Rings and Fields

Tomáš Vávra

Preface

Disclaimer   Much of the information on this set of notes is transcribed directly/indirectly from the lectures of PMATH 334 during Winter 2022 as well as other related resources. I do not make any warranties about the completeness, reliability and accuracy of this set of notes. Use at your own risk.

References:

- Dummit, Foote: *Abstract algebra*.

- http://www.math.uwaterloo.ca/~lwmarcou/notes/pmath334.pdf

- https://notes.sibeliusp.com/pmath347

For any questions, send me an email via https://notes.sibeliusp.com/contact.

You can find my notes for other courses on https://notes.sibeliusp.com/.

Sibelius Peng

Contents

Introduction & Motivation

1.1 Fermat's Last Theorem

> **Fermat's Last Theorem**
>
> The equation $x^m + y^m = z^m$ has no non-trivial solutions in integers for $m \geq 3$.

For example, $(1, 0, 1)$, $(-1, 0, 1)$ for m even, are trivial solutions.

In 1897, Gabriel Lamé announced that he has a proof. First he assumed that m is a prime. He writes

$$z^p = x^p + y^p = (x + y)(x + \zeta_p y)(x + \zeta_p^2 y) \cdots (x + \zeta_p^{p-1} y)$$

where $\zeta_p = \cos(\frac{2\pi}{p}) + i \sin(\frac{2\pi}{p})$. Consider the ring

$$\mathbb{Z}[\zeta_p] = \{a_1 + a_2 \zeta_p + a_3 \zeta_p^2 + \cdots + a_{p-2} \zeta^{p-2} : a_i \in \mathbb{Z}\}$$

which is the smallest ring containing $\mathbb{Z}$ and ζ_p.

Then the next step is to show that $(x + \zeta_p^j y)$'s are coprime in $\mathbb{Z}[\zeta_p]$. Let q_i's be primes.

$$\prod_i q_i^{p\alpha_i} = z^p = (x + y)(x + \zeta_p y) \cdots (x + \zeta_p^{p-1} y)$$

If $(x + \zeta_p^j y)$'s are coprime in $\mathbb{Z}[\zeta_p]$, then $(x + \zeta_p^j y) = (\cdots)^p$ is of p-th power ($*$). But this is wrong if the factorization is non-unique. However, we have $\mathbb{Z}[\zeta_p]$ can be a unique factorization domain (UFD). This means ($*$) works. Kummer salvages the argument for approximately (conjecturally) 60% of prime exponents. And these primes are called regular primes.

1.2 Straightedge and compass construction

We are given a length 1 straightedge ruler, and a compass. With these, we can

- connect two points with a straightedge,

- draw a circle, centered at A, and going through B,

- draw intersections of two line segments, circle & line, two circles.

What lengths are constructible? where length means distance between two points. We can do $+, -, \times, \div, \sqrt{\ }$. Then we can do field extensions:

$$\mathbb{Q} \to \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2}, \sqrt{3}) \to \cdots$$

Is trisection of an angle doable? No, not possible.

Possible to double the cube, square the circle of the same area?

What regular m-gons are constructible? This is equivalent to the question: is $\cos(\frac{2\pi}{m}) + i\sin(\frac{2\pi}{m})$ constructible?

These can be answered via field extensions.

Other applications including coding theory.

An introduction to Rings

2.1 Definitions and basic properties

> **ring**
>
> A ring is a set with two binary operations $+, \times$, such that
>
> 1. $(R, +)$ is an abelian group.
>   - $+$ is commutative and associative.
>   - $\exists 0 \in \mathbb{R}, 0 + a = a + 0 = a$ for all $a \in R$.
>   - $\forall a \in \mathbb{R}, \exists(-a) \in R, a + (-a) = (-a) + a = 0$.
> 2. $\times$ is associative $(a \times b) \times c = a \times (b \times c)$.
> 3. distributive laws hold: $(a + b) \times c = (a \times c) + (b \times c)$.

The ring is called commutative if $\times$ is commutative. The ring is said to have an identity if $\exists 1 \in R$, $1 \times a = a \times 1 = a$, for all $a \in R$, and this does not require the existence of inverse.

For simplicity, we write
$$ab := a \times b, \qquad b - a = b + (-a)$$

Example:

$\mathbb{Z}$ is a commutative ring with identity.

Trivial rings: Let $(R, +)$ be an abelian group. We define $a \times b = 0$ for all $a, b \in R$. The result is a commutative ring with "trivial structure".

$R = \{0\}$ is a zero ring. $0 = 1$ in this case, and it is the only such ring. It leads to assumption $0 \neq 1$, saying $R \neq \{0\}$.

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are commutative rings with identity.

$\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$ with $+, \times \mod m$ is a ring with identity, and commutative.

The real quaternions: $\{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$. Addition is "component-wise". And the multiplication follows
$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j$$

And this is non-commutative ring, with identity 1.

Let X be a set, A be a ring. Consider the set $F = \{f : X \to A\}$. Define

$$(f + g)(x) = f(x) + g(x), \qquad (f \times g)(x) = f(x) \times g(x)$$

F commutative & having identity is inherited from the ring A.

$M_m(\mathbb{Z})$ is the ring of square $m \times m$ matrices with coefficients in $\mathbb{Z}$. It is non-commutative ring with identity.

