
 $4\mathbb{Z}$ is not maximal: $p\mathbb{Z}$ is maximal $\forall p \text{ prime}$

Theorem: Let R be a ring and I an ideal. Then I is maximal iff R/I is a field.

Corollary: $\mathbb{Z}/p\mathbb{Z}$ is a field.

PRINCIPAL IDEAL DOMAINS

Recall the notation $\langle x_1, x_2, x_3, \dots \rangle$ for a group:
 $\langle x \rangle = \{x^i \mid i \in \mathbb{Z}\}$
 $\langle x, y \rangle = \{x^i y^j \mid i, j \in \mathbb{Z}\}$ etc.

the x_i are called generators.

Since ideals are closed under mult. by ring elts we can ask about "generators" of rings by mult.

Recall ideals are normal subgroups w/ addition, but typically not subgroups at all w/ multiplication. So the use of "generator" is a abuse of terminology.

eg in $\mathbb{Z}$, the ideal $2\mathbb{Z} = \{-4, -2, 0, 2, 4, \dots\}$
 $= \{2z \mid z \in \mathbb{Z}\}$
 $= (2)$

Such an ideal is called principal.
Let's compare some rings w/ principal & non principal ideals.

Ex] in $\mathbb{Z}$ every ideal is of the form $n\mathbb{Z} = (n)$, so every ideal is principal. (f.w.)
in $\mathbb{Z}_n$ ideals are $d\mathbb{Z}$, $1|n$

Ex] Consider the subrings of $\mathbb{C}$:

$$\mathbb{Z}(\sqrt{-n}) = \{a + b\sqrt{-n} \mid a, b \in \mathbb{Z}, n \in \mathbb{N}\}$$

if $n=1$ we have $a+bi$, $a, b \in \mathbb{Z}$ - Gaussian integers

if $n=3$ we have Eisenstein integers

$$\mathbb{Z}(\sqrt{-3}) = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}$$

$(z) = \{az + bz\sqrt{-3} \mid a, b \in \mathbb{Z}\}$ is an ideal
for any $z \in \mathbb{Z}$: $(0) = \{0\}$ & $(1) = \mathbb{Z}$.

But what about $(1, 1+\sqrt{-3})$?

$$\{1(a+b\sqrt{-3}) + (1+\sqrt{-3})(c+d\sqrt{-3}) \mid a, b, c, d \in \mathbb{Z}\}$$

$(a+b\sqrt{-3})$ can be chosen freely, so we can form
any elt. of $\mathbb{Z}[\sqrt{-3}]$, i.e. $(1, 1+\sqrt{-3}) = \mathbb{Z}[\sqrt{-3}]$

What about $(2, 1+\sqrt{-3})$?

Interlude: Prime & irreducible

In a ring R , $x \in R$ is called irreducible if x is not invertible and for every $x = ab$ either a or b is invertible.

eg: in $\mathbb{Z}$, $4 = 2 \cdot 2$. 2 is not invertible, so 4 is not irreducible.

However $3 = 3 \cdot 1 = 1 \cdot 3$ (only options) & 1 invertible
So 3 irreducible.

In a ring R , $x \in R$ is prime if whenever $x \mid ab$ either $x \mid a$ or $x \mid b$

eg. in $\mathbb{Z}$ $7 \mid 49 \cdot 3$ so $7 \mid 49$ (7 is prime)

⌊

Note that, in $\mathbb{Z}[\sqrt{-3}]$, 2 is NOT prime

$$(1 + \sqrt{-3})(1 - \sqrt{-3}) = 1 - (-3) = 4 = 2 \cdot 2$$

So $2 \mid 4$ so $2 \mid (1 + \sqrt{-3})(1 - \sqrt{-3})$ but

$2 \nmid (1 + \sqrt{-3})$. 2 is irreducible but not prime.

Say $(2, 1+\sqrt{-3}) = (\alpha)$, some $\alpha \in \mathbb{Z}[\sqrt{-3}]$

Then $2 = z_1 \alpha$, some $z_1 \in \mathbb{R}''$
i.e. $\alpha \mid 2$

So $\alpha = \pm 2$ or $\alpha \in \{\pm 1\}$ $z_1 \in \mathbb{R}$

If $\alpha = \pm 2$ then $1+\sqrt{-3} = z_2 \alpha = \pm 2 z_2$

So $2 \mid 1+\sqrt{-3} \Rightarrow \Leftarrow$

if $\alpha = \pm 1$ then $(2, 1+\sqrt{-3}) = \mathbb{Z}[\sqrt{-3}]$

Then $2 z_1 + (1+\sqrt{-3}) z_2 = 1$ for some $z_1, z_2 \in \mathbb{R}$

Then $2 z_1 (1-\sqrt{-3}) + (1+\sqrt{-3})(1-\sqrt{-3}) z_2 = 1-\sqrt{-3}$

Then $2 \mid 1-\sqrt{-3} \Rightarrow \Leftarrow$

So $(2, 1+\sqrt{-3})$ is not principal.

