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

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

Then the next step is to show that $(x + \zeta_p^? y)$ are coprime.

$$q_1^{\alpha_1} q_2^{\alpha_2} \cdots = z^p = (x+y)(x+\zeta_p y)\cdots(\quad)$$

Then $(x + \zeta_p y) = (\cdots)^p$ $(*)$. But this is wrong if the factorization is non-unique. However, we have

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

can be a unique factorization domain (UFD). This means $(*)$ works. Kummer salvages the argument for approximately 60% of prime exponents.

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: $ab = ac \implies b = c$. However, this is not true in general.

Index

R