MATH3704: ALGEBRAIC NUMBER THEORY

SARAH ZERBES

Lecture 1

Recommended books. I will be following roughly the book *Algebraic Number Theory and Fermat's Last Theorem* by Ian Stewart and David Tall (3rd edition, Taylor & Francis, 2001). It is an excellent book, with many additional exercises. Other books that cover roughly the same material are *Algebraic Number Theory* by Fröhlich and Taylor (Cambridge University Press, 1991) and *Introductory Algebraic Number Theory* by Alaca and Williams (Cambridge University Press, 2003).

Course website: https://metaphor.ethz.ch/x/2022/hs/401-3111-72L/

Contents

1. Introduction

1.1. **Euclidean and Unique factorisation domains.** By a ring, we will always mean a commutative ring R with an identity element 1 distinct from 0.

Example 1.1. The Gaussian integers

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$$

form a ring with the natural addition and multiplication.

Definition 1.2. *An element $a \in R$ is a* unit *if there exists $b \in R$ such that $ab = 1$. We denote this element by a^{-1}. Note that a^{-1} is unique. We denote by $R^\times$ the set of units in R; note that $R^\times$ is a group under multiplication.*

Example 1.3. (Exercise) We have $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.

Definition 1.4. *A ring R is an* integral domain *if it has no zero-divisors; i.e. if $a, b \in R$ satisfy $ab = 0$, then $a = 0$ or $b = 0$.*

Example 1.5. The ring $\mathbb{Z}[i]$ is an integral domain, as it is a subring of $\mathbb{C}$ (which is a field, and hence automatically an integral domain). One can also show explicitly that the product of two non-zero Gaussian integers cannot be zero.

Definition 1.6.
(1) An element $r \in R - \{0\}$ is irreducible if it is not a unit, but if we write $r = ab$ for some $a, b \in R$, then one of a, b must be a unit. Otherwise r is reducible, and a, b are factors of r.
(2) Two elements $r, s \in R$ are associate if there exists $u \in R^\times$ such that $r = su$. In this case we write $r \sim s$.

Example 1.7. Define the norm map

$$N : \mathbb{Z}[i] \to \mathbb{Z}, \quad a + ib = a^2 + b^2.$$

I claim that $2+i$ is irreducible in $\mathbb{Z}[i]$. Indeed, we have $N(2+i)=5$. Suppose now that $2+i=xy$ for some $x,y\in\mathbb{Z}[i]$. Then by the multiplicativity of the norm, we must have

$$N(x)N(y)=5,$$

so either $N(x)=1$ or $N(y)=1$. But the only elements with norm 1 are the units, so we get a contradiction.

Remark 1.8. *We can easily show that any $x\in\mathbb{Z}[i]$ such that $N(x)$ is a prime is irreducible. However, the converse is false!*

Definition 1.9. *A ring R is a unique factorisation domain (UFD) if it is an integral domain, and if*

(1) every non-zero element $x\in R-R^\times$ factors as a product

$$x=r_1\dots r_n,$$

where the r_i are irreducible;

(2) this factorisation is unique up to units and up to reordering of the factors.

Example 1.10. $\mathbb{Z}$ is a unique factorisation domain.

Theorem 1.11. *The ring $\mathbb{Z}[i]$ is a UFD.*

To prove this result, we need to introduce the notion of a Euclidean domain:

Definition 1.12. *Let R be an integral domain, and let $\phi:R\to\mathbb{Z}$ be a function such that $\phi(x)\geq 0$ for all $x\in R$, and $\phi(0)=0$. Then R is a Eucliden domain if the division algorithm holds: for all $x,y\in R$, $y\neq 0$, there exist $q,r\in R$ such that $x=qy+r$ and either $r=0$ or $\phi(r)<\phi(y)$.*

Remark 1.13. *The elements q and r are not required to be unique.*

Proposition 1.14. *Any Euclidean domain is a UFD.*

Proof. See Algebra 1. □

We can now prove Theorem 1.11:

Proof. We take ϕ to be the norm map N. We need to show that it satisfies the axioms of Definition 1.12.

Let $x,y\in\mathbb{Z}[i]$ with $y\neq 0$. Let $z=\frac{x}{y}$, and let q be an element of $\mathbb{Z}[i]$ such that

$$|z-q|\leq|z-q'|$$

for all $q'\in\mathbb{Z}[i]$ (i.e. q is the lattice point closest to z.) By elementary geometry, we have $|z-q|\leq\frac{1}{\sqrt{2}}$.