A function $f : \mathbb{R} \to \mathbb{R}$ is said to have compact support, if $\exists a, b \in \mathbb{R}$, $f(x) = 0$ for $x \notin [a, b]$. $R = \{f : \mathbb{R} \to \mathbb{R} : f$ has compact support$\}$ is a commutative ring, without identity.

Proposition 2.1

Let R be a ring. Then

1. $0a = a0$ for all $a \in R$.

2. $(-a)b = a(-b) = -(ab)$ for all $a, b \in R$.

3. $(-a)(-b) = ab$ for all $a, b \in R$.

4. If R has an identity 1, then it is unique, and $(-a) = (-1)a$.

Proof:
We see that

$$0a = (0 + 0)a = 0a + 0a$$

$$0a - 0a = (0a + 0a) - 0a = 0a + (0a - 0a)$$

$$0a = 0$$

We also see that

$$(-a)b + ab = ((-a) + a)b = 0b = 0$$

$\square$

We would like to be able to cancel with respect to x: $ab = ac$ then $b = c$. However, this is not true in general.

Example:

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

However,

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

2.2 Zero divisor and integral domain

---

zero divisor

A nonzero element $a \in R$ is called a zero divisor, if there exists $b \in R$ and $b \neq 0$, such that $ab = 0$ or $ba = 0$.

> **integral domain**
>
> A commutative ring with identity, $1 \neq 0$, is called an integral domain, if it contains no zero divisor.

> **Proposition 2.2**
>
> Let R be a ring. Assume that $a, b, c \in R$, and a is not a zero divisor. If $ab = ac$, then either $a = 0$ or $b = c$ (i.e., we can multiplicatively cancel).

Proof:
Observe that

$$ab = ac$$
$$ab - ac = 0$$
$$a(b - c) = 0$$

As a is not zero divisor, then either $a = 0$ or $b - c = 0$. □

If zero divisors exist, then cancellation does not hold:

$$ab = 0 = a \cdot 0 \nRightarrow b = 0$$

Remark:
In integral domains, $ab = 0 \implies a = 0$ or $b = 0$.

2.3 Field

> **division ring**
>
> A ring with identity 1, $1 \neq 0$, is called a division ring, if every nonzero element has a multiplicative inverse, i.e., for all $a \in R, a \neq 0$, there exists $b \in R$, such that $ab = ba = 1$.

Consider an example $ab = 1$ existing and $ba = 1$ not existing.

Example:
Real sequences $(x_1, x_2, \ldots)$. Ring of operators on the sequences, $\times$ is composition. Take

$$D : (x_1, x_2, x_3, \ldots) \mapsto (x_2, x_3, x_4, \ldots)$$
$$S : (x_1, x_2, x_3, \ldots) \mapsto (0, x_1, x_2, x_3, \ldots)$$

Then

$$D(S(x_1, x_2, \ldots)) = Id(x_1, x_2, \ldots)$$

but $S \circ D \neq Id$.

> **field**
>
> A commutative division ring is called a field.

Example:
$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields. Quaternions are "only" a division ring because non-commutative. $\mathbb{Z}_p$ is a field for p prime.

> **Proposition 2.3**
>
> Any finite integral domain is a field.

$\mathbb{Z}$ is an integral domain, but far from a field.

Proof:
Check Corollary 10.13 of PMATH 347. □

2.4 Subring

> **subring**
>
> Let R be a ring. A nonzero subset $S \subseteq R$ is called a subring of R, if it is a ring with the operations from $(R, +, \times)$ restricted to S.

That means: $S \neq \varnothing$. $x + (-y) \in S, \forall x, y \in S$. $xy \in S, \forall x, y \in S$.

Example:
$\mathbb{Z}_2 \subseteq \mathbb{Z}$, but $\mathbb{Z}_2$ is not a subring of $\mathbb{Z}$.

$2\mathbb{Z} = \{2 \cdot z : z \in \mathbb{Z}\}$ (ring has no identity) is a subring of $\mathbb{Z}$ (ring has identity).

Ring of matrices $M_2(\mathbb{R})$ (1 is identity matrix) has a subring $S = \left\{ \begin{pmatrix} a & a \\ a & a \end{pmatrix} : a \in \mathbb{R} \right\}$ and

$\begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$ is the identity in S.

2.5 Unit

> **unit**
>
> Assume that R is a ring with an identity $1 \neq 0$. A $a \in R$ is called a unit, if there exists $b \in R$ such that $ab = ba = 1$. Set of units of R is denoted by $R^\times$.

Example:
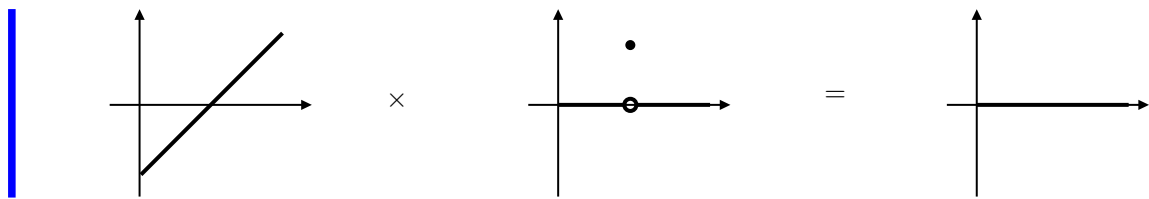$\mathbb{Z}^\times = \{\pm 1\}$

$\mathbb{Z}_m^\times = \{a \in \mathbb{Z}_m : \gcd(a, m) = 1\}$, $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{0\}$ for p prime.

