# MAS439 Lecture 3
# Subrings

October 5th

# Today we discuss subrings, tomorrow we discuss ideals

Let $\varphi : R \to S$ be a ring homomorphism.

## Definition (image)

$$\mathrm{Im}(\varphi) = \{s \in S | s = \varphi(r) \text{ for some } r \in R\}$$

## Definition (kernel)

$$\ker(\varphi) = \{r \in R | \varphi(r) = 0_S\}$$

- $\mathrm{Im}(\varphi)$ is a *subring* of $S$, which we will discuss today.
- $\ker(\varphi)$ is an *ideal* of $R$, which we will discuss tomorrow.

# Definition of a subring

Let $R$ be a ring. A subset $S \subset R$ is a *subring* of $R$ if

- $S$ is closed under addition and multiplication:

$$r, s \in S \text{ implies } r + s, r \cdot s \in S$$

- $S$ is closed under additive inverses: $r \in S$ implies $-r \in S$.
- $S$ contains the identity: $1_R \in S$

This is the *minimal* structure needed

But of course subrings are actually rings...

# Subrings are rings

### Lemma

*Let $S$ be a subring of $R$. Then $S$ is a ring, with addition and multiplication inherited from $R$. If $R$ is commutative, so is $S$.*

### Proof.

- Since $S$ is closed under addition and multiplication, they're binary operations on $S$.
- Second two properties guarantee additive inverses and identities
- Since $R$ is a ring, $+, \cdot$ satisfy associativity, distributivity, (commutativity)

$\square$

# First examples of subrings

- $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \subset \mathbb{H}$ is a chain of subrings.
- if $R$ any ring, $R \subset R[x] \subset R[x, y] \subset R[x, y, z]$ is a chain of subrings.

# Another example

We have the chain of subrings

$$\mathbb{R} \subset \mathbb{R}[x] \subset C^\infty(\mathbb{R}, \mathbb{R}) \subset C(\mathbb{R}, \mathbb{R}) \subset \mathrm{Fun}(\mathbb{R}, \mathbb{R})$$

Where, working backwards:

- $\mathrm{Fun}(\mathbb{R}, \mathbb{R})$ is the space of all functions from $\mathbb{R}$ to $\mathbb{R}$
- $C(\mathbb{R}, \mathbb{R})$ are the continuous functions
- $C^\infty(\mathbb{R}, \mathbb{R})$ are the *smooth* (infinitely differentiable) functions
- $\mathbb{R}[x]$ are the polynomial functions
- We view $\mathbb{R}$ as the space of constant functions

# Non-examples of subrings

- $\mathbb{N} \subset \mathbb{Z}$ is not a ring, as it is not closed under additive inverses
- Let $\mathcal{K}$ be the set of continuous functions from $\mathbb{R}$ to itself with compact (equivalently, bounded) support. That is,

$$f \in \mathcal{K} \iff \exists M \text{ s.t. } |x| > M \implies f(x) = 0$$

  Then $\mathcal{K}$ is not a ring as it doesn't contain the identity.
- Let $R = \mathbb{Z} \times \mathbb{Z}$, and let $S = \{(x, 0) \in R | x \in \mathbb{Z}\}$.
  Then $S$ *is* a ring, but it is not a subring of $R$, as the identity of $S$ is $(1, 0)$, while the identity of $R$ is $(1, 1)$.

# And our original example of a subring is in fact a subring

## Lemma

*Let $\varphi : R \to S$ be a homomorphism. Then $Im(\varphi) \subset S$ is a subring.*

## Proof.

We need to check $\mathrm{Im}(\varphi)$ is closed under addition and multiplication and contains $1_S$.