Let $r=x-qy$. Then

$$N(r)=N(x-qy)=|x-qy|^2=\left|y\left(\frac{x}{y}-q\right)\right|^2=|y|^2|z-q|^2\leq\frac{1}{2}N(y)<N(y).$$

□

1.2. **Solving Diophantine equations.** We will now see that we can use the property of unique factorisation to solve some Diophantine equations.

Problem 1.15. Determine all $x,y\in\mathbb{Z}$ which satisfy

$$x^3=y^2+1. \tag{1}$$

Remark 1.16. *The equation (1) is an example of an elliptic curve. Elliptic curves play an important role in modern number theory; for example, they are central to Wiles' proof of Fermat's Last Theorem.*

Proposition 1.17. *The only solution is $(x,y)=(1,0)$.*

Proof. Suppose that (x,y) is a solution. If x is even, then

$$x^3\equiv 0 \pmod 8 \quad\Rightarrow\quad y^2\equiv -1 \pmod 8.$$

But this gives a contradiction since -1 is not a quadratic residue $\pmod 8$.

Hence x is odd and y is even. Now factor (1) in $\mathbb{Z}[i]$:

$$(y+i)(y-i)=x^3.$$

Claim. $y+i$ and $y-i$ do not have a common factor: they are relatively prime. Proof of claim: suppose there exists $\alpha\in\mathbb{Z}[i]$ which is not a unit such that $\alpha|(y+i)$ and $\alpha|(y-i)$. Then

$$\alpha|\,[(y+i)-(y-i)]=2i,$$

so since $2i = (1+i)^2$ and $1+i$ is irreducible, we deduce from unique factorisation that $(1+i)|\alpha$. Then

$$(1+i)|(y+i)(y-i) = x^3,$$

so by unique factorisation we deduce that $1+i$ devides x, i.e. there exists $\beta \in \mathbb{Z}[i]$ such that $x = (1+i)\beta$. But then

$$x^2 = x\bar{x} = (1+i)(1-i)\beta\bar{\beta} = 2\beta\bar{\beta},$$

so x^2 (and hence x) is even, which gives a contradiction. This proves the claim.

We now deduce from unique factorisation that each of $y+i$ and $y-i$ are of the form $u\beta^3$ for some $u \in \mathbb{Z}[i]^\times$ and $\beta \in \mathbb{Z}[i]$. Now the units in $\mathbb{Z}[i]$ are all perfect cubes, so $y+i$ and $y-i$ are both cubes in $\mathbb{Z}[i]$.

Write $y+i = (a+ib)^3$ for some $a, b \in \mathbb{Z}$. Then

$$y+i = (a^3 - 3ab^2) + (3a^2b - b^3)i \quad \Rightarrow \quad y = a(a^2 - 3b^2) \quad \text{and} \quad 1 = b(3a^2 - b^2).$$

We deduce that $b = \pm 1$.

Lecture 2

(1) If $b = 1$, then $3a^2 = 2$, which is clearly impossible.
(2) If $b = -1$, then $a = 0 \Rightarrow y = 0 \Rightarrow x = 1$.

□

Remark 1.18. *The proof relies crucially on the fact that unique factorisation holds in $\mathbb{Z}[i]$. It is tempting to use similar ideas in order to tackle more complicated equations.*

Remark 1.19. *Finding the integral solutions of the equation*

$$x^3 = y^2 - 1$$

is much harder. Euler showed that the only non-trivial solutions (i.e. with $xy \neq 0$) are $(x, y) = (2, \pm 3)$.

Example 1.20. Let $p \geq 5$ be a prime, and consider Fermat's equation

$$Z^p = X^p + Y^p. \tag{2}$$

Suppose that there exists an integer solution with $p \nmid xyz$. Let ζ be a primitive pth root of unity, and consider the ring $\mathbb{Z}[\zeta]$. Then (2) factorizes over $\mathbb{Z}[\zeta]$ as

$$z^p = (x+y)(x+\zeta y)(x+\zeta^2 y)\dots(x+\zeta^{p-1}y). \tag{3}$$

Assume now that $\mathbb{Z}[\zeta]$ is a UFD. It is then not difficult to prove (exercise) that the terms on the right of (3) are pairwise relatively prime, so each of these terms can be written as ur^p for some unit u and some $r \in \mathbb{Z}[\zeta]$. One can then derive a contradiction, similar to the argument above. The idea was pursued by Lamé and Kummer in trying to prove Fermat's last theorem. But Kummer realised that the ring $\mathbb{Z}[\zeta]$ is almost never a unique factorisation domain! (In fact, it is only a UFD if and only if $p \leq 19$.)