Consider ring R of $[0, 1] \to \mathbb{R}$, where $(f \times g)(x) = f(x) \cdot g(x)$, $1_R = 1(x)$. Units are the functions such that $f(x) \neq 0$ for $\forall x \in [0, 1]$. Then $f(x)^{-1} = \frac{1}{f(x)}$. All non-units are zero divisors. If $g(y) = 0$,

then $h(x) = \begin{cases} 1 & \text{if } x = y \\ 0 & \text{otherwise} \end{cases}$ gives $(g \times h) = 0(x) = 0_R$.

Ring of all continuous functions $[0, 1] \to \mathbb{R}$ is a subring of the previous ring. Units as before, because $1/f$ exists and is continuous.

Consider $f(x) = x - 1/2$.

3

Ring Homomorphisms

> **ring homomorphism**
>
> Let R, S be rings.
>
> 1. A ring homomorphism is $\phi : \mathbb{R} \to S$, such that
>
>   (a) $\phi(a + b) = \phi(a) + \phi(b)$, for all $a, b \in R$.
>
>   (b) $\phi(ab) = \phi(a)\phi(b)$, for all $a, b \in R$.
>
> 2. The kernel of ϕ, $\ker \phi = \{a \in R : \phi(a) = 0_S\}$.
>
> 3. A bijective homomorphism is called isomorphism.

Remark:
Isomorphism means "same ring", denote $R \cong S$.

Example:
$\{0, 1\} = \mathbb{Z}_2 = R$, $S = \{a, b\}$ with $a + a = a, a + b = b, \ldots$ Then $R \cong S$.

Example:
$\mathbb{Q} = \{\frac{a}{b} : a, b \in \mathbb{Z}\}$ with cancellation $\frac{a}{b} = \frac{ca}{cb}$

Can we say $\mathbb{Z} \subseteq \mathbb{Q}$? not in the purest sense. $\mathbb{Z}$ corresponds to $\{\frac{a}{1} : a \in \mathbb{Z}\}$.

$\mathbb{Q}$ contains an isomorphic copy of $\mathbb{Z}$. $S \subseteq \mathbb{Q}$ such that $S \cong \mathbb{Z}$.

Example:
$\phi : \mathbb{Z} \to \mathbb{Z}_2$. $\phi(2k) = 0$, $\phi(2k + 1) = 1$. Then

$$
\begin{aligned}
\ker \phi &= 2\mathbb{Z} \\
\phi^{-1}(0) &= 2\mathbb{Z} = \ker \phi \\
\phi^{-1}(1) &= 1 + 2\mathbb{Z} \\
&= 1 + \ker \phi \\
&= 3 + \ker \phi
\end{aligned}
$$

> **Example:**
>
> $\phi : \mathbb{Z}[x] \to \mathbb{Z} : p(x) \mapsto p(0)$. Then
>
> $$\ker \phi = \phi^{-1}(0) = \{a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + 0 : a_i \in \mathbb{Z}\}$$
> $$= x\mathbb{Z}[x] = \{x \cdot p(x) : p(x) \in \mathbb{Z}[x]\}$$
>
> and
>
> $$\phi^{-1}(a) = x\mathbb{Z}[x] + ax^0 = \ker \phi + ax^0$$

> **Example:**
>
> $\phi : \mathbb{Z}[x] \to \mathbb{Z}_2 : p(x) \mapsto p(0) \bmod 2$. Then
>
> $$\ker \phi = \phi^{-1} = x\mathbb{Z}[x] + 2\mathbb{Z}$$
>
> $$\phi^{-1}(1) = 1 + \ker \phi$$

> **Example:**
>
> $\phi : \mathbb{Z} \to \mathbb{R} : a \mapsto a$, then $\ker \phi = \{0_{\mathbb{R}}\}$.

Proposition 3.1

Let R, S be rings, $\phi : R \to S$ be homomorphism.

1. The image of ϕ, $(\mathrm{Im}(\phi)$, or $\phi(R))$ is a subring of S.

2. $\ker \phi$ is a subring of R. Moreover, $\forall r \in R, \forall \alpha \in \ker \phi, r\alpha \in \ker \phi, \alpha \in \ker \phi$. (That is $\ker \phi$ is closed under multiplication by the elements from R)

> **Proof:**
>
> 1. If $a, b \in \phi(R)$, then
>
> $$a - b = \phi(x_a) - \phi(x_b) = \phi(x_a - x_b) = \phi(x_{a-b}) \in \phi(R)$$
>
> 2. $\phi(r\alpha) = \phi(r) \cdot \phi(\alpha) = \phi(r) \cdot 0 = 0$

$\square$

Can we get a ring structure on $a + \ker \phi$? There is a factor ring $R/\ker \phi$. For example, $\mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}_2$.

3.1   Ideals & Quotient rings

---

ideal

Let R be a ring, let $I \subseteq R$ be a subring, let $r \in R$.