Remark: In $\mathbb{Z}[\sqrt{-3}]$ the fundamental theorem of algebra does not hold: there is not unique factorisation of every element.
Unique factorisation always holds in PIDs (and some other rings)... HW

POLYNOMIAL RINGS & EXTENSION FIELDS

We have seen $\mathbb{Z}[i] = \{a+ib \mid a, b \in \mathbb{Z}\}$
& $\mathbb{Z}[\sqrt{3}] = \{a+b\sqrt{3} \mid a, b \in \mathbb{Z}\}$

These are subrings of $\mathbb{C}$.

$\mathbb{Z}$ is a subring of both.

We call these extension rings of $\mathbb{Z}$.

Defⁿ. An extension ring of a ring R is any ring that R is a subring of.

eg] $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$

Defⁿ Let R be a ring and $x \notin R$.

Then $R[x] = \{a_0 + a_1x + \dots + a_nx^n \mid a_i \in R, n \in \mathbb{N}\}$ is the polynomial ring of R .

HW: Show $R[x]$ is actually a ring.

Remark: In fact, $R[x]$ is the smallest ring that contains $R \cup \{x\}$.

Remark: More generally one can consider

$$R[x_1, \dots, x_m] = \left\{ \sum_{i=1}^n a_i \prod_{j=1}^m x_j^{\alpha_j} \mid n \in \mathbb{N}, a_i \in R, \alpha_j \in \mathbb{N}_0 \right\}$$

Ex $\mathbb{Z}[x] = \{a_0 + a_1x + a_2x^2 + \dots + a_nx^n \mid a_i \in \mathbb{Z}, n \in \mathbb{N}\}$

Consider $\sqrt{-1}$: then $\sqrt{-1}^2 = -1$

$$\begin{aligned} \text{So } \mathbb{Z}[\sqrt{-1}] &= \{a_0 + a_1\sqrt{-1} + a_2\sqrt{-1}^2 + a_3\sqrt{-1}^3 + \dots\} \\ &= \{a_0 + a_1\sqrt{-1} - a_2 - a_3\sqrt{-1} + \dots\} \\ &= \{(a_0 - a_2 + a_4 - \dots) + (a_1 - a_3 + a_5 - \dots)\sqrt{-1}\} \\ &= \{a + b\sqrt{-1} \mid a, b \in \mathbb{Z}\} \end{aligned}$$

Similarly, if $d^3 \in \mathbb{R}$ & $d, d^2 \notin \mathbb{R}$ then
 $\mathbb{R}[d] = \{a_0 + a_1d + a_2d^2 \mid a_i \in \mathbb{R}\}$ etc.

Similarly $\mathbb{Z}[\sqrt{2}, \sqrt{3}] = \{a_0 + a_1\sqrt{2} + a_2\sqrt{3} + a_3\sqrt{2}\sqrt{3} \mid a_i \in \mathbb{Z}\}$

Remark: $\mathbb{Z} \subseteq \mathbb{Z}[\sqrt{2}] \subset \mathbb{Z}[\sqrt{2}, \sqrt{3}]$

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

HW: Show $(\mathbb{Z}[\sqrt{2}])[\sqrt{3}] = \mathbb{Z}[\sqrt{2}, \sqrt{3}]$

Q. What is the story here?

We can arbitrarily add non ring elts to a ring... so what?

PRINCIPAL
&

MAXIMAL
IDEALS

There is a connection between extension rings of fields, principal & maximal ideals, quotient rings, & irreducibility.

Example: Consider the field $\mathbb{Q}$.

Consider $x^2 - 2 \in \mathbb{Q}[x]$. This is irreducible: $x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2})$ and neither is in $\mathbb{Q}[x]$ as $\sqrt{2} \notin \mathbb{Q}$.

Consider the ideal $(x^2 - 2) \subset \mathbb{Q}[x]$.