Nonetheless, Kummer was able to make a lot of progress towards resolving Fermat's Last Theorem by suitably modifying this argument. First of all, he realized that even though unique factorization of elements into irreducibles often fails in $\mathbb{Z}[\zeta]$, a weaker property always holds: every ideal factors uniquely into a product of prime ideals. This discovery was really the birth of modern algebraic number theory. Kummer then initiated a careful study of the discrepancy between ideals of $\mathbb{Z}[\zeta]$ and elements of $\mathbb{Z}[\zeta]$. This involves studying the so-called ideal class group, as well as the unit group, of the number ring $\mathbb{Z}[\zeta]$. In this way, Kummer was able to sufficiently understand the units, and to recover enough of a fragment of the unique factorization property in $\mathbb{Z}[\zeta]$, to show that Fermat's Last Theorem holds for what are now called "regular primes". We will discuss all of this in more detail later in the course. In fact, it can be fairly said that understanding the ideal class group and unit group of a number ring is our primary objective in this class.

Remark 1.21. *Already the ring $\mathbb{Z}[\sqrt{6}]$ does not have unique factorisation. Can you give an example?*

1.3. **Field extensions.** We recall some results about field extensions:

Definition 1.22. *Let $K \subset L$ be fields. The dimension of L as a K-vector space is the* degree *of the extension L/K, denoted $[L:K]$. We say that the extension L of K is* finite *if $[L:K] < \infty$.*

Proposition 1.23. *(Tower law) If $F \subset K \subset L$ are finite field extensions, then*

$$[L:F] = [L:K][K:F].$$

Definition 1.24. *Let L/K be a field extension, and let $\alpha \in L$. Then α is* algebraic *over K if there exists a polynomial $f(t) \in K[t]$ such that $f(\alpha) = 0$. If no such f exists, we say that α is* transcendental *over K.*

Definition 1.25. *If α is algebraic over K, there exists a unique monic polynomial $f(t) \in K[t]$ of smallest degree such that $f(\alpha) = 0$. This polynomial is the* minimal polynomial of α over K.

Definition 1.26. *If L/K is a field extension and $\alpha_1, \ldots, \alpha_n \in L$, we define $K(\alpha_1, \ldots, \alpha_n)$ to be the smallest subfield of L containing $\alpha_1, \ldots, \alpha_n$. We call this field the* field obtained by adjoining to K the elements $\alpha_1, \ldots, \alpha_n$.

The following theorem will be of fundamental importance in this course:

Theorem 1.27. *If L/K is a field extension and $\alpha \in L$, then α is algebraic over K if and only if $K(\alpha)$ is a finite field extension of K. In this case, we have $[K(\alpha) : K] = \partial(f)$, where $f \in K[t]$ is the minimal polynomial of α, and a basis of $K(\alpha)$ as a K-vector space is given by $\{1, \alpha, \ldots, \alpha^{\partial(f)-1}\}$.*

2. Algebraic number fields

2.1. **Algebraic numbers.** We now have all the necessary ingredients for studying field extensions. We will be particularly interested in the *algebraic extensions* of $\mathbb{Q}$:

Definition 2.1. *We say that a complex number α is* algebraic *if it is algebraic over $\mathbb{Q}$, i.e. if there exists a non-zero polynomial $f(t) \in \mathbb{Q}[t]$ such that $f(\alpha) = 0$. Let $\mathbb{A}$ denote the set of algebraic numbers.*

Definition 2.2. *An extension K of $\mathbb{Q}$ is* algebraic *if every element of K is algebraic, i.e. if $K \subset \mathbb{A}$.*

Theorem 2.3. *The set $\mathbb{A}$ is a subfield of the complex numbers.*

Proof. We use Theorem 1.27, which says that α is algebraic if and only if $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is finite. Suppose that α and β are algebraic. Then

$$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}].$$

Since β is algebraic over $\mathbb{Q}$, it is certainly algebraic over $\mathbb{Q}(\alpha)$, so $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)]$ is finite by Theorem 1.27. But each of $-\alpha$, $\alpha + \beta$, $\alpha\beta$, and (if $\beta \neq 0$) α/β belong to $\mathbb{Q}(\alpha, \beta)$. So all of these are in $\mathbb{A}$, which proves the theorem. □

Definition 2.4. *A* number field *is a subfield K of $\mathbb{C}$ such that $[K : \mathbb{Q}] < \infty$.*

Theorem 2.5 (Primitive element theorem)**.** *Let L be a number field. Then there exists $\theta \in L$ such that $L = \mathbb{Q}(\theta)$; θ is called a* primitive element *for the extension $L/\mathbb{Q}$.*

Intuitive proof. By Galois theory, K has only finitely many subfields. Let θ be any element of K which does not lie in any of the subfields. Then we must have $K = \mathbb{Q}(\theta)$.

