Introduction to Algebraic Number Theory Part III

A. S. Mosunov

University of Waterloo
Math Circles

November 21st, 2018

RECALL

- We learned how to generalize **rational integers** and today we will look at the generalization of **rational numbers**.
- We looked at **quadratic rings**, like $\mathbb{Z}[\sqrt{2}]$ or $\mathbb{Z}\left[\frac{-1+\sqrt{-3}}{2}\right]$, and today we will look at more general rings, like $\mathbb{Z}[\sqrt[3]{2}]$.
- Also, we learned that in certain algebraic rings the unique factorization can fail. For example, in $\mathbb{Z}[\sqrt{-5}]$:

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

  Today we will see how the unique factorization can be fixed with the **theory of ideals**.

GENERALIZING RATIONAL INTEGERS

Algebraic Numbers and Their Minimal Polynomials

- A number α is called **algebraic** if there exists a non-zero polynomial $f(x)$ with rational coefficients such that $f(\alpha) = 0$. Otherwise it is called **transcendental**.
- For each algebraic number α there exists the unique **minimal polynomial**

$$f(x) = c_d x^d + c_{d-1} x^{d-1} + \ldots + c_1 x + c_0.$$

  This polynomial satisfies the following five properties:
  1. $f(\alpha) = 0$;
  2. $c_0, c_1, \ldots, c_d \in \mathbb{Z}$;
  3. $c_d > 0$;
  4. $\gcd(c_0, c_1, \ldots, c_d) = 1$;
  5. $f(x)$ has the smallest degree d among all polynomials satisfying the conditions 1), 2), 3) and 4).
- We say that an algebraic number α has **degree** d, denoted $\deg \alpha$, if its minimal polynomial has degree d.

Algebraic Numbers and Their Minimal Polynomials

- **Example.** Consider the number $\sqrt{2}$. This number is algebraic, since $\sqrt{2}$ is a root of the polynomial $f(x) = x^2 - 2$. In fact, $f(x)$ is the minimal polynomial of $\sqrt{2}$. Note that it is also a root of

$$\begin{aligned} f_1(x) &= 0, \\ f_2(x) &= \tfrac{1}{2}x^2 - 1, \\ f_3(x) &= -x^2 + 2, \\ f_4(x) &= x^3 + 3x^2 - 2x - 6, \\ f_5(x) &= 6x^2 - 12. \end{aligned}$$

However, none of these polynomials satisfy the definition of a minimal polynomial.

EXERCISES

Exercises

- **Exercise 1.** For each $\alpha \in \left\{0, 1/2, i, \sqrt{\sqrt{2}+\sqrt{3}}\right\}$ find a non-zero polynomial such that $f(\alpha) = 0$ and then determine an upper bound on $\deg \alpha$.
- **Exercise 2.** Prove that every rational number has degree 1.
- **Exercise 3.** Prove that every quadratic irrational has degree 2. In other words, show that every number α of the form $a + b\sqrt{d}$, where $a, b, d \in \mathbb{Q}$ and $d \neq r^2$ for any $r \in \mathbb{Q}$, satisfies some non-zero polynomial $f(\alpha) = 0$ of degree 2 and does not satisfy any polynomial of degree 1.

Number Fields

- Let α be an algebraic number of degree d. The set

$$\mathbb{Q}(\alpha) = \{a_{d-1}\alpha^{d-1} + \ldots a_1\alpha + a_0 \colon a_{d-1}, \ldots, a_1, a_0 \in \mathbb{Q}\}$$

  is called a **number field** generated by α.
- **Example.** Gaussian rationals:

$$\mathbb{Q}(i) = \{a + bi \colon a, b \in \mathbb{Q}\},$$

  where i is a root of $x^2 + 1 = 0$.
- **Example.** Here is the first example of a **cubic field**:

$$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \colon a, b, c \in \mathbb{Q}\}.$$

- Every **field** is also a **ring**: you can add, subtract and multiply there. However, the division by a non-zero element is now allowed as well.

Number Fields

- **Example.** In order to divide two Gaussian rationals, we use the trick called **multiplication by a conjugate**. For example,

$$\frac{8+i}{1+i} = \frac{(8+i)(1-i)}{(1+i)(1-i)} = \frac{9-7i}{N(1+i)} = \frac{9}{2} - \frac{7}{2}i.$$

  In particular, we see that this number is not a Gaussian integer, so $1+i$ does not divide $8+i$.