1. I is called a left ideal, if $rI \subseteq I$ where $rI = \{ri : i \in I\}$.

2. I is called a right ideal, if $Ir \subseteq I$.

3. I is an ideal, if it is left & right ideal (two sided ideal).

Ideal Test

Check K is an ideal of R:

- $k - j \in K$ for all $j, k \in K$; and

- $rk, kr \in K$ for all $k \in K, r \in R$.

It is a quick generalization of previous definition. Reference: Laurent W. Marcoux's 334 notes.

additive quotient

Let $I \subseteq R$ be an ideal. The additive quotient is defined as $R/I = \{a + I : a \in R\}$.

Example:

$\mathbb{Z}/3\mathbb{Z} = \{\{\ldots, -6, 3, 0, 3, 6, \ldots\}, \{\ldots, -5, -2, 1, 4, \ldots\}, \{\ldots, -4, -1, 2, 5, 8, \ldots\}\}$. Additive group.

Let $I = 3\mathbb{Z}$. Then $a + I$ are called (additive) cosets.

Proposition 3.2

Let R be a ring, I an ideal of R, then R/I is a ring with the operations

$$(a + I) +_{R/I} (b + I) =: (a +_R b) + I$$

$$(a + I) \times_{R/I} (b + I) = (a \times_R b) + I$$

The ring properties R/I follow from R being a ring.

quotient ring

R/I is called the quotient ring of R by I.

Remark:

If I is not an ideal, then the definition of the operations on R/I is not well defined.

Example:

Let R be commutative ring with identity $1 \neq 0$, $m \geq 2$. Let $M_m(R)$ be ring of square matrices with coefficients in R.

Denote

$$L_j(R) = \{A \in M_m(R) \mid A_{ik} = 0, \forall i \in [n], k \in [m] \setminus \{j\}\}$$

which means only the j-th column can have non-zero entries. Then $L_j(R)$ is a left ideal in $M_m(R)$. This can be verified by the matrix multiplication. $L_j(R)$ is not a right ideal, i.e., $L_j(R) \cdot M \notin L_j(R)$ for some $M \in M_m(R)$.

Analogously, a right ideal can be obtained by taking

$$T_i(R) = \left\{A \in M_m(R) \,\middle|\, A_{kj} = 0, \forall k \in [n] \setminus \{i\}, j \in [m]\right\}$$

Example:

Let $R = \mathbb{Z}[x]$ and $I = x^2\mathbb{Z}[x]$.

Then $R/I = \{a + bx + p(x) : a, b \in \mathbb{Z}, p(x) \in I\}$.

For $a \in R/I$, $\bar{a}$ denotes $a + I$.

3.2 Isomorphism theorems

> **Lemma 3.3**
>
> Let I be an ideal in R, then $a + I = b + I$ ($\bar{a} = \bar{b}$) if and only if $b - a \in I$. Namely, every member of the coset can be the representative.

> **Theorem 3.4: First isomorphism theorem**
>
> If $\phi : R \to S$ is a ring homomorphism, then $\ker \phi$ is an ideal in R, Im ϕ is a subring of S, and $R/\ker \phi \cong \text{Im } \phi$.

Proof:
Theorem 4.2 of http://www.math.uwaterloo.ca/~lwmarcou/notes/pmath334.pdf

Consider $\tau : R/\ker \phi \to \phi(R) : r + \ker \phi \mapsto \phi(r)$. $\qquad \square$

Example:
$\mathbb{Z}[x]/2\mathbb{Z}[x] \cong \mathbb{Z}_2[x]$. We can define $\phi : p(x) \mapsto p(x) \mod 2$.

> **Theorem 3.5**
>
> For any ideal $I \subseteq R$, the map $R \to R/I$ defined by $\pi : r \mapsto r + I$ is a surjective ring homomorphism with kernel I. It is called the natural projection of R onto R/I. Thus every ideal is a kernel of some homomorphism.

Proof:
Prove surjectivity is as before in first iso theorem. The prove homomorphism, both $\times$ and $+$. Now prove $\ker \phi$.

- Let $i \in I$, then $\pi(i) = i + I = I = 0_{R/I}$.

- Let $a \in R/I$, then $\pi(a) = a + I$, but $a \notin I$. Thus by lemma, $a + I \neq I = 0 + I$. $\qquad \square$

> **Theorem 3.6: Second isomorphism theorem**
>
> Let A be a subring of R, B an ideal of R. Then $A + B = \{a + b : a \in A, b \in B\}$ is a subring of R. $A \cap B$ is an ideal of R and $(A + B)/B \cong A/A \cap B$.

Proof:
Consider the map $\phi : A \to (A + B)/B : a \mapsto a + B$. Then apply first isomorphism theorem.

Or check Theorem 4.3 of http://www.math.uwaterloo.ca/~lwmarcou/notes/pmath334.pdf. $\qquad \square$

Remark:
$(A + B)/B = \{a + b + B : a \in A, b \in B\} = \{a + B : a \in A\} \stackrel{?}{=} A/B$

This reduction can't happen because B is not necessarily an ideal of A.

