MAT4250 fall 2018: Algebraic number theory (with a view toward arithmetic geometry)

Håkon Kolderup

Welcome to MAT4250, a course on algebraic number theory. This fall we aim to cover the basic concepts and results of algebraic number theory, as well as giving a first taste of arithmetic geometry by proving the arithmetic Riemann–Roch theorem. Exercises will be provided roughly at a biweekly basis. The prerequisite for this course is (an equivalent of) MAT4200 – Commutative Algebra.

In order to give an idea of what algebraic number theory is about, let us proceed with a short informal discussion on the history of the subject, some of its aims, and a few of its central results. Most of the stated results will be proved later in the lectures. Keeping the "view toward arithmetic geometry" in mind, we will also provide a few remarks on the connection between number theory and geometry. These remarks are not necessary in order to understand the material, so those who are unfamiliar with algebraic geometry may safely ignore them. On the other hand, if you do know some algebraic geometry, the geometric remarks provide a small hint on the extent to which Grothendieck's algebraic geometry unifies number theory and geometry.

1 What is algebraic number theory?

In order to answer this question, let us start by investingating the roots of the subject. Algebraic number theory can be traced back to the third century AD in which the Greek mathematician Diophantus of Alexandria made significant contributions to the study of integer solutions to algebraic equations. Almost 2000 years later this particular problem still bears Diophantus' name: indeed, a polynomial equation of the form

$$f(x_1, \dots, x_n) = 0,$$

where $f \in \mathbf{Z}[X_1, \dots, X_n]$, and where we require that $(x_1, \dots, x_n) \in \mathbf{Z}^n$, is called a *Diophantine equation*. For example, the problem of finding all Pythagorean triples (that is, all right triangles with integer side lengths) precisely asks for the solutions of the Diophantine equation $x^2 + y^2 = z^2$. To this particular equation there are infinitely many solutions $(x, y, z) = (p^2 - q^2, 2pq, p^2 + q^2)$, as was known already to Euclid. More generally, in the 17^{th} century, Pierre de Fermat undertook the study of the Diophantine equation

$$x^n + y^n = z^n, \tag{1}$$

for $n \geq 1$ a natural number. He stated his famous "Fermat's Last Theorem", namely that once n is larger than 2, this Diophantine equation has no (nontrivial) solutions. The case $n = 4$ was certainly known to Fermat, but his infamous proof of the general case for which "the margin was too narrow" is widely believed to be nonexistent. Indeed, it took over 300 years and the collective contributions of several outstanding mathematicians before the British mathematician Andrew

Wiles in 1994 finally settled the Diophantine problem posed by Fermat. Wiles' solution to the problem—for which he was awarded the Abel price in 2016—heavily exploits the underlying geometry of the Diophantine equation. Very roughly speaking, a solution to (1) for $n > 2$ is known to give rise to an elliptic curve with very special properties—in fact, so special that Wiles could prove that such elliptic curves cannot exist.

1.1 Factorization in Z and other rings of integers

The *fundamental theorem of arithmetic* states that every nonzero integer n can be factored into a product of primes,

$$n = \pm p_1 \cdots p_m,$$

and that this factorization is *unique*; that is, if $n = \pm q_1 \cdots q_r$ is another factorization, then $m = r$ and we may reorder the q_i's such that $p_i = \pm q_i$ for each i. In other words, the primes occuring in the factorization of n are unique up to ordering and unit multiples.

At the Paris Academy the French mathematician Gabriel Lamé announced in 1847 a proposed proof of Fermat's Last Theorem. The basic idea was to factor the polynomial $X^p + Y^p$, for p an odd prime, using p-th roots of unity. More precisely, if ζ denotes a primitive p-th root of unity, we have the factorization

$$X^p + Y^p = (X + Y)(X + \zeta Y) \cdots (X + \zeta^{p-1} Y)$$

in the ring $\mathbf{Z}[\zeta]$. Hence a solution (x, y, z) to Fermat's equation would satisfy

$$\prod_{j=0}^{p-1} (x + \zeta^j y) = z^p.$$

Lamé then continued to show that all the terms $x + \zeta^j y$ are relatively prime. Since the product equals z^p, it follows that all the terms must be p-th powers. From this Lamé could derive a contradiction.