- Suppose $s_1, s_2 \in \mathrm{Im}(\varphi)$. Then $\exists r_i$ with $\varphi(r_i) = s_i$. Then

$$s_1 + s_2 = \varphi(r_1) + \varphi(r_2) = \varphi(r_1 + r_2) \in \mathrm{Im}(\varphi)$$

- Closed under multiplication is exactly the same.
- $1_S = \varphi(1_R) \in \mathrm{Im}(\varphi)$

$\square$

♫ Let's all go to the lobby ♫
♫ Let's all go to the lobby ♫
(2 minute intermission)

# Motivation for generators from Group theory

When working with groups, we often write groups down in terms of generators and relations.

## Generators are easy

To say a group $G$ is *generated* by a set of elements $E$, means that we can get $G$ by “mashing together” the elements of $E$ in all possible ways. More formally,

$$G = \{g_1 \cdot_2 \cdots g_n | g_i \text{ or } g_i^{-1} \in E\}$$

## Relations are harder

Typically there will be many different ways to write the same element in $G$ as a product of things in $E$; recording how is called relations.

# Reminder example? Okay if it's new to you

## Example

The dihedral group $D_8$ is the symmetries of the square. It is often written as

$$D_8 = \langle r, f | r^4 = 1, f^2 = 1, rf = fr^{-1} \rangle$$

Meaning that the group $D_8$ is *generated* by two elements, $r$ and $f$, satisfing the *relations* $r^4 = 1, f^2 = 1$ and $rf = fr^{-1}$.

We'll want a way to write down commutative rings in the same way

# Preview of rings from generators and relations

We will revist these examples further after we have developed ideals and quotient rings – you can think of these as the machinery that will let us impose relations on our generators.

### Example (Gaussian integers)

The Gaussian integers are written $\mathbb{Z}[i]$; they're generated by an element $i$ satisfying $i^4 = 1$.

### Example (Field with 4 element)

The field $\mathbb{F}_4$ of four elements can be written $\mathbb{F}_2[x]/(x^2 + x + 1)$ – to get $\mathbb{F}_4$, we add an element $x$ that satisfies the relationship $x^2 + x + 1 = 0$.

# Idea of generating set

The subring generated by elements in a set $T$ will again be "what you get when you mash together everything in $I$ in all possibly ways", but this is a bit inelegant and not what we will take to be the *definition*.

## Attempted definition

Let $T \subset R$ be any subset of a ring. The *subring generated by* $T$, denoted $\langle T \rangle$, *should be* the smallest subring of $R$ containing $T$.

This is not a good formal definition – what does "smallest" mean? Why is there a smallest subgring containing $T$?

# Intersections of subrings are subrings

**Lemma**

*Let $R$ be a ring and $I$ be any index set. For each $i \in I$, let $S_i$ be a subring of $R$. Then*

$$S = \bigcap_{i \in I} S_i$$

*is a subring of $R$.*

**Proof.**

Suppose $s_1, s_2 \in S$. Then by definition $s_1, s_2 \in S_j$ for all $j$. Hence $s_1 + s_2 \in S_j$ for all $j$, since $S_j$ is a subring. So $s_1 + s_2 \in S$, and $S$ is closed under addition.

The exact same argument shows $S$ is closed under multiplication and contains the unit.

# The elegant definition of $\langle T \rangle$

### Definition

Let $T \subset R$ be any subset. The *subring generated by* $T$, denoted $\langle T \rangle$, is the intersection of all subrings of $R$ that contain $T$.

### This agrees with our intuitive "definition"

$\langle T \rangle$ is the smallest subring containing $T$ in the following sense: if $S$ is any subring with $T \subset S \subset R$, then by definition $\langle T \rangle \subset S$.

### But it's all a bit airy-fairy

The definition is elegant, and can be good for proving things, but it doesn't tell us what, say $\langle \pi, i \rangle \subset \mathbb{C}$ actually looks like. Back to "mashing things up"...

# What *has* to be in $\langle \pi, i \rangle$? Start mashing!

Rings are a bit more complicated because there are two ways we can mash the elements of $T$ – addition and multiplication.

