

Last lecture

- An **integral domain** is a commutative ring with one and no zero divisors.
- Defined the ring of formal power series over an arbitrary ring
- A **subring** of a ring R is a non-empty subset S such that $x - y \in S$ and $xy \in S$ whenever $x, y \in S$ (Definition 4.3).
- Every subring is itself a ring (Proposition 4.4).

Question

If S is a subring of a ring R can we construct a **quotient ring** R/S ?

Answer

For a general **subring** the answer is **no**.
However, for an **ideal** the answer is **yes**.

Construct quotient rings is our next aim, although we will first talk about homomorphisms.

Subrings and ones

Question

Suppose that R is a ring and that S is a subring of R .

- 1 If R is a ring with one then must S necessarily have a one?
- 2 If R and S both have a one are they necessarily equal?

The answer to both of these questions is **No** !

Examples

- 1 $S = 2\mathbb{Z}$ is a subring of $R = \mathbb{Z}$ but $2\mathbb{Z}$ does not have a one.
- 2 $S = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in \mathbb{R} \right\}$ is a subring of $R = \text{Mat}_2(\mathbb{R})$.
Then $1_R = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $1_S = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, so that $1_R \neq 1_S$.
- 3 We have the following chain of subrings $1 \in \mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$.
- 4 Let $R = \text{Mat}_n(\mathbb{R})$ and $S = \{ M = (m_{ij}) \in R : m_{ij} = 0 \text{ if } i > j \}$ (the upper triangular matrices). Then S is a subring of R and the $n \times n$ identity matrix is the identity element of both rings.

Ring homomorphisms

Definition 5.1

Suppose that R and S are rings. A **ring homomorphism** is a map $\varphi : R \rightarrow S$ such that $\varphi(x + y) = \varphi(x) + \varphi(y)$ and $\varphi(xy) = \varphi(x)\varphi(y)$, for all $x, y \in R$.

Note that the definition intimately involves the possibly quite different operations in R and S ! We should really write

$$\varphi(x +_R y) = \varphi(x) +_S \varphi(y) \text{ and } \varphi(x \cdot_R y) = \varphi(x) \cdot_S \varphi(y).$$

Proposition 5.2

Suppose that $\varphi : R \rightarrow S$ is a ring homomorphism. Then $\text{im } \varphi = \{ \varphi(x) : x \in R \}$ is a subring of S .

Proof First, $\text{im } \varphi \neq \emptyset$ because $\varphi(0_R) \in \text{im } \varphi$.

Secondly, $\varphi(x) - \varphi(y) = \varphi(x - y) \in \text{im } \varphi$
and $\varphi(x)\varphi(y) = \varphi(xy) \in \text{im } \varphi$.

Hence, $\text{im } \varphi$ is a subring of S by Definition 4.3. \square

The kernel of a homomorphism

The **kernel** of a ring homomorphism $\varphi : R \rightarrow S$ is

$$\ker \varphi = \{ x \in R : \varphi(x) = 0_S \}.$$

Proposition 5.3

Suppose that $\varphi : R \rightarrow S$ is a ring homomorphism. Then $\ker \varphi$ is a subring of R .

Proof To show that $\ker \varphi \neq \emptyset$ we prove that $\varphi(0_R) = 0_S$. This follows because $\varphi(0_R) = \varphi(0_R + 0_R) = \varphi(0_R) + \varphi(0_R)$, so canceling $\varphi(0_R)$ from both sides proves the claim.

Secondly, $\ker \varphi$ is closed under addition and multiplication because if $x, y \in \ker \varphi$ then

$$\begin{aligned} \varphi(x - y) &= \varphi(x) - \varphi(y) = 0_S - 0_S = 0_S, \text{ and} \\ \varphi(xy) &= \varphi(x)\varphi(y) = 0_S \cdot 0_S = 0_S \text{ (by Lemma 3.6)} \end{aligned}$$

Hence, $\ker \varphi$ is a subring of R . \square

Examples of homomorphisms

- $\varphi: R \rightarrow R; r \mapsto r$ — the identity map on R .
This is a ring homomorphism.
- $\varphi: \mathbb{Z} \rightarrow 2\mathbb{Z}; z \mapsto 2z$.
No! — respects addition but not multiplication
- $\varphi: R \rightarrow R; r \mapsto -r$.
No! — respects addition but not multiplication
- $\varphi: \text{Mat}_n(\mathbb{R}) \rightarrow \mathbb{R}; M \mapsto \det M$.
No! — respects multiplication but not addition
- $\varphi: \text{Mat}_n(\mathbb{R}) \rightarrow \text{Mat}_n(\mathbb{R}); M \mapsto AMA^{-1}$, for $A \in \text{GL}_n(\mathbb{R})$.
This is a ring homomorphism.

Polynomial rings

Proposition 5.4

Suppose that R is a ring. Let

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

Then $R[x]$ is a subring of $R[[x]]$.