The flaw in Lamé's argument was that it relies on the assumption that unique factorization—as we have in $\mathbf{Z}$—also holds for the ring $\mathbf{Z}[\zeta]$. This is *not* true: starting with $p = 23$, the analogue of the fundamental theorem of arithmetic no longer holds in the ring $\mathbf{Z}[\zeta_{23}]$ (and in a certain sense, as p increases it only gets worse from here). This leads to the following fundamental question:

Question 1.1. For which rings of integers do we have unique factorization?

One of the basic goals of algebraic number theory is to answer this question. However, before even attempting to give an answer, we must specify what we mean by "rings of integers". By what we have seen above, this notion should at least contain all the rings $\mathbf{Z}[\zeta_n]$, for ζ_n an n-th root of unity. Now, all the roots of unity ζ_n share the property that they are roots of polynomials of the form $X^n - 1$, i.e., monic polynomials with integral coefficients. In other words, ζ_n is *integral* over $\mathbf{Z}$. So an element of some "ring of integers" should be something that is integral over $\mathbf{Z}$. A nice way to obtain such elements is to start with an algebraic field extension $K/\mathbf{Q}$ of the rational numbers, and then consider the integral closure A of $\mathbf{Z}$ in K. This situation is so common in algebraic number theory that both the ring A and the field K are given names of their own:

Definition 1.2. An *algebraic number field* is a finite field extension K of the field $\mathbf{Q}$ of rational numbers, contained in the complex numbers $\mathbf{C}$. The *ring of integers in* K, commonly denoted $\mathcal{O}_K$, [1] is the integral closure of $\mathbf{Z}$ in K.

[1] The "$\mathcal{O}$" in the notation $\mathcal{O}_K$ goes back to Dedekind, and stands for the German word *ordnung*. The notation reflects the fact that the ring $\mathcal{O}_K$ is an order in the sense of commutative algebra.

It was Richard Dedekind who abstracted the common features shared by all the rings $\mathcal{O}_K$ for varying number fields K, allowing for a proper generalization of the notion of "rings of integers". Nowadays, these objects go under the name *Dedekind rings*:

Definition 1.3. A *Dedekind ring* is a noetherian, integrally closed integral domain of Krull dimension 1.

Dedekind rings are the fundamental objects of study in algebraic number theory. Of course, we have the following result that ensures that the notion of a Dedekind ring generalizes the above situation of rings of integers in number fields:

Proposition 1.4 ([Neu99, I Theorem 3.1])**.** *Let A be a Dedekind ring with field of fractions K. Suppose that L is a finite field extension of K and let B be the integral closure of A in L. Then B is a Dedekind ring.*

Remark 1.5. Geometrically, the condition for a ring A to be a Dedekind ring means that $X := \operatorname{Spec} A$ is a nonsingular affine curve. Indeed, if $x \in X$ is a closed point, then $\mathcal{O}_{X,x}$ is a DVR if and only if $\mathcal{O}_{X,x}$ is integrally closed (see, e.g., [AM69, Proposition 9.2]), and being integrally closed is a local property.

Example 1.6. The following rings are Dedekind:

$$\mathbf{Z}; \quad \mathbf{Z}[\sqrt{-1}]; \quad \mathbf{Z}[\zeta_p]; \quad \mathbf{Z}[\sqrt{3}]; \quad \mathbf{Z}\left[\frac{1+\sqrt{5}}{2}\right]; \quad \mathbf{R}[x,y]/(x^2+y^2-1).$$

On the other hand, $\mathbf{Z}[\sqrt{5}]$ and $\mathbf{C}[x,y]/(x^2-y^3)$ are examples of 1-dimensional noetherian integral domains that are not Dedekind rings. Indeed, they are not integrally closed (or, equivalently, they are the coordinate rings of singular curves).