2.2. **Field embeddings.** We'll now think a bit about maps between fields, because that will help us to understand the structure of number fields. Lecture 3

Definition 2.6. *Let $K = \mathbb{Q}(\theta)$ be a number field. A* (complex) embedding *of K is a ring homomorphism $K \to \mathbb{C}$.*

Remark 2.7. *Suppose that $K = \mathbb{Q}(\theta)$, and let $n = [K : \mathbb{Q}]$. By Theorem 1.27, $1, \theta, \ldots, \theta^{n-1}$ is a $\mathbb{Q}$-basis of K. If σ is any complex embedding of K, then σ is uniquely determined by $\sigma(\theta)$: if $x = a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1}$, we have*

$$\sigma(x) = a_0 + a_1\sigma(\theta) + \cdots + a_{n-1}\sigma(\theta)^{n-1}.$$

Recall the following theorem from Galois theory:

Theorem 2.8. *Let $K = \mathbb{Q}(\theta)$ be a number field, with $[K : \mathbb{Q}] = n$. Then there are exactly n distinct embeddings $\sigma_i : K \hookrightarrow \mathbb{C}$. The elements $\sigma_i(\theta)$ are the distinct zeroes in $\mathbb{C}$ of the minimal polynomial of θ over $\mathbb{Q}$.*

Definition 2.9. *Let $\theta \in \mathbb{C}$ be algebraic, and let $K = \mathbb{Q}(\theta)$. Let $\sigma_1, \ldots, \sigma_n$ be the embeddings of K into $\mathbb{C}$. Define the* conjugates of x *to be the elements $\{\sigma_i(\theta) : i = 1, \ldots, n\}$.*

Note 2.10. *Let θ be algebraic, and let $\theta_1 = \theta$, $\theta_2, \ldots, \theta_n$ be the conjugates of θ. As $\prod_{i=1}^{n}(t - \theta_i)$ is the minimal polynomial of θ over $\mathbb{Q}$ by Theorem2.8, it follows that both $\theta_1 \cdots \theta_n$ and $\theta_1 + \cdots + \theta_n$ are in $\mathbb{Q}$. We will see in the next section that this observation can be generalized: if $g(X_1, \ldots, X_n) \in \mathbb{Q}[X_1, \ldots, X_n]$ is any* symmetric polynomial*, then $g(\theta_1, \ldots, \theta_n) \in \mathbb{Q}$. (Of course you can also prove this using Galois theory, but the results on symmetric functions are stronger, as they respect integral structures.)*

2.3. **Interlude: symmetric polynomials.**

Definition 2.11. *Let K be a field and let $f \in K[X_1, \ldots, X_n]$. Then f is called a* symmetric polynomial *(in n variables) if for all permutations $\sigma \in S_n$ we have*

$$f(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = f(X_1, \ldots, X_n).$$

Example 2.12. The polynomials $X_1 + X_2$, X_1X_2, $X_1^2 + 3X_1X_2 + X_2^2$ are symmetric in two variables.
The polynomial

$$f(X_1, X_2, X_3) = X_1^3X_2 + X_1^3X_3 + X_2^3X_1 + X_2^3X_3 + X_3^3X_1 + X_3^3X_2 - X_1^2X_2^2X_3^2$$

in $\mathbb{Q}[X_1, X_2, X_3]$ is symmetric in three variables. However, the polynomial

$$g(X_1, X_2, X_3) = X_1^2X_2 + X_2^2X_3 + X_3^2X_1$$

is not symmetric, as it is not invariant under the transposition $(2, 3)$.

Note 2.13. *The symmetric polynomials in n variables form a subring $\mathfrak{S}_n$ of $K[X_1, \ldots, X_n]$.*

Definition 2.14. *The* elementary symmetric polynomials *in n variables are defined as*

$$\begin{aligned}
s_1 &= X_1 + \ldots + X_n, \\
s_2 &= \sum_{1 \le i < j \le n} X_iX_j, \\
s_3 &= \sum_{1 \le i < j < k \le n} X_iX_jX_k, \\
&\cdots \\
s_n &= X_1X_2 \cdots X_n.
\end{aligned}$$

Example 2.15. The elementary symmetric polynomials in 3 variables are

$$\begin{aligned}
s_1 &= X_1 + X_2 + X_3, \\
s_2 &= X_1X_2 + X_2X_3 + X_3X_1, \\
s_3 &= X_1X_2X_3.
\end{aligned}$$

The following remark will be important later.