Proof First, $R[x] \neq \emptyset$ since $0 = 0 + 0x + 0x^2 + \dots \in R[x]$.

If $f(x) = \sum_i f_i x^i$ and $g(x) = \sum_i g_i x^i$ are polynomials in $R[x]$ then we can find $d, d' \geq 0$ such that $f_i = 0$ if $i > d$ and $g_i = 0$ if $i > d'$.

Therefore, the coefficient of x^k in $f - g$ is zero if $k > \max\{d, d'\}$ and the coefficient of x^l in fg is zero if $l > d + d'$.

Hence, $f - g, fg \in R[x] \implies R[x]$ is a subring of $R[[x]]$. \square

Definition 5.5

Suppose that R is a ring. Then the **ring of polynomials over R in an indeterminate x** is the subring $R[x]$ of $R[[x]]$.

Polynomial rings.../2

The **degree** of $f(x)$ is $\deg f = d$ if d is maximal such that $f_d \neq 0$.

By convention the zero polynomial has degree $-\infty$.

Thus, a polynomial (of degree d) over R in the indeterminate x is a formal expression of the form

$$f(x) = f_0 + f_1 x + f_2 x^2 + \dots + f_d x^d + 0x^{d+1} + \dots$$

Normally, we write $f(x) = f_0 + f_1 x + f_2 x^2 + \dots + f_d x^d$ if $d = \deg f$.

Terms with zero coefficient are usually omitted.

A polynomial $f(x)$ is **not a function**. However, a polynomial

$f(x) = f_0 + f_1 x + f_2 x^2 + \dots + f_d x^d$ determines a function

$$R \rightarrow R; r \mapsto f(r) \stackrel{\text{def}}{=} f_0 + f_1 r + f_2 r^2 + \dots + f_d r^d$$

Warning!!

If $p(x), q(x) \in R[x]$ and $f(x) = p(x)q(x)$ then it is **not** necessarily true that $f(r) = p(r)q(r)$, for all $r \in R$.

For example, let $p(x) = a + bx$ and $q(x) = c + dx$, for $a, b, c, d \in R$, and $f(x) = p(x)q(x) = ac + (ad + bc)x + bdx^2$. Then $f(r) = p(r)q(r)$ if and only if $(ad + bc)r = adr + brc$ and $bdr^2 = brdr$.

Polynomial rings.../3

Example 5.6

Suppose that $R = \text{Mat}_2(\mathbb{Z})$ and that

$$p(x) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} x, \quad q(x) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in R[x].$$

$$\implies f(x) \stackrel{\text{def}}{=} p(x)q(x) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} x$$

Taking $r = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$ we find that $f(r) = \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix}$

whereas, $p(r)q(r) = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} \neq f(r)$!!

- It is possible to have two different polynomials $f(x) \neq g(x) \in R[x]$ which give rise to the same function $R \rightarrow R$; that is, we can find $f(x) \neq g(x)$ such that $f(r) = g(r)$, for all $r \in R$. See question 3 of tutorial 3.
- A formal power series $f(x) \in R[[x]]$ which is not a polynomial does **not** give rise to a function $R \rightarrow R$ because the expression $f(r) = \sum_{i \geq 0} f_i r^i$ is, in general, not meaningful whenever there are an infinite number of non-zero terms in this sum.

Evaluation homomorphisms

For each $r \in R$ define a map $\text{eval}_r : R[x] \rightarrow R$ by mapping the polynomial $p = p(x) \in R[x]$ to $p(r) = \sum_{i \geq 0} p_i r^i$.

Proposition 5.7

Suppose that R is a **commutative ring** and that $r \in R$. Then the map $\text{eval}_r : R[x] \rightarrow R$ is a ring homomorphism.

Proof Suppose that $p(x), q(x) \in R[x]$ and that $r \in R$.

$$\begin{aligned} \text{Then } \text{eval}_r(p + q) &= (p + q)(r) = \sum_{i \geq 0} (p_i + q_i) r^i \\ &= \sum_{i \geq 0} p_i r^i + \sum_{i \geq 0} q_i r^i = p(r) + q(r) \\ &= \text{eval}_r(p) + \text{eval}_r(q) \end{aligned}$$

Note that there are only finitely many non-zero terms here!

Evaluation homomorphisms.../2

$$\begin{aligned} \text{Also, } \text{eval}_r(pq) &= (pq)(r) = \sum_{k \geq 0} \sum_{i+j=k} p_i q_j r^{i+j} \\ &= \sum_{k \geq 0} \sum_{i+j=k} p_i r^i q_j r^j \end{aligned}$$

since R is commutative. Therefore,

$$\begin{aligned} \text{eval}_r(pq) &= \left(\sum_{i \geq 0} p_i r^i \right) \left(\sum_{j \geq 0} q_j r^j \right) \\ &= p(r)q(r) = \text{eval}_r(p) \text{eval}_r(q). \end{aligned}$$

Hence, $\text{eval}_r : R[x] \rightarrow R$ is a ring homomorphism.