Exercise 1.7. Let d be a squarefree integer. Show that the integral closure of $\mathbf{Z}$ in $\mathbf{Q}(\sqrt{d})$ is

- $\mathbf{Z}[\sqrt{d}]$ if $d \not\equiv 1 \pmod 4$;
- $\mathbf{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ if $d \equiv 1 \pmod 4$.

The following "fundamental theorem of Dedekind rings" states that an analogue of the fundamental theorem of arithmetic (albeit for ideals) holds in any Dedekind ring:

Theorem 1.8 ([Neu99, I Corollary 3.3])**.** *Let A be a Dedekind ring and $\mathfrak{a} \subseteq A$ a proper ideal. Then*

$$\mathfrak{a} = \prod_{\mathfrak{p}\ prime} \mathfrak{p}^{\operatorname{ord}_{\mathfrak{p}}(\mathfrak{a})},$$

where the $\operatorname{ord}_{\mathfrak{p}}(\mathfrak{a})$'s are uniquely determined integers.

In other words, any proper ideal in A can be written uniquely as a product of powers of prime ideals.

Now we are ready to return to Question 1.1. As we have seen, not all of the rings $\mathbf{Z}[\zeta_n]$ are unique factorization domains. A more straightforward example is $\mathbf{Z}[\sqrt{-5}]$ (which is Dedekind by Exercise 1.7), in which the element 6 admits two distinct factorizations, namely $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$.

Proposition 1.9. *A Dedekind ring is a unique factorization domain if and only if it is a principal ideal domain.*

The above proposition suggests that we can define a measure of how far a Dedekind ring A is from being a UFD by taking the set of all ideals and modding out by the principal ideals. In order for this to work properly (in particular, in order to obtain an abelian group rather than just a set) we need to include a bit more than just the ideals in A:

Definition/Proposition 1.10. Let A be a Dedekind ring, with field of fractions K. A *fractional ideal*[2] of A is a nonzero finitely generated A-module $\mathfrak{a}$ contained in K.

Let J_K denote the set of fractional ideals of A. For each $\mathfrak{a} \in J_K$, let

$$\mathfrak{a}^{-1} := \{x \in K^\times : x\mathfrak{a} \subseteq A\}.$$

Then J_K is an abelian group under multiplication, with identity element $(1) = A$. Let

$$P_K := \{(a) : a \in K^\times\}$$

denote the subgroup of J_K consisting of *principal fractional ideals*. We define the *class group of* A (also referred to as the class group of K)[3] as the quotient group

$$\mathrm{Cl}_K := J_K/P_K.$$

The order of Cl_K is called the *class number* of K, and is often denoted h_K.

Thus a Dedekind ring is a UFD if and only if its class group is trivial. Moreover, the class group fits into an exact sequence

$$1 \to A^\times \to K^\times \xrightarrow{\mathrm{div}} J_K \to \mathrm{Cl}_K \to 1, \tag{2}$$

where the map div is defined by $\mathrm{div}(x) := (x)$ for any $x \in K^\times$.

Remark 1.11. If you have heard about divisors, then you can keep in mind that the group of fractional ideals of A is nothing but the group $\mathrm{Div}(\operatorname{Spec} A)$ of divisors on the curve $\operatorname{Spec} A$, and the class group of A is precisely the Picard group of $\operatorname{Spec} A$. The sequence (2) is then a special case of the defining sequence for Cartier divisors

$$0 \to \Gamma(X, \mathcal{O}_X^\times) \to \Gamma(X, \mathscr{K}_X^\times) \to \Gamma(X, \mathscr{K}_X^\times/\mathcal{O}_X^\times) \to \mathrm{Pic}(X) \to 0.$$

