Definition of a subring

Let R be a ring, and let $S \subset R$ be a subset.

Idea

We say S is a subring of R if it is a ring, and all its structure comes from R.

Definition

We say $S \subset R$ is a subring 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: $1_R \in S$

Lemma

A subring S is a ring.

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.
- Others?

Another 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

- $\mathbb{N} \subset \mathbb{Z}$
- Let $\mathcal{K}$ be the set of continuous functions from $\mathbb{R}$ to itself with bounded support. That is,

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

- Let $R = \mathbb{Z} \times \mathbb{Z}$, and let $S = \{(x, 0) \in R | x \in \mathbb{Z}\}$.
- $\{0, 2, 4\} \subset \mathbb{Z}/6\mathbb{Z}$

Subrings are exactly the images of homomorphisms

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. $\square$

Lemma

If $S \subset R$, then the inclusion map $i : S \to R$ is a ring homomorphism, and $Im(i) = S$.

Clickers – ttpoll.eu

Generating subrings

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,

$$G = \{g_1 \cdot g_2 \cdots g_n | g_i \text{ or } g_i^{-1} \in E\}$$

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.

? ? ? ? ?

$\square$

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 $(5 + \pi)^4 i^3 - 7i + 3\pi^2$
- $\cdots$

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.

- $X_T \subset \langle T\rangle$?
- $\langle T\rangle \subset X_T$?

□

Example: The Gaussian integers

What's $\langle i \rangle \subset \mathbb{C}$?

- What's the set of monomials?
- But can we simplify even more?

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).