

# 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

Recommended books	1
1. Introduction	1
1.1. Euclidean and Unique factorisation domains	1
1.2. Solving Diophantine equations	2
1.3. Field extensions	4
2. Algebraic number fields	4
2.1. Algebraic numbers	4
2.2. Field embeddings	4
2.3. Interlude: symmetric polynomials	5
2.4. Norms, traces and discriminants	7

## 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

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

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  $\phi : R \rightarrow \mathbb{Z}$  be a function such that  $\phi(x) \geq 0$  for all  $x \in R$ , and  $\phi(0) = 0$ . Then  $R$  is a Euclidean 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  $\phi$  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

$$(1) \quad x^3 = y^2 + 1.$$

**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  $1 + i$  divides  $x$ , 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  $b = \pm 1$ .

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

□

Lecture 2

**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

$$(2) \quad Z^p = X^p + Y^p.$$

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

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

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  $\alpha$  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  $\alpha$  is transcendental over  $K$ .

**Definition 1.25.** If  $\alpha$  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  $\alpha$  over  $K$ .

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

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  $\alpha$  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  $\alpha$ , and a basis of  $K(\alpha)$  as a  $K$ -vector space is given by  $\{1, \alpha, \dots, \alpha^{\partial(f)-1}\}$ .

## 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  $\alpha$  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  $\alpha$  is algebraic if and only if  $[\mathbb{Q}(\alpha) : \mathbb{Q}]$  is finite. Suppose that  $\alpha$  and  $\beta$  are algebraic. Then

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

Since  $\beta$  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  $\beta \neq 0$ )  $\alpha/\beta$  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  $L = \mathbb{Q}(\theta)$ ;  $\theta$  is called a primitive element for the extension  $L/\mathbb{Q}$ .

*Intuitive proof.* By Galois theory,  $K$  has only finitely many subfields. Let  $\theta$  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.

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

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

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

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  $\theta$  over  $\mathbb{Q}$ .

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

**Note 2.10.** Let  $\theta$  be algebraic, and let  $\theta_1 = \theta, \theta_2, \dots, \theta_n$  be the conjugates of  $\theta$ . As  $\prod_{i=1}^n (t - \theta_i)$  is the minimal polynomial of  $\theta$  over  $\mathbb{Q}$  by Theorem 2.8, 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  $g(X_1, \dots, X_n) \in \mathbb{Q}[X_1, \dots, X_n]$  is any symmetric polynomial, then  $g(\theta_1, \dots, \theta_n) \in \mathbb{Q}$ . (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  $f \in K[X_1, \dots, X_n]$ . Then  $f$  is called a symmetric polynomial (in  $n$  variables) if for all permutations  $\sigma \in S_n$  we have

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

**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  $K[X_1, \dots, X_n]$ .

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

$$\begin{aligned} s_1 &= X_1 + \dots + X_n, \\ s_2 &= \sum_{1 \leq i < j \leq n} X_i X_j, \\ s_3 &= \sum_{1 \leq i < j < k \leq n} X_i X_j X_k, \\ &\dots \\ s_n &= X_1 X_2 \cdots X_n. \end{aligned}$$

**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

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

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  $K[X_1, \dots, X_n]$  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  $a_i \in \mathbb{Z}_{\geq 0}$  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  $a_1 \geq a_2 \geq \cdots \geq a_n$  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.  $\square$

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

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

The leading term is  $-2X_1^2 X_2 X_3$ , so  $a_1 = 2, a_2 = a_3 = 1$  and we subtract  $-2s_1 s_3$ :

$$f(X_1, X_2, X_3) - s_2^2 + 2s_1 s_3 = 0,$$

so  $f = s_2^2 + 2s_1 s_3$ .

