Algebraic Number Theory
代数的整数論

Topics in Mathematical Science IV (数理科学特論 IV), Nagoya University, Fall 2021

Henrik Bachmann (Math. Building Room 457, henrik.bachmann@math.nagoya-u.ac.jp)
Lecture notes and exercises are available at: https://www.henrikbachmann.com/algnt_2021.html

---

注意：These notes are under construction and therefore may contain mistakes and change without notice. If you find any typos/errors or have any suggestions, please let me know!

Already a big thanks to Vic Austen for helping to prepare these notes.

Contents

1 Introduction & Basics

We will start by giving a short answer to the question **"What is Algebraic number theory?"**. There are several possible answers to this question. As the name suggests, it is number theory with the help of algebraic methods. Algebraic number theory is the study of **algebraic number fields** [代数体], which are field extensions $K/\mathbb{Q}$ of finite degree. In these number fields, we will be in particular interested in the **ring of integers of** K [整数環], denoted by $\mathcal{O}_K$. This ring of integers takes the same place in K as the usual integers do in the rational numbers, i.e., in particular $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$. The integers $\mathbb{Z}$ satisfy a lot of nice properties. For example, $\mathbb{Z}$ is a unique factorization domain (UFD) [一意分解環], i.e., any element can be written uniquely (up to units) as a product of irreducible elements, which are given by the prime numbers. As we will see, not every ring of integers $\mathcal{O}_K$ will be an UFD. This problem will be solved by considering ideals in $\mathcal{O}_K$. We will see that on the level of ideals, we will again have a kind of unique factorization property.

$$\begin{array}{ccc} \mathbb{Q} & \hookrightarrow & K \\ \uparrow & & \uparrow \\ \mathbb{Z} & \hookrightarrow & \mathcal{O}_K \end{array}$$

Examples 1.1. Example of number fields K and their ring of integers $\mathcal{O}_K$.

(i) The field extension $K = \mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{C}\}$ has degree $[K : \mathbb{Q}] = \dim_{\mathbb{Q}} K = 2$ and is therefore a number field. Its ring of integers is $\mathcal{O}_K = \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{C}\}$. These are the so-called **Gaussian integers** and we will study their properties in the first section.

(ii) We will see that for the number field $K = \mathbb{Q}(\sqrt{5})$ the ring of integers is given by $\mathcal{O}_K = \mathbb{Z}\left[\frac{\sqrt{5}+1}{2}\right]$.

Version 1 (October 11, 2021)

(iii) The ring of integers for $K = \mathbb{Q}(\sqrt{-5})$ is $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. This ring is not a UDF, since for example in this ring we can write 6 in two different ways

$$6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 + \sqrt{-5})$$

and 2,3, $(1 + \sqrt{-5})$ and $(1 + \sqrt{-5})$ are all irreducible elements in this ring.

The next question one might ask is, why one should care about algebraic number field, and one could therefore ask **"Why is Algebraic number theory?"**. Algebraic number fields appear naturally when studying **Diophantine equations**. These are polynomial equations where one is interested in integer solutions.

Examples 1.2. Here are some examples of Diophantine equations. For a more detailed overview see [IR, Chapter 17] and [KKS, Chapter 1].

i) Linear Diophantine equation: Given $a, b, c \in \mathbb{Z}$ find all $x, y \in \mathbb{Z}$ with

$$ax + by = c\,.$$

It is an easy exercise to show that a solution for given a, b, c exists if and only if c divides the greatest common divisor of a and b, which we denote by $\gcd(a, b)$.

ii) Pell's equation: Given a non-square integer n we consider

$$x^2 - ny^2 = 1. \tag{1.1}$$

It was then shown by Lagrange (1768): For any non-saure n the equation (1.1) has infinitely many distincts solutions $x, y \in \mathbb{Z}$.