> Example:
>
> Let $R = \mathbb{Z}$, then $a\mathbb{Z} + b\mathbb{Z} = \gcd(a,b) \cdot Z$. $a\mathbb{Z} \cap b\mathbb{Z} = \operatorname{lcm}(a,b) \cdot \mathbb{Z}$. Then by second iso thm
>
> $$\frac{\gcd(a,b)\mathbb{Z}}{b\mathbb{Z}} \cong \frac{a\mathbb{Z}}{\operatorname{lcm}(a,b)\mathbb{Z}}$$

Lemma 3.7

If $m \mid n$, then $m\mathbb{Z}$ is an ideal of $m\mathbb{Z}$, and $|m\mathbb{Z}/n\mathbb{Z}| = \frac{n}{m}$.

The coset representative in $(m\mathbb{Z}/n\mathbb{Z})$ are $\{0, m, 2m, \ldots, (\frac{n}{m} - 1)m\}$. Applying to $A + B/B \cong A/A \cap B$, we have

$$\frac{b}{\gcd(a,b)} = \frac{\operatorname{lcm}(a,b)}{a} \implies ab = \operatorname{lcm}(a,b) \cdot \gcd(a,b)$$

Theorem 3.8: Third isomorphism theorem

Let $I \subseteq J$ be ideals in R. Then J/I is an ideal in R/I and $(R/I)/(J/I) \cong R/J$.

> Proof:
>
> Define $\phi : R/I \to R/J : a + I \mapsto a + J$. Then show that $\ker \phi = J/I$ and then use first isomorphism theorem.
>
> Or check Theorem 4.4 of http://www.math.uwaterloo.ca/~lwmarcou/notes/pmath334.pdf   □

> Example:
>
> $(\mathbb{Z}/6\mathbb{Z})/(3\mathbb{Z}/6\mathbb{Z}) \cong \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}_3$.

Theorem 3.9: Fourth isomorphism theorem/correspodence theorem

Let R be ring, I ideal in R. The correspondence $A \leftrightarrow A/I$ is an inclusion preserving bijection between the set of subrings (A) of R, $I \subseteq A \subseteq R$, and the set of subrings of R/I. Furthermore, A/I is an ideal in R/I if and only if A is an ideal in R $(I \subseteq A)$.

> Proof:
>
> No first isomorphism theorem. Expand and verify the definitions.   □

The interesting part is: subring of R/I gives subring of R.

4

More on Ideals

Let $A \subseteq R$ with identity.

> **(A)**
>
> 1. $(A) =$ the smallest ideal containing A (in R)
>
> 2. Let
>
> $$RA = \left\{ \sum r_i a_i : r_i \in R, a_i \in A \right\}$$
> $$AR = \left\{ \sum a_i r_i : r_i \in R, a_i \in A \right\}$$
> $$RAR = \left\{ \sum r_i a_i r_i' : r_i, r_i' \in R, a_i \in A \right\}$$
>
> where these are all finite sums.
>
> 3. If $A = \{a\}$, then $(A) =: (a)$ is called a principal ideal.
>
> 4. If an ideal $I = (A)$ for A finite, we call I finitely generated.

Remark:

$$(A) = \bigcap_{\substack{I \text{ ideal of } R \\ A \subseteq I}} I$$

The intersection is indeed an ideal.

$(A) \subseteq \cap I$ because (A) is the smallest. $\cap I \subseteq (A)$ because it contains $I = (A)$.

Note that $\cup I_\alpha$ is not an ideal in general.

What is (A)?

Assume R is commutative. Then (A) contains $a \in R$, and also $ra, r \in R, a \in R$, and their sums. This is precisely the definition of RA. Thus $RA \subseteq (A)$.

Note that $1 \in R$. Then $A \subseteq RA$, and RA is an ideal itself. By minimality, $(A) \subseteq RA$.

To conclude, $(A) = RA = AR = RAR$ in the commutative case.

In particular, the principal ideal $(A) = a \cdot R = \{ar : r \in R\}$, because let $A = \{a\}$, we have

$$AR = \left\{ \sum ar_i : r_i \in R \right\} = \left\{ a \left(\sum r_i \right) : r_i \in R \right\}$$

works in commutative rings.

Warning   In non-commutative rings, we have $(A) = RAR$, so

$$(a) = RaR \neq \{r_i a r_i' : r_i, r_i' \in R\}$$

Example:

$R = \mathbb{Z}$, the principal ideal (m) is $m\mathbb{Z}$.

Example:

Let $R = \{f : [0,1] \to \mathbb{R}\}$. Then $I = \{f \in R : f(1/2) = 0\}$ is an ideal. And $I = (g)$ where

$$g(x) = \begin{cases} 0 & \text{if } x = 1/2 \\ 1 & \text{otherwise} \end{cases}$$

For $h \in I$, $h = g \cdot h \in (g)$. Note that g is an identity element of I, but not of R.

Example:

$C = \{f : [0,1] \to \mathbb{R} \mid f \text{ is continuous}\}$ is a subring of R. $I = \{f \in C : f(1/2) = 0\}$ is again an ideal. BUT! I is not a principal ideal, I is not even finitely generated (not easily proven).

Note that I here is different from last example, where the instructor made a mistake at first.

Example:

Let $R = \mathbb{Q}[x]$. Consider subring $S = x\mathbb{Q}[x] + \mathbb{Z}$. An ideal $I = x\mathbb{Q}[x]$.