**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  $s_1^3$ :

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

The leading term of this expression is  $-3X_1^2 X_2$ , so we subtract  $-3s_1 s_2$ :

$$f(X_1, X_2, X_3) - s_1^3 - (-3s_1 s_2) = 3X_1 X_2 X_3 = 3s_3.$$

We deduce that

$$(4) \quad X_1^3 + X_2^3 + X_3^3 = s_1^3 - 3s_1 s_2 + 3s_3.$$

We can apply this identity to study properties of the zeroes of polynomials of degree 3. Suppose for example that  $\alpha, \beta, \gamma$  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

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

**Remark 2.20.** The same proof shows that the subring of symmetric polynomials of  $\mathbb{Z}[X_1, \dots, X_n]$  is generated over  $\mathbb{Z}$  by the elementary polynomials.

Combining Remark 2.16 and Theorem 2.17, we obtain the following corollary:

**Corollary 2.21.** Let  $L$  be a field extension of  $K$ , and let  $f \in K[t]$  be a monic polynomial of degree  $n$  such that all the roots of  $f$  are contained in  $L$ . Denote the roots by  $\alpha_1, \dots, \alpha_n$ . If  $h(X_1, \dots, X_n) \in K[X_1, \dots, X_n]$  is symmetric, then  $h(\alpha_1, \dots, \alpha_n) \in K$ .

*Proof.* By assumption,  $f(t)$  factorises in  $L[t]$  as

$$f(t) = (t - \alpha_1) \cdots (t - \alpha_n),$$

so since  $f \in K[t]$ , we deduce from (2.16) that  $s_i(\alpha_1, \dots, \alpha_n) \in K$  for all  $i$ . By Theorem 2.17, it follows that  $h(\alpha_1, \dots, \alpha_n) \in K$  for all symmetric polynomials  $h(X_1, \dots, X_n) \in K[X_1, \dots, X_n]$ .  $\square$

**Remark 2.22.** The same proof works if we replace the field  $K$  by the ring  $\mathbb{Z}$ : Let  $L$  be a field extension of  $\mathbb{Q}$ , and let  $f \in \mathbb{Z}[t]$  be a monic polynomial of degree  $n$  such that all the roots of  $f$  are contained in  $L$ . Denote the roots by  $\alpha_1, \dots, \alpha_n$ . If  $h(X_1, \dots, X_n) \in \mathbb{Z}[X_1, \dots, X_n]$  is symmetric, then  $h(\alpha_1, \dots, \alpha_n) \in \mathbb{Z}$ . This result is not immediate from Galois theory.

We can now give a new and explicit proof of Theorem 2.3 which states that  $\mathbb{A}$  is a field:

*Proof.* We have to show that if  $\alpha, \beta \in \mathbb{A}$ , then  $\alpha + \beta, -\alpha, \alpha\beta, \frac{1}{\alpha} \in \mathbb{A}$ . We first show that  $\alpha + \beta \in \mathbb{A}$ . We do this by constructing *explicitly* a monic polynomial  $h(t) \in \mathbb{Q}[t]$  such that  $h(\alpha + \beta) = 0$ . For  $\star \in \{\alpha, \beta\}$ , let  $f_\star(t) \in \mathbb{Q}[t]$  be the minimal polynomial of  $\star$  over  $\mathbb{Q}$ ; let  $m = \partial(f_\alpha)$  and  $n = \partial(f_\beta)$ . Let  $\beta_1 = \beta, \dots, \beta_n$  be the conjugates of  $\beta$ . We will show that the polynomial

$$h(t) = f_\alpha(t - \beta_1) \cdots f_\alpha(t - \beta_n)$$

has coefficients in  $\mathbb{Q}$ . As it clearly satisfies  $h(\alpha + \beta) = 0$ , this will finish the proof.