Remark 2.16. *The elementary symmetric polynomials arise as follows: if $f(X) \in \mathbb{C}[X]$ is of the form*

$$f(X) = \prod_{i=1}^{n} (X - \alpha_i),$$

then by expanding this we obtain

$$f(X) = X^n - s_1(\alpha_1, \ldots, \alpha_n)X^{n-1} + \ldots + (-1)^n s_n(\alpha_1, \ldots, \alpha_n).$$

The following theorem shows that the elementary symmetric functions are the building blocks for all symmetric functions:

Theorem 2.17. *(Newton's theorem) Let K be a field. Then the subring $\mathfrak{S}_n$ of $K[X_1, \ldots, X_n]$ is generated as a ring over K by the elementary symmetric polynomials in n variables, i.e. every element $h \in \mathfrak{S}_n$ can be written as a K-linear combination of elements of the form $s_1^{a_1} \cdots s_n^{a_n}$, where $a_i \in \mathbb{Z}_{\ge 0}$ for all i.*

Proof. The idea is to order the monomials lexicographically:

$$X_1^{a_1} \cdots X_n^{a_n} > X_1^{b_1} \cdots X_n^{b_n}$$

if and only if $a_1 > b_1$ or $a_1 = b_1$ and $a_2 > b_2$ or $a_1 = b_1$, $a_2 = b_2$ and $a_3 > b_3$ etc. We can therefore define the leading term of a polynomial in n variables. In particular, if f is symmetric, then its leading term is of the form $\alpha X_1^{a_1}X_2^{a_2} \cdots X_n^{a_n}$ for some $a_1 \ge a_2 \ge \cdots \ge a_n$ and $\alpha \in K$. Then the symmetric polynomial

$$\alpha s_1^{a_1 - a_2} s_2^{a_2 - a_3} \cdots s_n^{a_n}$$

has the same leading term as f, so $f - \alpha s_1^{a_1 - a_2} s_2^{a_2 - a_3} \cdots s_n^{a_n}$ has a smaller leading term. We can now proceed by induction. □

Example 2.18. Consider $f(X_1, X_2, X_3) = X_1^2X_2^2 + X_2^2X_3^2 + X_3^2X_1^2$. The leading term of f is $X_1^2X_2^2$, so $a_1 = a_2 = 2$ and $a_3 = 0$. Hence we subtract $s_1^0 s_2^2 s_3^0 = s_2^2$:

$$\begin{aligned} f(X_1, X_2, X_3) - s_2^2 &= X_1^2X_2^2 + X_2^2X_3^2 + X_3^2X_1^2 - (X_1X_2 + X_2X_3 + X_3X_1)^2 \\ &= -2(X_1^2X_2X_3 + X_1X_2^2X_3 + X_1X_2X_3^2). \end{aligned}$$

The leading term is $-2X_1^2X_2X_3$, so $a_1 = 2$, $a_2 = a_3 = 1$ and we subtract $-2s_1s_3$:

$$f(X_1, X_2, X_3) - s_2^2 + 2s_1s_3 = 0,$$

so $f = s_2^2 + 2s_1s_3$.

Example 2.19. Let $f(X_1, X_2, X_3) = X_1^3 + X_2^3 + X_3^3$. The leading term of f in the lexicographic ordering is X_1^3, so we subtract s_1^3: Lecture 4

$$f(X_1, X_2, X_3) - s_1^3 = -3(X_1^2X_2 + X_2^2X_3 + X_3^2X_1 + X_1X_2^2 + X_2X_3^2 + X_3X_1^2) - 6X_1X_2X_3.$$

The leading term of this expression is $-3X_1^2X_2$, so we subtract $-3s_1s_2$:

$$f(X_1, X_2, X_3) - s_1^3 - (-3s_1s_2) = 3X_1X_2X_3 = 3s_3.$$

We deduce that

$$X_1^3 + X_2^3 + X_3^3 = s_1^3 - 3s_1s_2 + 3s_3. \tag{4}$$

We can apply this identity to study properties of the zeroes of polynomials of degree 3. Suppose for example that α, β, γ are the zeros of the polynomial $t^3 + 3t^2 + 6t + 15$, i.e.

$$t^3 + 3t^2 + 6t + 15 = (t - \alpha)(t - \beta)(t - \gamma).$$

We then see from Remark 2.16 that

$$\begin{aligned} -s_1(\alpha, \beta, \gamma) &= 3 \\ s_2(\alpha, \beta, \gamma) &= 6, \\ -s_3(\alpha, \beta, \gamma) &= 15. \end{aligned}$$

Then it follows from (4) that

$$\alpha^3 + \beta^3 + \gamma^3 = (-3)^3 - 3(-3 \times 6) + 3 \times (-15) = -27 + 54 - 45 = -18.$$