Example 1.12. The class groups of $\mathbf{Z}$, $\mathbf{Z}[\sqrt{-1}]$, $\mathbf{Z}[\sqrt{3}]$ and $\mathbf{Z}[\frac{1}{2}(1+\sqrt{5})]$ are trivial, while the class group of $\mathbf{Z}[\sqrt{-5}]$ is cyclic of order 2. As hinted to above, the class group of $\mathbf{Z}[\zeta_p]$ is trivial for $p < 23$, but for $p = 23$ we have $h_{\mathbf{Q}(\zeta_{23})} = 3$. As p increases, the class number of $\mathbf{Q}(\zeta_p)$ tends to ∞ [Was82, Theorem 4.20]. Thus there are only finitely many cyclotomic fields $\mathbf{Q}(\zeta_p)$ such that $\mathbf{Z}[\zeta_p]$ has unique factorization.

A fundamental result in algebraic number theory states that the class group of a number field K is finite. This result follows from the so-called *Minkowski bound-theorem*, which gives an upper bound on the norm of ideals [Neu99, I §6].

[2] Norsk: *bruddent ideal*.

[3] Often in algebraic number theory we refer only to the algebraic number field K when we actually speak of the ring of integers $\mathcal{O}_K$. Thus we may say things like "K has unique factorization", or "the class group of K" when we really care about $\mathcal{O}_K$.

1.2 Splitting of primes

Let K be an algebraic number field. We have seen that a fundamental question is whether unique factorization holds in $\mathcal{O}_K$. The introduction of the class group reduces this question to a study of the prime ideals[4] in $\mathcal{O}_K$, and by the "lying over-theorem" any prime ideal of $\mathcal{O}_K$ lies over some prime ideal of $\mathbf{Z}$. So we are interested in the behavior of the primes (p) of $\mathbf{Z}$ when extended to $\mathcal{O}_K$. In general, we distinguish between three scenarios. Indeed, by the fundamental theorem for Dedekind rings we know that the extended ideal $p\mathcal{O}_K$ is a product of powers of prime ideals, say

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}. \tag{3}$$

If any of the exponents e_i are > 1, we say that p *ramifies* in the extension $K/\mathbf{Q}$. If $r > 1$ and $e_i = 1$ for all i, then p is said to *split*; if $r = 1$ and $e_1 = 1$ (that is, if (p) remains a prime ideal when extended to $\mathcal{O}_K$), we say that p is *inert*. Understanding the behavior of primes when extended to other rings of integers lies at the heart of algebraic number theory. In fact, knowing the set of primes that split in a Galois extension of number fields is enough to determine the extension [Mil13, p. 2].

Let us take a look at the connection between this point of view and the problem of solving Diophantine equations. Assume for simplicity that we are given a Diophantine problem $f = 0$ defined by a monic irreducible polynomial in a single variable, so $f \in \mathbf{Z}[X]$ (this case is certainly complicated enough!). Then f defines an algebraic number field $K := \mathbf{Q}[X]/(f)$. Let us also suppose that the ring of integers $\mathcal{O}_K$ is given by $\mathcal{O}_K = \mathbf{Z}[X]/(f)$ (in general this is usually a little more complicated—for example, if $f = X^2 - 5$, then $\mathcal{O}_{\mathbf{Q}(\sqrt{5})} \neq \mathbf{Z}[\sqrt{5}]$). To understand $p\mathcal{O}_K$, we could start out by trying to understand the quotient $\mathcal{O}_K/p\mathcal{O}_K$. We compute

$$\mathcal{O}_K/p\mathcal{O}_K \cong \mathbf{Z}[X]/(p, f) \cong \mathbf{F}_p[X]/(\overline{f}),$$

where $\overline{f}$ is the reduction of f modulo p. Thus, understanding the extended ideal $p\mathcal{O}_K$ is essentially equivalent to solving the equation $f = 0$ modulo p. When f is a quadratic polynomial, the essential ingredient to this problem is the famous *law of quadratic reciprocity* of Gauss:

Theorem 1.13 (Quadratic reciprocity)**.** *Let p and q be distinct odd primes. Then*[5]

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right).$$

Moreover, the following supplementary laws hold, for p an odd prime:

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \qquad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Example 1.14. Let f be the polynomial $f := X^2 + 1$. Thus $K = \mathbf{Q}(i)$, where $i = \sqrt{-1}$, and $\mathcal{O}_K$ is the *ring of Gaussian integers* $\mathbf{Z}[i]$. Let us determine which primes that split in the extension $\mathbf{Q}(i)/\mathbf{Q}$.

1. If $p = 2$, we have $\mathbf{F}_2[X]/(X^2 + 1) = \mathbf{F}_2[X]/(X + 1)^2$. Thus $2\mathbf{Z}[i] = (1 + i)^2$, so the prime 2 ramifies.

[4] In fact, by reducing the study of Diophantine equations to a study of ideals one allows for commutative algebra to enter the picture, and this is one of the reasons for why the word "algebraic" appears in "algebraic number theory".

[5] Recall that the *Legendre symbol* $\left(\frac{p}{q}\right)$ is defined as 1 if p is a square modulo q, and -1 otherwise.

2. Now suppose that p is an odd prime. Consider first the case when $p \equiv 1 \pmod 4$. By the first supplementary law of quadratic reciprocity we then obtain

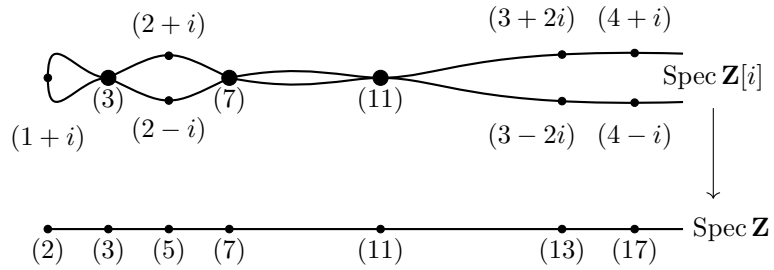
$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1.$$

Hence f splits modulo p, and $\mathbf{F}_p[X]/(X^2+1) \cong \mathbf{F}_p \oplus \mathbf{F}_p$. Equivalently, the ideal $p\mathbf{Z}[i]$ splits as a product of two prime ideals in $\mathbf{Z}[i]$.

3. If $p \equiv 3 \pmod 4$ then $\left(\frac{-1}{p}\right) = -1$. Hence f is irreducible modulo p, and $\mathbf{F}_p[X]/(X^2+1)$ is isomorphic to the finite field $\mathbf{F}_{p^2}$ with p^2 elements. Equivalently, p is inert in the extension $\mathbf{Q}(i)/\mathbf{Q}$.

Point 2 above illustrates a classical theorem of Fermat, namely that a rational prime p is the sum of two squares if and only if $p \equiv 1 \pmod 4$. Indeed, let $N\colon \mathbf{Z}[i] \to \mathbf{Z}$ denote the norm map, defined by $N(a+ib) := a^2+b^2$. Then p is a sum of two squares if and only if p lies in the image of the norm map. Now, if $p \in \operatorname{im} N$ then clearly p splits in $\mathbf{Z}[i]$. On the other hand, if p splits, i.e., $p = \alpha\beta$ in $\mathbf{Z}[i]$, then $N(p) = p^2 = N(\alpha)N(\beta)$ since the norm map is multiplicative. Since we assume neither α nor β is a unit, we must have $p = N(\alpha) = N(\beta)$. Hence p is a sum of two squares $\iff p \in \operatorname{im} N \iff p$ splits in the extension $\mathbf{Q}(i)/\mathbf{Q}$. But by the above discussion, p splits if and only if $p \equiv 1 \pmod 4$.