- $1, \pi, i$
- Sums of those; say, $5 + \pi, 7i$
- Negatives of those, say $-7i$
- Products of those, say $(5 + \pi)^4 i^3$
- Sums of what we have so far, say $(5 + \pi)^4 i^3 - 7i + 3\pi^2$
- $\ldots$

leading to things like:

$$\left(\left((5+\pi)^4 i^3 - 7i + 3\pi^2\right) \cdot (-2 + \pi i) + \pi^3 - i\right)^{27} - 5\pi^3 i$$

Of course, could expand that out into just sums of terms like $\pm\pi^m i^m$...

# Formalizing our insight

## Definition

Let $T \subset R$ be any subset. Then a *monomial in $T$* is a (possibly empty) product $\prod_{i=1}^{n} t_i$ of elements $t_i \in T$. We use $M_T$ to denote the set of all monomials in $T$.

## Note:

The empty product is the identity $1_R$, and so $1_R \in M_T$.

## Our insight:

From the "mashing" point of view $\langle T \rangle$ should be all $\mathbb{Z}$-linear combination of monomials.

# The elegant and "mashing" definitions agree

**Lemma**

*$\langle T \rangle = X_T$, where $X_T$ consists of those elements of $R$ that are finite sums of monomials in $T$ or their negatives. That is:*

$$X_T = \left\{ \sum_{k=0}^{n} \pm m_k \middle| m_k \in M_T \right\}$$

**Proof.**

- $X_T \subset \langle T \rangle$ since everything in $X_T$ is built up from $T$ by multiplying, adding, and taking negatives, and $\langle T \rangle$ contains $T$ and is a closed under these operations.
- $\langle T \rangle \subset X_T$ since $X_T$ is a subring containing $T$. $X_T$ clearly contains $T$ and is closed under addition and negatives, and it's closed under products by the distributive property.

$\square$

# Example: The Eisenstein integers

Let $\omega \in \mathbb{C}$ be a cube root of unity, different from one: $\omega^3 = 1, \omega \neq 1$.

What's $\langle \omega \rangle$?

Since $\omega^3 = 1$, the set of monomials is just $\{1, \omega, \omega^2\}$, so:

$$\langle \omega \rangle = \{a + b\omega + c\omega^2 | a, b, c \in \mathbb{Z}\}$$

In this case, we can simplify:

Since $0 = \omega^3 - 1 = (\omega - 1)(\omega^2 + \omega + 1)$, we have $\omega^2 = -1 - \omega$, and so we don't need to include powers of $\omega$:

$$\langle \omega = \rangle = \{a + b\omega | a, b \in \mathbb{Z}\}$$

# Generating sets for rings

### Definition

We say that a ring $R$ is *generated by* a subset $T$ if $R = \langle T \rangle$. We say that $R$ is *finitely generated* if $R$ is generated by a finite set.

# Examples of generating sets

- $\mathbb{Z} = \langle \emptyset \rangle$
- $\mathbb{Z}/n\mathbb{Z} = \langle \emptyset \rangle$
- $\mathbb{Z}[x] = \langle x \rangle = \langle 1 + x \rangle$
- $\mathbb{Z}[i] = \langle i \rangle$

# Some of your best friends are not finitely generated

- The rationals $\mathbb{Q}$ are not finitely generated: any finite subset of rational numbers has only a finite number of primes appearing in their denominator.
- The real and complex numbers are uncountably; a finitely generated ring is countable

# A non-finitely generated subring of a finitely generated ring

We've seen that $\mathbb{Z}[x] = \langle x \rangle$ and so is finitely generated.

$$S = \{a_0 + 2a_1 x + \cdots + 2a_n x^n\}$$

that is, $S$ consists of polynomials all of whose coefficients, except possibly the constant term, are even.

## Challenge:

Show that $S$ is a subring of $\mathbb{Z}[x]$ (easy), but that $S$ is not finitely generated (harder).