- **Exercise 4.** Consider the ring of Eisenstein rationals $\mathbb{Q}(\omega)$, where $\omega^2+\omega+1=0$. The number $a-b-b\omega$ is called a **conjugate** of $a+b\omega$. Note that

$$N(a+b\omega) = a^2 - ab + b^2 = (a+b\omega)(a-b-b\omega).$$

  Use multiplication by a conjugate to compute $\frac{4+5\omega}{1+2\omega}$ and $\frac{1-4\omega}{1-2\omega}$. Determine whether $1+2\omega \mid 4+5\omega$ or $1-2\omega \mid 1-4\omega$.

Rings of Integers

- An algebraic number α is an **algebraic integer** if the leading coefficient of its minimal polynomial is equal to 1.
- **Example.** The numbers $\sqrt{2}, \frac{-1+\sqrt{-3}}{2}$ are algebraic integers because their minimal polynomials are $x^2 - 2$ and $x^2 + x + 1$, respectively.
- **Example.** The number $\cos\left(\frac{2\pi}{7}\right)$ is not an algebraic integer because its minimal polynomial is $8x^3 + 4x^2 - 4x - 1$.
- **Fact:** The set of all algebraic numbers forms a field, denoted by $\overline{\mathbb{Q}}$. The set of all algebraic integers forms a ring.
- Let α be an algebraic integer. Then the set of all algebraic integers of $\mathbb{Q}(\alpha)$ is called the **ring of integers** of $\mathbb{Q}(\alpha)$. It is denoted by $\mathscr{O}$.
- The ring $\mathscr{O}$ inside a number field $\mathbb{Q}(\alpha)$ is a natural generalization of the ring $\mathbb{Z}$ inside the field $\mathbb{Q}$.

Rings of Integers

- **Exercise 5.** Show that $\mathbb{Q}(\sqrt{5}) = \mathbb{Q}(\sqrt{5}+k)$ for any integer k.
- **Exercise 6.** Show that $\mathbb{Z}[\sqrt{2}]$ is the ring of integers of $\mathbb{Q}(\sqrt{2})$ by proving that every $a+b\sqrt{2}$, where either a or b is not an integer, necessarily has a minimal polynomial whose leading coefficient is greater than 1.
- **Exercise 7.** Show that $\mathbb{Z}[\sqrt{5}]$ is **not** the ring of integers of $\mathbb{Q}(\sqrt{5})$ by finding $a+b\sqrt{5} \in \mathbb{Q}(\sqrt{5})$, where either a or b is not an integer, whose minimal polynomial has leading coefficient equal to 1.
- **Conclusion.** The ring of integers $\mathscr{O}$ always contains

$$\mathbb{Z}[\alpha] = \{a_{d-1}\alpha^{d-1} + \dots a_1\alpha + a_0 \colon a_{d-1}, \dots, a_1, a_0 \in \mathbb{Z}\}$$

but need not be equal to it. Determining the ring of integers of a given number field can be quite difficult.

The Norm Map

- Every number field $\mathbb{Q}(\alpha)$ admits a multiplicative norm.
- **Example.** For n a positive rational number, consider $z = a + b\sqrt{-n} \in \mathbb{Q}(\sqrt{-n})$. Then $z = a + b\sqrt{n}i$ is a complex number and its conjugate is

$$\bar{z} = a - b\sqrt{-n}.$$

  We define $N(z) = |z|^2 = z\bar{z}$. Then the multiplicativity of N follows from the properties of an absolute value.
- **Example.** Consider the ring of Gaussian integers $\mathbb{Z}[i]$. Then the conjugate of $a + bi$ is $a - bi$, and so

$$N(a+bi) = |a+bi|^2 = (a+bi)(a-bi) = a^2 + b^2.$$

- **Exercise 8.** Let $\mu = \frac{1+\sqrt{-7}}{2}$. Determine the conjugate of $a + b\mu$ in $\mathbb{Z}[\mu]$. Write down the norm map on $\mathbb{Z}[\mu]$.

