Rings and Fields

PMATH 334

Tomáš Vávra

LaTeXed by Sibelius Peng

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.

For the table of contents, I am most likely following Dummit, Foote: *Abstract algebra*.

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

1

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.

2

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 $x \notin [a, b]$. $R = \{f : \mathbb{R} \to \mathbb{R} : f \text{ has compact support}\}$ 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

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

□

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 $b - c = 0$. $\square$

If zero divisors exist, then cancellation does not hold:

$$ab = 0 = a \cdot 0 \not\Rightarrow b = 0$$

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. $\square$

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 $R^\times$.

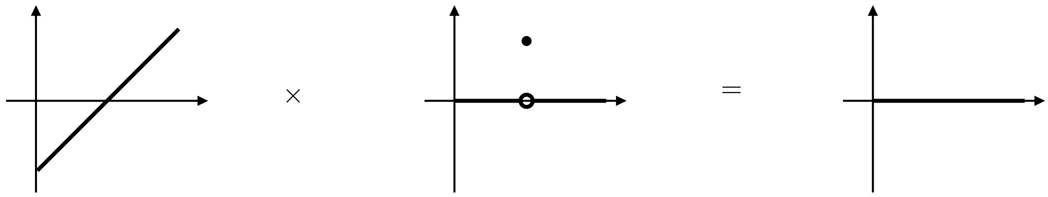
Example:
$\mathbb{Z}^\times = \{\pm 1\}$

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

$$\begin{aligned}\ker\phi = \phi^{-1}(0) &= \{a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + 0 : a_i \in \mathbb{Z}\} \\ &= x\mathbb{Z}[x] = \{x \cdot p(x) : p(x) \in \mathbb{Z}[x]\}\end{aligned}$$

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, $\phi : \mathbb{R} \to \S$ be homomorphism.

1. The image of ϕ, (Im(ϕ), 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 x 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. $\phi(r\alpha) = \phi(r) \cdot \phi(\alpha) = \phi(r) \cdot 0 = 0$

□

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 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).

additive quotient

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

Example:

$\mathbb{Z}/3\mathbb{Z} = \{\{\dots, -6, 3, 0, 3, 6, \dots\}, \{\dots, -5, -2, 1, 4, \dots\}, \{\dots, -4, -1, 2, 5, 8, \dots\}\}$. 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 $\tau : R/\ker\phi \to \phi(R) : r + \ker\phi \mapsto \phi(r)$. ☐

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 $a \in R \setminus I$, then $\pi(a) = a + I$, but $a \notin I$. Thus by lemma, $a + I \neq I = 0 + I$.

☐

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. ☐

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 $a\mathbb{Z} + b\mathbb{Z} = \gcd(a,b) \cdot \mathbb{Z}$. $a\mathbb{Z} \cap b\mathbb{Z} = \text{lcm}(a,b) \cdot \mathbb{Z}$. Then by second iso thm

$$\frac{\gcd(a,b)\mathbb{Z}}{b\mathbb{Z}} \cong \frac{a\mathbb{Z}}{\text{lcm}(a,b)\mathbb{Z}}$$

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 idea; 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.

Index