iii) Sum of four squares: For any positive integer $n \in \mathbb{N}$ one can ask if this integer can be written as a sum of four squares, i.e. if one can find $a, b, c, d \in \mathbb{Z}$ such that

$$a^2 + b^2 + c^2 + d^2 = n\,. \tag{1.2}$$

Again Lagrange (1770) showed: (1.2) has a solution for any n. For example, we have

$$2021 = 0^2 + 1^2 + 16^2 + 42^2 = 1^2 + 18^2 + 20^2 + 36^2\,.$$

In particular we see that there can be several different solutions for some n. The question of how many solutions there are for a given n was answered by Jacobi (1893): If $r_4(n) = \#\{a, b, c, d \in \mathbb{Z} \mid (1.2)\}$ then

$$r_4(n) = 8 \sum_{\substack{m|n \\ 4 \nmid m}} m\,.$$

This result can be proven by using modular forms for the congruence subgroup $\Gamma_0(4)$ (See Todo: add reference).

iv) Sum of two squares: Instead of the sum of four squares one can also consider the sum of two squares. Clearly not every number can be written as a sum of two squares, since 3 is already the first counter-example. We will discuss in detail how to determine if a prime is a sum of two squares in Section 1.1, by using methods of algebraic number theory.

v) Fermat's last theorem: For a given $n \geq 1$ consider the equation

$$x^n + y^n = z^n \,. \tag{1.3}$$

For $n = 1$ this equation is trivial to solve and for $n = 2$ one can find infinitely many integer solutions, the so-called **Pythagorean triples**. A few examples are given by $3^2 + 4^2 = 5^2$ or $5^2 + 12^2 = 13^2$. In 1637 Pierre de Fermat claimed that (1.3) has no non-trivial integer solutions (meaning $x \cdot y \cdot z \neq 0$) if $n \geq 3$. It took more than 300 years until Andrew Wiles gave a proof of this claim in 1994 (Todo: add reference).
Todo: Include timetable of events around FLT and add more history.

1.1 Primes as a sum of two squares and some ring theory

In this section we will answer the question when a prime is a sum of two squares. The first few examples are

$$2 = 1^2 + 1^2, \quad 5 = 1^2 + 2^2, \quad 13 = 2^3 + 3^2, \quad 17 = 1^2 + 4^2, \ldots \,.$$

For some primes, such as $3, 7$ or 11, this is not possible. This follows from the following simple observation: Any square is congruent to 0 or 1 modulo 4. Therefore if a prime is a sum of two squares, it can just be congruent to 0,1 or 2 modulo 4. But since it is prime, it can never be congruent to 0 modulo 4 and 2 is the only prime that can be congruent to 2 modulo 4. Therefore any prime $p \geq 3$, which is the sum for two squares, has to be congruent to 1 modulo 4. It was first shown by Fermat that also the converse is true:

Theorem 1.3. *A prime $p \geq 3$ can be written as a sum of two squares if and only if $p \equiv 1 \mod 4$.*

To prove this theorem, we will leave the ring of integers and work in a larger ring. Before doing this, we will recall some basic notations from algebra.

Definition 1.4. (i) A **ring** [環] is a triple $(R, +, \cdot)$ of a set R together with two binary operations $+$ (addition) and $\cdot$ (multiplication), such that

- $(R, +)$ is an abelian group [アーベル群].
  (i.e. $+$ is commutative and associative, there exists a neutral element $0 \in R$ and for each $a \in R$ an inverse $-a \in R$ with $a + (-a) = 0$.)
- $(R, \cdot)$ is a semigroup [半群].
  (i.e. $\cdot$ is associative)
- Addition and multiplication satisfy the distributive law [分配律]

$$a \cdot (b + c) = a \cdot b + a \cdot c$$
$$(a + b) \cdot c = a \cdot c + b \cdot c$$

for all $a, b, c \in R$. If $\cdot$ is commutative, we call R a **commutative ring** [可換環]. Instead of $(R, +, \cdot)$ we will usually just write R.

(ii) A ring R is **unitary** [単位環] if there exists a $1 \in R$ with $1 \cdot a = a \cdot 1 = a$ for all $a \in R$. In other words $(R, \cdot)$ is a monoid [モノイド].

(iii) Let R, S be rings. A **ring homomorphism** [環準同型] is a map $\varphi : R \to S$, such that for all $a, b \in R$

$$\varphi(a+b) = \varphi(a) + \varphi(b), \quad \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b). \tag{1.4}$$

If R, S are unitary one usually considers unitary ring homomorphisms which in addition satisfy $\varphi(1) = 1$.

(iv) A (non-zero) commutative ring R is called an **(integral) domain** [整域] if for all $a, b \in R$ the equation $a \cdot b = 0$ implies $a = 0$ or $b = 0$.