General Fields and Norms

- More generally, if α is an algebraic number and

$$f(x) = c_d x^d + \ldots + c_1 x + c_0$$

its minimal polynomial, then the number c_0/c_d is precisely the norm of α.

- **Example.** If a, b are integers, the minimal polynomial of a number $a + b\sqrt{2}$ is $x^2 - 2ax - (a^2 - 2b^2)$. Therefore the norm on $\mathbb{Z}[\sqrt{2}]$ is $N(a + b\sqrt{2}) = a^2 - 2b^2$.
- **Example.** The norm on

$$\mathbb{Z}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \colon a, b, c, \in \mathbb{Z}\}$$

is

$$N(a + b\sqrt[3]{2} + c\sqrt[3]{4}) = a^3 - 6abc + 2b^3 + 4c^3.$$

DETOUR

Detour: Abel-Rufini Theorem

- So far, we have been working with algebraic numbers like $0, \frac{3}{2}, i, \frac{1+\sqrt{-3}}{2}$, etc. These numbers can be **expressed in radicals**, i.e. they can be written in terms of addition, subtraction, multiplication, division and root extraction.
- **Degree 2.** The solutions to $ax^2 + bx + c = 0$ are
$$\frac{-b+\sqrt{b^2-4ac}}{2a} \text{ and } \frac{-b-\sqrt{b^2-4ac}}{2a}.$$
- **Degree 3.** Cardano's formula (1545): one of the roots of $x^3 + px + q$ is
$$x = \sqrt[3]{-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}.$$
- **Degree 4.** There is an analogous formula for degree 4, see the Wikipedia article on "Quartic function".
- **Question.** Can all algebraic numbers be expressed in radicals?

Detour: Abel-Rufini Theorem

- **Answer: No.** This is asserted by the Abel-Ruffini Theorem. In 1799 Paolo Ruffini made an incomplete proof and in 1824 Niels Henrik Abel provided a complete proof.
- **Example.** The roots of $x^5 - x + 1$, such as

$$\alpha \approx -1.1673039782614\ldots,$$

  are not expressible in radicals.
- It also follows from the Abel-Ruffini Theorem that for every rational number r the numbers $\sin(r\pi)$ and $\cos(r\pi)$ are expressible in radicals.
- **Example.**

$$\cos\left(\frac{\pi}{48}\right) = \frac{1}{2}\sqrt{2+\sqrt{2+\sqrt{2+\sqrt{3}}}}.$$

Detour: Abel-Rufini Theorem

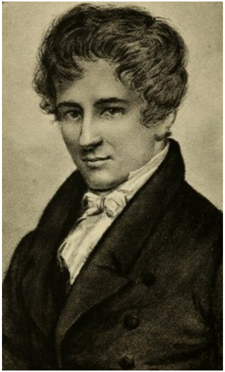


Figure: Paolo Ruffini (left) and Niels Henrik Abel (right)

FIXING UNIQUE FACTORIZATION

Ideals

- Recall how the unique factorization fails in $\mathbb{Z}[\sqrt{-5}]$. We will explain how to fix it by introducing **ideals**.
- Let $\mathbb{Q}(\alpha)$ be a number field and let $\mathscr{O}$ be its ring of integers. A subset I of $\mathscr{O}$ is called an **ideal** if
    1. $0 \in I$;
    2. If $\alpha, \beta \in I$ then $\alpha - \beta \in I$;
    3. If $\alpha \in I$ and $\beta \in \mathscr{O}$ then $\alpha\beta \in I$.
- The most important property is 3: an ideal I **absorbs multiplication by the elements of $\mathscr{O}$**.
- If there exists $\alpha \in \mathscr{O}$ such that $I = \{\alpha\beta \colon \beta \in \mathscr{O}\}$ then I is called a **principal ideal** and it is denoted by $I = (\alpha)$. The number α is called the **generator** of I.
- **Example.** Consider an ideal (2) in $\mathbb{Z}$. We have $(2) = \{2n \colon n \in \mathbb{Z}\}$, so the ideal (2) consists of all even numbers. Further, for any $2k \in (2)$ and any $n \in \mathbb{Z}$ we have $2kn$ even, so $2kn \in (2)$. Therefore (2) absorbs multiplication by the elements of $\mathbb{Z}$.