1. $I = (x)$ in R

2. I is an ideal in S where I is not finitely generated

If I is finitely generated in S, then there exists $p_1, \ldots, p_k \in I$

$$I = (p_1, \ldots, p_k) = \left\{ \sum_{i=1}^{k} p_i(x) q_i(x) : q_i \in S \right\}$$

As p_i are in ideal $I = x\mathbb{Q}[x]$, p_i don't have constant term. However, this is not possible. Take an element $\frac{a}{b} x \in I$, then

$$\frac{a}{b} x = \sum_{i=1}^{k} p_i(x) q_i(x)$$

As p_i's are fixed, one need to find proper q_i's to make this equation hold. Now consider b to be a prime such that b does not divide the product of denominators of p_i's, then it's impossible to find any q_i's to make this equation holds. Therefore I is not a finite generated ideal in S.

Proposition 4.1

Let I be an ideal in R with identity $1 \neq 0$.

1. $I = R$ if and only if I contains a unit.

2. Let R be commutative. Then R is a field if and only if the only ideals in R are 0 and R.

Proof:

Statement 1

($\Rightarrow$) Because $1 \in R = I$, and 1 is a unit.

($\Leftarrow$) Let $u \in I$ be a unit. Then $u \cdot u^{-1} = 1 \in I$. Let $r \in I$, as $1 \in I$, then $1 \cdot r \in I$, hence $I = R$.

Statement 2

($\Rightarrow$) Let $0 \neq I \subseteq R$ be an ideal. Then it contains a unit. Then by (1), $I = R$.

($\Leftarrow$) Take arbitrary $0 \neq r \in R$. The ring (r) can't be zero ideal, hence $(r) = R$. Thus $1 \in (r)$. That means there exists $s \in R$, such that $1 = r \cdot s$. Then $s = r^{-1}$. Hence r is a unit. $\qquad\square$

Corollary 4.2

A nonzero homomorphism from a field to a ring is an injection.

Proof:

Let ϕ be such a homomorphism. $\ker \phi$ is an ideal of the field. This implies $\ker \phi = 0$ (injective homomorphism) or R, the whole field. And the second possibility tells us ϕ is a zero map, which is eliminated by the assumption. $\qquad\square$

4.1 Maximal ideals

---

maximal ideal

An ideal M is an arbitrary ring R is called a maximal ideal if $M \neq R$ and there is no proper ($\neq R$) ideal I, $M \subseteq I \subseteq R$.

Alternatively, ideal I of a ring R is maximal if the only ideals containing I are I and R.

Theorem 4.3

Assume that R ring is commutative. The ideal M is maximal if and only if R/M is a field.

Proof:

By 4th iso thm, or correspondence theorem, R/M is a field $\Leftrightarrow$ ideals of R/M are zero ideals and $R/M \Leftrightarrow$ only ideals of R containing M are M and $R \Leftrightarrow M$ is maximal. $\qquad\square$

Example:

$p\mathbb{Z}$ is maximal ideal for any p prime.

Theorem 4.4

$p\mathbb{Z}$ is maximal if and only if $\mathbb{Z}/p\mathbb{Z}$ is a field.

Example:

$(2, x)$ in $\mathbb{Z}[x]$ is maximal. $\mathbb{Z}[x]/(2, x) \cong \mathbb{Z}_2$ because $(2, x)$ is a kernel of $\phi : p(x) \mapsto p(0) \bmod 2$.

Example:

Let $R = \{f : [0, 1] \to \mathbb{R}\}$ and $M_c = \{f \in R : f(c) = 0\}$. Consider $\phi : R \to \mathbb{R} : f \mapsto f(c)$. Then $\ker \phi = M_c$. As $\mathbb{R} = \phi(R)$, then $R/M_c \cong \mathbb{R}$ is a field. Hence M_c maximal.

4.2 Maximal ideals and Zorn's Lemma

Consult Section 10.3 of PMATH 347 if needed.

Is every ideal (proper) contained in some maximal ideal? No. Consider $\mathbb{Q}$ with standard $+$ and $a \times b = 0_+$ for all $a, b \in \mathbb{Q}$. We have ideals

$$\left\{ \frac{a}{2} : a \in \mathbb{Z} \right\} \subseteq \left\{ \frac{a}{4} : a \in \mathbb{Z} \right\} \subseteq \cdots \subseteq \left\{ \frac{a}{2^k} : a \in \mathbb{Z} \right\} \subseteq \cdots$$

These ideals are not contained in a maximal ideal. This happens because there's no identity.

Theorem 4.5

In a ring with an identity, every proper is contained in some maximal ideal.

Wrong idea   Given I, then $I \subseteq \bigcup_{\substack{I \subseteq A \\ A \neq R}} A$. But this is not an ideal. For example, $\mathbb{Z}_6 \subseteq \mathbb{Z}_2 \cup \mathbb{Z}_3$ is not an ideal.

Right idea $I \subseteq \bigcup_{A \in C} A$ for C being a "chain"

$$I \subseteq A_1 \subseteq A_2 \subseteq \cdots \subseteq A_m \subseteq \cdots$$

---

partial order

A partial order on a set S is a relation on X such that

1. $a \leq a$ for all $a \in S$,

2. If $a \leq b$ and $b \leq a$ then $a = b$ for all $a, b \in S$,

3. If $a \leq b$ and $b \leq c$, then $a \leq c$ for all $a, b, c \in S$.

So set inclusion $\subseteq$ is a partial order.