Usually, all rings we consider in this course will be commutative and unitary if not stated otherwise.

Examples 1.5. (i) $\mathbb{Z}, \mathbb{R}[X], \mathbb{C}[X]$ are integral domains

(ii) $\mathbb{Z}/6\mathbb{Z}$ is not an integral domain since $\overline{2} \cdot \overline{3} = \overline{6} = \overline{0}$.

(iii) The ring of Gaussian integers $\mathbb{Z}[i] = \{a + bi \mid a, b, \in \mathbb{Z}\} \subset \mathbb{C}$ is a domain.

In the ring $\mathbb{Z}[i]$ the equation $p = x^2 + y^2$ can be written as

$$p = (x + iy)(x - iy)\,. \tag{1.5}$$

Definition 1.6. (i) An element $a \in R$ in an (unital) ring R is called a **unit** [可逆元] if there exists $b \in R$ with $a \cdot b = 1$.

(ii) $R^\times$ denotes the set of all units of R and $(R^\times, \cdot)$ is a group, the **unit group** [単元群].

(iii) If R is commutative and $R^\times = R \backslash \{0\}$ then R is called a **field** [体].

Examples 1.7. (i) $\mathbb{Z} = \{1, -1\}$.

(ii) If R is a domain then $R[X]^\times = R^\times$. If R is not a domain there are also non-constant polynomials which can be units. For example, in the case $R = \mathbb{Z}/4\mathbb{Z}$ we have $(1 + 2X)^2 = 1$ in $R[X]$ and therefore $1 + 2X \in R[X]^\times$.

(iii) One can show (Homework 1) that the units of the Gaussian integers are $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$.

Definition 1.8. (i) An element $a \in R$ with $a \notin R^\times$ is called **irreducible** [既約元] if from $a = b \cdot c$ we obtain $b \in R^\times$ or $c \in R^\times$.

(ii) An element $p \in R \backslash \{0\}$ with $p \notin R^\times$ is called **prime** [素元] if whenever $p \mid a \cdot b$ then $p \,|\, a$ or $p \,|\, b$.

In HW1, we prove that in an (integral) domain, every prime element is irreducible.
However, the converse is not always true. For example, in the domain $R = \mathbb{Z}[\sqrt{-5}]$, 2 is irreducible, and

$$6 = 2 \cdot 3 = (1 - \sqrt{-5})(1 + \sqrt{-5})\,,$$

but $2 \nmid (1 - \sqrt{-5})$ and $2 \nmid (1 + \sqrt{-5})$, so 2 is not prime.

Until here in lecture 1 (8th October, 2021)

Algebraic Number Theory Dictionary

In this section, we give an English-Japanese-German dictionary for important words in Algebraic Number Theory. There exists a nice dictionary for general mathematical terms (English-Japanese) by D. Zagier, which can be found here:
`http://people.mpim-bonn.mpg.de/zagier/files/scanned/EnglishJapaneseDictMathTerm/fulltext.pdf`.

(Please anyone feel free to add words here)

English	**Japanese**	**German**
Algebraic number theory	代数的(だいすうてき) 整数論(せいすうろん)	Algebraische Zahlentheorie
field	体(たい)	Körper
ring	環(かん)	Ring
Algebraic number field	代数体(だいすうたい)	Algebraischer Zahlkörper
—		-
—		-
—		-
—		-

References

[IR] Kenneth Ireland, Michael Rosen, A Classical Introduction to Modern Number Theory, *Graduate Texts in Mathematics*, Second Edition, Springer-Verlag, Berlin.

[KKS] Kazuya Kato (加藤 和也), Nobushige Kurokawa (黒川 信重), Takeshi Saito (斎藤 毅), 数論〈*1*〉*Fermat* の夢と類体論 単行本, Tankobon Hardcover 2005/1/7.
English version: *Number Theory 1: Fermat's Dream*, Translations of Mathematical Monographs, Vol 186, First Edition.

[N] Jürgen Neukirch, Algebraic Number Theory, *Grundlehren der Mathematischen Wissenschaften* 322. Springer-Verlag.

[ST] Ian Stewart, David Tall, Algebraic Number Theory and Fermat's Last Theorem, *Chapman and Hall/CRC* 4th edition.