Ideals

- Let I and J be ideals of $\mathscr{O}$. We say that I **divides** J, denoted $I \mid J$, if $I \supseteq J$.
- An ideal I is called **prime** if
  1. $I \neq \mathscr{O}$;
  2. For any $\alpha, \beta \in \mathscr{O}$ such that $\alpha\beta \in I$ either $\alpha \in I$ or $\beta \in I$.
- **Exercise 9.** Prove that (0) and $\mathscr{O}$ are ideals of $\mathscr{O}$.
- **Exercise 10.** Show that $(3), (5)$ and (6) are ideals in $\mathbb{Z}$. Prove that $(3) \mid (6)$ and $(5) \nmid (6)$. Prove that (3) and (5) are prime ideals and (6) is not a prime ideal.
- A ring $\mathscr{O}$ where every ideal is principal is called the **Principal Ideal Domain** (PID).
- For rings of integers of number fields, the **Unique Factorization Domain** and the **Principal Ideal Domain** is the same thing.

Ideal Arithmetic

- Every ideal has generators and there are finitely many of them. For $\alpha_1, \ldots, \alpha_n \in \mathscr{O}$, we use the notation

$$(\alpha_1, \ldots, \alpha_n) = \{a_1\alpha_1 + \ldots + a_n\alpha_n \colon a_1, \ldots, a_n \in \mathscr{O}\}$$

  to denote the ideal generated by $\alpha_1, \ldots, \alpha_n$.
- **Example.** Note that in $\mathbb{Z}$ we have $(4, 6) = (2)$.
- **Example.** In $\mathbb{Z}[\sqrt{-5}]$ there is an ideal $(2, 1 + \sqrt{-5})$, which is **not** a principal ideal.
- **Addition.** If I, J are ideals in $\mathscr{O}$ then we can compute their sum, which is also an ideal:

$$I + J = \{\alpha + \beta \colon \alpha \in I,\ \beta \in J\}.$$

- **Multiplication.** If $I = (\alpha_1, \ldots, \alpha_m), J = (\beta_1, \ldots, \beta_n)$ are ideals in $\mathscr{O}$ then we can compute their product, which is an ideal:

$$IJ = (\alpha_1\beta_1, \alpha_1\beta_2, \ldots, \alpha_m\beta_{n-1}, \alpha_m\beta_n).$$

Unique Factorization of Ideals

- (Special case of) **Dedekind's Theorem.** Every ideal I of $\mathscr{O}$ can be written uniquely (up to reordering) as the product of prime ideals.
- **Example.** In $\mathbb{Z}$ we have $(6) = (2)(3)$.
- **Example.** Though in $\mathbb{Z}[\sqrt{-5}]$ we have

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

so unique factorization fails, the unique factorization of ideals holds:

$$\begin{aligned}
(6) &= (2, 1+\sqrt{-5})^2(3, 1+\sqrt{-5})(3, 1-\sqrt{-5}) \\
(2) &= (2, 1+\sqrt{-5})^2 \\
(3) &= (3, 1+\sqrt{-5})(3, 1-\sqrt{-5}) \\
(1+\sqrt{-5}) &= (2, 1+\sqrt{-5})(3, 1+\sqrt{-5}) \\
(1-\sqrt{-5}) &= (2, 1+\sqrt{-5})(3, 1-\sqrt{-5}).
\end{aligned}$$

Open Problems in Algebraic Number Theory

- There are many big open problems in algebraic number theory, but we will present only two of them.
- An integer d is **squarefree** if it is not divisible by a perfect square > 1. For example, 6 is squarefree but 12 is not because $4 \mid 12$.
- **Gauss's class number problem.** There are infinitely many squarefree integers $d > 0$ such that the ring of integers of a real quadratic field $\mathbb{Q}(\sqrt{d})$ is a UFD.
- **The Cohen-Lenstra Heuristics.** In 1993–84, Cohen and Lenstra gave a heuristic argument that "approximately" 75.446% of real quadratic fields are UFD's. There is a lot of computational evidence that their conjecture is true, but why it is true is still unknown.