The ordering does not have to be "linear": sth $\leq$ sth $\leq$ sth $\leq \cdots$. For sets, we can have

$$
\begin{array}{ccc}
\{a, b\} & \subseteq & \{a, b, d\} \\
\end{array}
$$

$$\{a\} \qquad\qquad\qquad\qquad \{a, b, c, d, e\}$$

$$
\begin{array}{ccc}
\{a, c\} & \subseteq & \{a, c, e\} \\
\end{array}
$$

A chain C in a partially ordered set $(S, \leq)$ is a subset such that for all $x, y \in C$, $x \leq y$ or $y \leq x$ (i.e., all elements are comparable).

Zorn's Lemma

Let $(S, \leq)$ be a partially ordered set with the property that each chain has an upper bound in S. Then S contains a maximal element.

Theorem 4.6

Let R be a ring with 1. Then every proper ideal I is contained in some maximal ideal.

Let $F = \{J : J$ is a **proper** ideal of $R, M \subseteq J\}$. Notice $(F, \subseteq)$ is a poset (partially ordered set). Recall some notations/definitions:

- Chain: subset $G \subseteq F$, s.t. $\forall x, y \in G$, $x \subseteq y$ or $y \subseteq x$ (comparable)

- Upper bound of $G \in F$, $m \in F$, s.t. $\forall g \in G$, $g \subseteq m$.

- Maximal in F: $m \in F$, s.t. $\forall a \in F$, $(m \leq a) \implies (a = m)$.

Let $C \subseteq F$ be a chian. Put $M := \bigcup_{a \in C} A$. M is an ideal because

1. nonempty: $A \in C$, $I \subseteq A$, then $I \in M$.

2. Let $a \in A, b \in B$, and $A, B \in C$. WLOG, assume $A \subseteq B$. Then $a, b \in B$, then $a - b \in B$, then $a - b \in M$.

3. $\forall r \in R, a \in M$, we have $a \in A \in C$, then $ra \in A$, $ra \in M$.

We claim that M is an upper bound of C in F. If $M = R$, then $1 \in A \in C$. But then by proposition, $A = R$. Contradiction.

Then apply Zorn lemma.

Or check proposition 10.8 of PMATH 347. □

Polynomial Rings & Rings of Fractions

5.1   How to make new rings from old rings?

I don't want to put this section to the previous chapter. So here it is.

Direct products

Let $(R_i, +_i, \times_i)$ be rings. $R_1 \times R_2$ is a ring with

$$(r_1, r_2) \oplus (s_1, s_2) = (r_1 +_1 s_1, r_2 +_2 s_2)$$
$$(r_1, r_2) \otimes (s_1, s_2) = (r_1 \times_1 s_1, r_2 \times_2 s_2)$$

Then this applies to $\prod_i R_i$ (works for at most countable R_i's).

Direct sum

For finitely many R_i's, it is just direct product. For infinitely many R_i's

$$\bigoplus_{i \in I} R_i = \left\{ (r_1, r_2, r_3, \ldots) : r_i \in R_i, \text{ only finitely many } r_1 \neq 0 \right\}$$

5.2   Basic Definitions and Examples

Let R be a commutative ring with identity. A polynomial with coefficients in R with undeterminate/-variable x is a **formal** expression

$$p(x) = a^n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

with $a_i \in R$, $\forall i \in 0, \ldots, n$. If $a_m \neq 0$, then $\deg p = n$. If $a_n = 1$, we call $p(x)$ monic.

$R[x] = \{ a^n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 : n \in \mathbb{N}, a_i \in R \}$ with operations

$$\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} b_i x^i = \sum_{i=0}^{n} (a_i + b_i) \, x^i$$

$$\left(\sum_{i=0}^{n} a_i x^i \right) \times \left(\sum_{i=0}^{m} b_i x^i \right) = \sum_{k=0}^{n+m} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) x^k$$

Observe that R appears in $R[x]$ as constant polynomials. $R[x]$ is commutative ring with identity.

> **Proposition 5.1**
>
> Let R be an integral domain, let $p, q \in R[x]$ be nonzero elements. Then
>
> 1. $\deg pq = \deg p + \deg q$
>
> 2. the units of $R[x]$ are precisely the units of R.
>
> 3. $R[x]$ is an integral domain.

Proof:

$$p(x)q(x) = \underbrace{a_n b_m}_{\neq 0} x^{n+m} + \cdots$$

Let $p(x) \in R[x]$ be invertible, then there exists q such that $pq = 1$. By (1), $\deg p = 0$. Thus $\deg q = 0$. p, q are constant polynomials.

$pq = 0$, then $\deg p + \deg q = 0$. Then $\deg p = \deg q = 0$. Then they are all constant polynomials. As R is integral domain, we have $p = q = 0$. $\qquad \square$

Formal power series

Ring of all power series $R[[x]] = \left\{ \sum_{i=0}^{\infty} a_i x^i : a_i \in R \right\}$ with the same operations defined as polynomial rings.

1. $R[[x]]$ is a commutative ring identity.