Say I is an ideal in $\mathbb{Q}[x]$ and $(x^2 - 2) \subset I$. Then, since $\mathbb{Q}[x]$ is PID (we will show later), $I = (d)$, $d \in \mathbb{Q}[x]$

$x^2 - 2 \in (d)$ so $x^2 - 2 = qd$, some $q \in \mathbb{Q}[x]$

Then d is a unit: $(d) = \mathbb{Q}[x]$

or $d = x^2 - 2$: $(d) = (x^2 - 2)$

Hence $(x^2 - 2)$ is maximal.

So $\mathbb{Q}[x]/(x^2 - 2)$ is a field.

What is this field?

$$\mathbb{Q}[x]/(x^2-2) \cong \mathbb{Q}[\sqrt{2}] \quad !$$

elements are $p(x) + (x^2-2)$, $p(x) \in \mathbb{Q}[x]$

$$\text{Note: } x^2 + (x^2-2) = x^2 - x^2 + 2 + (x^2-2) = 2 + (x^2-2)$$

i.e. we can extract any product $q \cdot (x^2-2)$ w/o changing the term:

$$a + (x^2-2) = a + \underbrace{q(x^2-2)}_{\text{poly}} + \underbrace{(x^2-2)}_{\text{ideal}}$$

In particular:

$$x^3 \mapsto 2x, \quad x^4 \mapsto 2x^2 \mapsto 4 \text{ etc.}$$

$$\text{if } p(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \dots$$

$$\text{then } p(x) + (x^2-2) = a_0' + a_1'x + (x^2-2), \text{ some } a_0', a_1' \in \mathbb{Q}$$

$$\text{Also: in } \mathbb{Q}[x]/(x^2-2) \quad x^2 + (x^2-2) = 2 + (x^2-2)$$

$$\begin{aligned} & (a + bx + (x^2-2))(c + dx + (x^2-2)) \\ &= ac + bdx^2 + (ad+bc)x + (x^2-2) \\ &= ac + 2bd + (ad+bc)x + (x^2-2) \end{aligned}$$

$$\text{Consider } (a + b\sqrt{2})(c + d\sqrt{2}) \in \mathbb{Q}[\sqrt{2}]$$

$$= ac + 2bd + (ad + bc)\sqrt{2}$$

Exactly the same algebraic structure!
In fact

$$\mathbb{Q}[x]/(x^2-2) \cong \mathbb{Q}[\sqrt{2}]$$

An isomorphism is the map

$$f: \mathbb{Q}[x]/(x^2-2) \rightarrow \mathbb{Q}[\sqrt{2}]$$

$$\text{defined by } f(x + (x^2-2)) = \sqrt{2}$$

○

Theorem:

Let F be a field. Let $f \in F[x]$ be irreducible. Then

$$F[x]/(f) \cong F[\alpha] \quad , \quad \alpha \text{ is a root of } f.$$

Lemma: Let R be a ring and u is a unit in R .
Then $(u) = R$.

Proof: A unit is an invertible elt., so $u^{-1} \in R$.

Let $x \in R$. Then $u^{-1} \cdot x \in R$, so $u \cdot (u^{-1} \cdot x) = x \in (u)$

So $(u) = R$. $\square$

Lemma: Let R be a PID. If $x \in R$ is irreducible then (x) is maximal.

Proof: if $(x) \subseteq I$, an ideal in R , then
 $I = (y)$ (R is a PID).

So $x = ay$. So either y is a unit or $y = x$
i.e. $I = (x)$ or $I = R$. $\square$

Ex As before, in $\mathbb{Z}$ 4 is reducible &
 $(4) \subseteq (2)$, so (4) is not maximal.

Irreducibility is necessary for generality.

Lemma: Let F be a field. Then $F[x]$ is
PID.

Proof:

Simple gps

This is non-examiable

Every group has trivial normal subgps. Recall for a gp G that $\{e\} \triangleleft G$ & $G \triangleleft G$.

Def: A gp G is called simple if it has no non-trivial normal subgps.

Note: Every subgp of an abelian gp is normal. Simple gps are in some sense the simplest "not simple" gps: Abelian gps are "simpler" but simple gps have no abelian-like structure inside.