Remark 1.15. Using Example 1.14 we can draw a picture of (the closed points of) $\operatorname{Spec}\mathbf{Z}[i]$:



We can think of the morphism $\operatorname{Spec}\mathbf{Z}[i] \to \operatorname{Spec}\mathbf{Z}$ as an analogue of a two-sheeted covering of a Riemann surface, ramified only at the point (2). Of course, there are not always two points in each fiber, but this is in some sense accounted for by the fact that if p is inert, then $\mathbf{F}_p[X]/(\overline{f})$ is a degree 2 extension of $\mathbf{F}_p$. This is in fact a general phenomenon: if we in the equation (3) above let f_i denote the degree of the extension of residue fields

$$f_i := [k(\mathfrak{p}_i) : \mathbf{F}_p],$$

then we have the formula

$$\sum_i e_i f_i = [K : \mathbf{Q}]$$

(see [Neu99, I Proposition 8.2]). The numbers f_i are usually referred to as the *local degrees*, while the e_i's are known as the *ramification indices*. The above sum formula can be thought of as an arithmetic version of Bézout's theorem, where we in addition to the intersection multiplicities also need to take into account the local degrees.

As we have seen above, we can at least achieve a good understanding of number fields K defined by a quadratic polynomial in a single variable. We have also hinted that key tool to classifying such quadratic extensions of $\mathbf{Q}$, along with the primes that split in the given extension, is Gauss' law of quadratic reciprocity. The natural follow-up question is then, what about higher degree polynomials? A satisfying classification should involve a suitable reciprocity law—i.e., a way to solve higher degree polynomials modulo various primes. This question dates back to Gauss, who gave some generalizations of his quadratic reciprocity to, e.g., cubic and quartic reciprocity laws. It was later reannounced by Hilbert as one of his 23 problems:

Problem 1.16 (Hilbert's Problem 9)**.** *Find the most general law of the reciprocity theorem in any algebraic number field.*

To this date, Problem 9 remains unresolved. However, in the special case that the Galois group of the polynomial f defining the number field K is abelian, a solution is given by *class field theory* and *Artin's reciprocity law*. Class field theory is one of the major achievements in mathematics in the 20^{th} century, and successfully describes any abelian extension of a number field K in terms of arithmetic invariants intrinsic to K.

2 Syllabus and reading material

To begin with we will cover roughly the first two chapters of:

- Jürgen Neukirch, *Algebraic number theory* [Neu99].

For alternative sources and additional reading material, you can also check out:

- James Milne, *Algebraic number theory*, [Mil17],

or

- Gerald Janusz, *Algebraic number fields*, [Jan96],

or

- Geir Ellingsrud's course notes from 2013, `http://www.uio.no/studier/emner/matnat/math/MAT4250/h13/index.html`.

In the second part of the course we aim to prove the *arithmetic Riemann–Roch theorem*. A possible source is

- Chapter III of Jürgen Neukirch, *Algebraic number theory* [Neu99],

as well as notes from the lectures.

References

[AM69] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969, pp. ix+128.

[Jan96] Gerald J. Janusz. *Algebraic number fields*. Second. Vol. 7. Graduate Studies in Mathematics. American Mathematical Society, Providence, RI, 1996, pp. x+276.

[Mil13] James S. Milne. *Class Field Theory (v4.02)*. Available at `www.jmilne.org/math/`. 2013.

[Mil17] James S. Milne. *Algebraic Number Theory (v3.07)*. Available at `www.jmilne.org/math/`. 2017.

[Neu99] Jürgen Neukirch. *Algebraic number theory*. Vol. 322. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. Springer-Verlag, Berlin, 1999, pp. xviii+571.

[Was82] Lawrence C. Washington. *Introduction to cyclotomic fields*. Vol. 83. Graduate Texts in Mathematics. Springer-Verlag, New York, 1982, pp. xi+389.