2. Units of $R[[x]]$ are $\sum_{i=0}^{\infty} a_i x^i$ with a_0 unit in R.

Laurent series

$$R((x)) = \left\{ \sum_{i=N}^{\infty} a_i x^i : a_i \in R, N \in \mathbb{Z} \right\}$$

5.3 Rings of fractions

Construct $\mathbb{Q}$ from $R = \mathbb{Z}$. Define

$$\mathbb{Q} = \left\{ \frac{p}{q} : p, q \in \mathbb{Z}, q \neq 0 \right\}$$

$\frac{p}{q}$ is a "formal" fraction. ($p \cdot q^{-1}$ does not work). However, $\frac{1}{1}, \frac{2}{2}, \frac{3}{3}$ are distinct formal fractions. We want to have them be in equivalent classes.

We define $\frac{a}{b} \sim \frac{c}{d}$ iff $ad = bc$ (use only the ring operations). Then define $\mathbb{Q}$ be the equivalence classes of $\sim$. For that, we need to show that $\sim$ is equivalence: reflexive, symmetric, transitive.

We define addition as

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

is well-defined on equivalence classes. We can obtain $+$ on the equivalence classes through definition of $+$.

We define multiplication as

$$\frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}$$

is well-defined on equivalence classes.

Then we obtain $\mathbb{Q}$. Note that the well-definednesses need a proof. See Section 11.1 of PMATH 347.

$\frac{2}{1}, \frac{1}{2} \in \mathbb{Q}$, then $\frac{2}{1} \cdot \frac{1}{2} = \frac{2}{2} \sim \frac{1}{1}$ is an identity. Thus 2 is invertible in $\mathbb{Q}$. Every integer is a unit in $\mathbb{Q}$.

If R have zero divisors, $ab = 0$ and $a, b \neq 0$. Then if a invertible: $1 = a^{-1} \cdot a$, then $b = a^{-1}(a \cdot b) = 0$. Contradiction. Thus **zero divisors do not have inverses in any ring**. Now consider

$$a = \frac{a}{1} = \frac{ab}{b} = \frac{0}{b} = 0$$

contradiction to $a \neq 0$. Thus we will avoid zero divisors.

> **Theorem 5.2**
>
> Let R be a commutative ring. Let D be any subset of R closed under multiplication and not containing zero divisors and 0. Then there exists a commutative ring Q with identity such that Q contains R as a subring and every element of D is a unit of Q. Moreover,
>
> 1. every element of Q is of the form $\frac{r}{d}$ for some $r \in R, d \in D$. If $D = R \setminus \{0\}$, then Q is a field.
>
> 2. The ring Q is the smallest ring containing R in which all elements of D are units.

Here we formalize the definition of "smallest": Let S be any commutative ring with identity and let $\phi : R \to S$ be any injective homomorphism such that $\phi(d)$ is a unit of S for each $d \in D$. Then there is an injective homomorphism $\Phi : Q \to S$ such that $\Phi_R = \phi$. In other words, any ring containing an isomorphic copy of R in which elements of D become units must contain Q.

$$R \overset{id}{\hookrightarrow} Q$$

with ϕ injective and Φ injective mapping to S.

Thus $R "\subseteq" S$.

6

Chinese Remainder Theorem

to be filled later.

7

Domains

7.1 Euclidean Domains

> **norm**
>
> A norm on a ring R is a function $N : \mathbb{R} \to \mathbb{Z}^+ \cup \{0\}$, s.t. $N(0) = 0$.

> **Euclidean domain**
>
> An integral domain (identity, commutative, no zero divisors) for which there exists a Norm, such that: $\forall a, b \in R$, $b \neq 0$, there exists $q, r \in R$ s.t. $a = qb + r$ with $N(r) < N(b)$ or $r = 0$. This is called a Euclidean domain.

Example:

$R = \mathbb{Z}$, $N(x) = |x|$. Then $a = qb + r$ follows from division with remainder. We don't have to keep r positive/negative.

Example:

Fields with $N(x) = 0$. We have $a = (ab^{-1})b = 0$

Example:

F a field. Then $F[x]$ is a Euclidean domain with $N(p(x)) = \deg(p(x))$. Then we can have polynomial long division.

Example:

Consider Gaussian integers.
$$Z[i] = \{a + bi : a, b \in \mathbb{Z}\}$$
is ED with $N(a + bi) = a^2 + b^2 = (a + bi)(a - bi)$.

> **Theorem 7.1**
>
> Every ideal in a Euclidean domain is principal.

Proof:
Let $I \subseteq R$ an ideal. Take a nonzero element d in I of the smallest norm. Let $x \in I$, then $x = qd + r$ where $N(r) = 0$ or $N(r) < N(d)$. But $N(r) < N(d)$ is not possible. So $N(r) = 0$. Since $r = x - qd \in I$, then we must have $r = 0$. Then $x = qd$. This holds for any $x \in I$. Thus $I = (d)$. $\qquad\square$

Remark:
Every ideal is principal: principal ideal domain (PID). We have ED $\subseteq$ PID, not other way around.

---

greatest common divisor

Let R be commutative.

1. We say that $b \mid a$ (b divides a), if there exists $x \in R$, $a = bx$.

2. $d \in R$ is called a $\gcd(a, b)$ if

   $*$) $d \mid a, d \mid b$

   $\triangle$) if $d' \mid a$ and $d' \mid b$, then $d' \mid d$.