Simple gps are analogous to primality of natural numbers, though much more complicated. Let's examine the structure of gps using their normal subgps

Def: A composition series of a group G is a sequence

$$\{e\} = H_0 \triangleleft H_1 \triangleleft H_2 \triangleleft \dots \triangleleft H_n \triangleleft G$$

where H_i is a maximal normal subgp in H_{i+1} & H_i is. $\nexists N$ s.t. $H_i \triangleleft N \triangleleft H_{i+1}$ w/ $H_i \neq N \neq H_{i+1}$

To get a better understanding of composition series we prove the fourth iso. thm (Lattice thm)

Theorem: (Fourth Isomorphism Theorem)

Let G be a gp, $N \triangleleft G$, $\mathcal{G} = \{A \mid N \subseteq A \triangleleft G\}$ (set of subgps of G containing N) & $\mathcal{H} = \{A \mid A \triangleleft G/N\}$ (set of subgps of G/N)
Then there is a bijection between $\mathcal{G}$ & $\mathcal{H}$ sending
 $A \mapsto A/N$ $\square$

The usefulness is immediately seen in the corollary

Corollary: A series $\{e\} = H_0 \triangleleft \dots \triangleleft H_n \triangleleft G$ is a composition series iff H_i/H_{i+1} is simple for all i .

Proof: $H_i \triangleleft H_{i+1}$. Let $H =$ subgps of H_{i+1} containing H_i .
 H_i is maximal, so H contains only H_i & H_{i+1} .
So the subgps of H_{i+1}/H_i number two, the trivial subgps. Hence H_{i+1}/H_i is simple.

Example: Recall the cyclic gps $C_n = \langle \alpha \rangle = \{e, \alpha, \dots, \alpha^{n-1}\}$
 $\cong (\mathbb{Z}/n\mathbb{Z}, +(\text{mod } n))$

The cyclic gp C_{10} has composition series
 $\{e\} = C_1 \triangleleft C_2 \triangleleft C_{10} : |C_{10}/C_2| = 5, |C_2/C_1| = 2$
 $\{e\} = C_1 \triangleleft C_5 \triangleleft C_{10} : |C_{10}/C_5| = 2, |C_5/C_1| = 5$

This corresponds to the Fund. thm of arithmetic
In fact the decomposition series is essentially
unique

Lemma: Every finite gp has a composition series $\square$

Theorem: (Jordan - Hölder theorem)

Let G be a gp w/ a composition series.

Let $\{e\} = H_1 \triangleleft H_2 \triangleleft \dots \triangleleft H_s \triangleleft G$ &
 $\{e\} = N_1 \triangleleft N_2 \triangleleft \dots \triangleleft N_r \triangleleft G$ be two comp.
series for G . Then $s=r$ & there is some
permutation $N \in S_r$ s.t.

$$H_{i+1}/H_i \cong N_{N(i)+1}/N_{N(i)} \quad \square$$

In other words the composition series is unique
up to permutation & isomorphism of quotients.

We close our discussion of Simple
groups w/ some important classes of
examples of simple groups.

Theorem: Every finite gp of prime order
is simple.

Proof: Lagrange's thm says that if $|G| < \infty$ &
 $H \triangleleft G$ then $|H| \mid |G|$. If $|G| = p$ then $|H| = 1$ or p .
If $|H| = 1$, $H = \{e\}$. If $|H| = p$, $H = G$. $\square$

We can show more about the structure of
gps of prime order.

Theorem: Let G be a finite gp w/ prime order

$|G| = p$. Then $G \cong \mathbb{Z}_p$.

Proof. Let $g \in G, g \neq e_G$. Consider $\langle g \rangle$.

$e = g^p \in \langle g \rangle$. For every $g^n \in \langle g \rangle$, $g^{p-n} \in \langle g \rangle$ so

$$g^n \cdot g^{p-n} = g^p = e$$

So identity & inverses are in $\langle g \rangle$. $\langle g \rangle$ inherits associativity from G . Hence $\langle g \rangle < G$. By Lagrange's thm: $|\langle g \rangle| \mid |G|$ so $\langle g \rangle = \{e\}$ or G . $g \neq e_G$ so $|\langle g \rangle| > 1$ so $\langle g \rangle = G$ & so G is cyclic.

Typically abelian groups won't be $\square$ simple.

Theorem: Let $H < G$, G an abelian group.
Then $H \trianglelefteq G$.

Proof: for $g \in G$, $gH = \{gh \mid h \in H\} = \{hg \mid h \in H\} = Hg$ $\square$

Corollary: If G is abelian and contains a non-trivial subgrp then G is not simple.

When does G contain a subgrp of a particular order? We study more in Abstract Algebra II.

For now:

HW Let G be abelian & simple
Show $G \cong \mathbb{Z}_p$ p prime