DETOUR

Detour: Kummer's Progress on Fermat's Last Theorem

- **Fermat's Last Theorem**. For every $n \geq 3$ the equation $x^n + y^n = z^n$ has no solutions in positive integers x, y, z.
- This "theorem" was stated without proof by Fermat in 1670 and proved by Andrew Wiles and Richard Taylor in 1995.
- It is sufficient to prove the theorem for $n = 4$ (done by Fermat) and for every n that is an odd prime.
- If p is an odd prime, then there exists an algebraic integer ζ_p of degree $p - 1$ whose minimal polynomial is

  $$x^{p-1} + x^{p-2} + \ldots + x + 1.$$

  The roots of this polynomial are $\zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}$.
- This number is called the **primitive p-th roof of unity**, as it satisfies $\zeta_p^p = 1$.

Detour: Kummer's Progress on Fermat's Last Theorem

- Note that for every prime p we can write

$$z^p = x^p + y^p = (x+y)\prod_{i=1}^{p-1}(x+\zeta_p^i y).$$

  Therefore we factored $x^p + y^p$ over $\mathbb{Z}[\zeta_p]$.
- This reminds us of Euler's idea for solving $y^2 = x^3 - 2$! If $\mathbb{Z}[\zeta_p]$ is a UFD then each number

$$x+y,\ x+\zeta_p y,\ \ldots,\ x+\zeta_p^{p-1}y$$

  is a perfect p-th power.
- In 1847 Gabriel Lamé outlined the proof of Fermat's Last Theorem based on this method. Liouville pointed out that his premise that $\mathbb{Z}[\zeta_p]$ is a UFD is false.
- Using this method, in 1850 Ernst Kummer proved that FLT is true for all **regular** primes.

Detour: Kummer's Progress on Fermat's Last Theorem

- To understand the statement of Kummer's Theorem we need to introduce just two more definitions.
- Two ideals I and J of $\mathscr{O}$ are **equivalent**, written $I \sim J$, if there are $\alpha, \beta \in \mathscr{O}$ such that $(\alpha)I = (\beta)J$.
- Ideals that are equivalent to each other form an **equivalence class**. The number of equivalence classes of $\mathscr{O}$ is always finite and it is called the **class number**, denoted by $h(\mathscr{O})$.
- The ring of integers $\mathscr{O}$ is a UFD if and only if $h(\mathscr{O}) = 1$.
- **Example.** In $\mathbb{Z}$ we have $(2) \sim (3)$ because $(3)(2) = (2)(3)$. The class number of $\mathbb{Z}$ is 1.
- **Example.** In $\mathbb{Z}[\sqrt{-5}]$ we have $(2, 1+\sqrt{-5}) \sim (3, 1+\sqrt{-5})$. The class number of $\mathbb{Z}[\sqrt{-5}]$ is 2, so it is not a UFD.

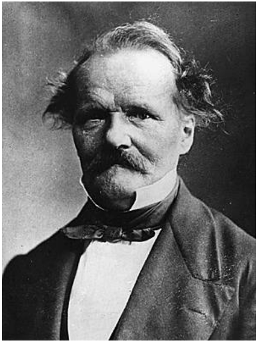
Detour: Kummer's Progress on Fermat's Last Theorem

- An odd prime p is **regular** if it does not divide $h(\mathbb{Z}[\zeta_p])$. It is called **irregular** otherwise.
- **Kummer's Theorem.** (1850) FLT is true for regular primes.
- The first 10 irregular primes are

$$37, 59, 67, 101, 103, 131, 149, 157, 233, 257.$$

- In 1915, Jensen proved that there are infinitely many irregular primes.
- **Siegel's Conjecture.** (1964) "Approximately" 60.65% of all primes are regular. (BIG OPEN PROBLEM!)

Detour: Kummer's Progress on Fermat's Last Theorem



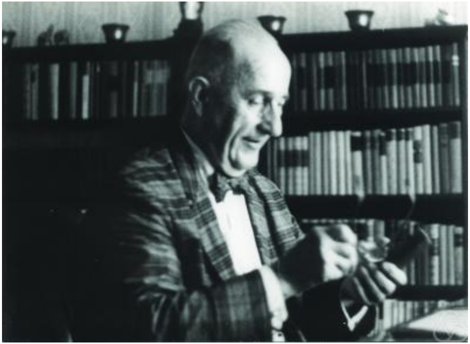


Figure: Ernst Kummer (left) and Carl Ludwig Siegel (right)

THANK YOU FOR COMING!