

Last lecture

- The definition of a ring

Definition 3.1

A **ring** is a set R equipped with two operations, **addition** $+$ and **multiplication** \cdot , such that for $a, b, c \in R$

- 1 $(R, +)$ is an **additive** (abelian) group:
 $a + (b + c) = (a + b) + c$, $a + 0 = a = 0 + a$,
 $a + (-a) = 0 = (-a) + a$, $a + b = b + a$
- 2 Multiplication is **associative**: $a(bc) = (ab)c$
- 3 The two **distributive** laws hold:
 $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$.

- Many examples of rings
- Left and right (multiplicative) inverses
- Commutative rings, fields
- Some properties of the zero element

Zero divisors and integral domains

Suppose that a and b are non-zero elements of R such that $ab = 0$. Then a and b are **zero divisors** in R .

We single out a particularly nice class of rings.

Definition 4.1

An **integral domain** is a commutative ring with one which does not have any zero divisors.

Examples

- \mathbb{Z} — this is the prototypical integral domain
- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$
- any field is an integral domain
- $\text{Mat}_n(\mathbb{R})$ is not an integral domain if $n > 1$
- The space of continuous functions $\mathcal{C}_0(\mathbb{R})$ is not an integral domain.
- $\mathbb{Z}[x]$ is an integral domain

The ring of formal power series

Suppose that R is a ring. We define formal power series over R .

Set $\mathcal{P}(R) = \{ (a_0, a_1, a_2, \dots) : a_i \in R \}$, the set of infinite sequences of elements of R .

Define addition and multiplication on $\mathcal{P}(R)$ by

$$(a_0, a_1, a_2, \dots) + (b_0, b_1, b_2, \dots) = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots)$$
$$(a_0, a_1, a_2, \dots)(b_0, b_1, b_2, \dots) = (a_0 b_0, a_0 b_1 + a_1 b_0, a_0 b_2 + a_1 b_1 + a_2 b_0, \dots).$$

So $(a_0, a_1, a_2, \dots)(b_0, b_1, b_2, \dots) = (c_0, c_1, c_2, \dots)$, where
$$c_k = \sum_{i+j=k} a_i b_j.$$

Lemma 4.2

Suppose that R is a ring. Then $\mathcal{P}(R)$ is a ring.

Proof Check the axioms!

The ring of formal power series...

There is a more intuitive notation for the ring of formal power series.

Let x be an **indeterminate** over R .

$$\text{Define } R[[x]] = \left\{ \sum_{i \geq 0} a_i x^i : a_i \in R \right\}.$$

There is a bijection $\mathcal{P}(R) \xrightarrow{\cong} R[[x]]$ given by

$$(a_0, a_1, a_2, \dots) \mapsto \sum_{i \geq 0} a_i x^i.$$

The addition and multiplication laws become

$$\left(\sum_{i \geq 0} a_i x^i \right) + \left(\sum_{i \geq 0} b_i x^i \right) = \sum_{i \geq 0} (a_i + b_i) x^i$$
$$\left(\sum_{i \geq 0} a_i x^i \right) \left(\sum_{j \geq 0} b_j x^j \right) = \sum_{k \geq 0} \left(\sum_{i+j=k} a_i b_j \right) x^k$$

The ring of polynomials $R[x]$ is the **subring** of $R[[x]]$ consisting of those formal power series with only **finitely many non-zero coefficients**.

Subrings

Definition 4.3

A subset S of a ring R is a **subring** of R if

- 1 $S \neq \emptyset$
- 2 If $x, y \in S$ then $x - y \in S$ (\iff additive subgroup)
- 3 If $x, y \in S$ then $xy \in S$ (\iff closed under multiplication)

(1) \implies addition on R restricts to give an addition $+: S \times S \rightarrow S$

(2) \implies multiplication on R restricts to give a multiplication $\cdot: S \times S \rightarrow S$

Proposition 4.4

Suppose that S is a subring of R . Then S is a ring with operations being the restriction of the operations of R to S .

Proof As all of the ring axioms hold in R they also hold in S . The important point is that $+$ and \cdot restrict to give binary operations on S .

□