Consider the product

$$(5) \quad f_\alpha(t - x_1) f_\alpha(t - x_2) \cdots f_\alpha(t - x_n) = t^{mn} + u_{mn-1}(x_1, \dots, x_n) t^{mn-1} + \cdots + u_0(x_1, \dots, x_n).$$

Note that we obtain  $h(t)$  by substituting  $\beta_1, \dots, \beta_n$  for  $x_1, \dots, x_n$  in (5), so we need to show that  $u_i(\beta_1, \dots, \beta_n) \in \mathbb{Q}$  for all  $1 \leq i \leq mn$ . Now as  $f_\alpha \in \mathbb{Q}[t]$ , it is clear that  $u_i(x_1, \dots, x_n) \in \mathbb{Q}[x_1, \dots, x_n]$  for all  $i$ . Moreover, it is clear from the construction that the  $u_i$  are symmetric polynomials. By Corollary 2.21 we therefore deduce that

$$u_i(\beta_1, \dots, \beta_n) \in \mathbb{Q} \quad \forall 1 \leq i \leq mn,$$

as required. Hence  $\alpha + \beta \in \mathbb{A}$ . The proofs that  $-\alpha, \alpha\beta, \frac{1}{\alpha} \in \mathbb{A}$  are similar and left as exercises.  $\square$

**Remark 2.23.** *Using Remark 2.22, we see that the proof shows indeed something stronger: it proves that if both  $f_\alpha$  and  $f_\beta$  have coefficients in  $\mathbb{Z}$ , then there exists a monic polynomial  $h(t) \in \mathbb{Z}[t]$  such that  $h(\alpha + \beta) = 0$  (and similarly for  $\alpha\beta$  and  $-\alpha$ ). This will be very important later!*

**2.4. Norms, traces and discriminants.** Let  $K = \mathbb{Q}(\theta)$  be a number field of degree  $n$ , and let  $\sigma_1, \dots, \sigma_n$  be the complex embeddings of  $K$ . Let  $\alpha \in K$ .

**Definition 2.24.** *Define the norm and trace of  $\alpha$  by*

$$N_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^n \sigma_i(\alpha) \quad \text{and} \quad \text{Tr}_{K/\mathbb{Q}}(\alpha) = \sum_{i=1}^n \sigma_i(\alpha).$$

**Note 2.25.** *It is clear from the definitions that*

- *the norm is multiplicative:  $N(xy) = N(x)N(y)$ , and*
- *the trace is additive:  $\text{Tr}(x + y) = \text{Tr}(x) + \text{Tr}(y)$ .*

We can use the theory of symmetric functions to show the following result:

**Proposition 2.26.** *Both  $N_{K/\mathbb{Q}}(\alpha)$  and  $\text{Tr}_{K/\mathbb{Q}}(\alpha)$  are in  $\mathbb{Q}$ .*

*Proof.* Let  $\theta_i = \sigma_i(\theta)$ , so  $\theta_1, \theta_2, \dots, \theta_n$  are the conjugates of  $\theta$ . As  $K = \mathbb{Q}(\theta)$ , there exists  $g(t) \in \mathbb{Q}[t]$  such that  $\alpha = g(\theta)$ . Then

$$N_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^n \sigma_i(g(\theta)) = \prod_{i=1}^n g(\sigma_i(\theta)) = \prod_{i=1}^n g(\theta_i),$$

which is clearly a symmetric polynomial in the  $\theta_i$  and hence lies in  $\mathbb{Q}$  by Corollary 2.21. The proof that  $\text{Tr}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Q}$  is similar.  $\square$

**Example 2.27.** Consider the quadratic field  $K = \mathbb{Q}(\sqrt{d})$ . If  $\alpha = a + b\sqrt{d} \in K$ , then

$$N_{K/\mathbb{Q}}(\alpha) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2,$$

$$\text{Tr}_{K/\mathbb{Q}}(\alpha) = (a + b\sqrt{d}) + (a - b\sqrt{d}) = 2a.$$

**Example 2.28.** Let  $K = \mathbb{Q}(\zeta)$ , where  $\zeta = e^{\frac{2\pi i}{5}}$ . Then the minimal polynomial of  $\zeta$  over  $\mathbb{Q}$  is  $f(t) = t^4 + t^3 + t^2 + t + 1$  (why?), and the elements  $\{1, \zeta, \zeta^2, \zeta^3\}$  are a  $\mathbb{Q}$ -basis of  $K$ . Let  $\alpha = 1 - \zeta$ . Then  $N(\alpha) = 5$  and  $\text{Tr}(\alpha) = 5$ .

We now introduce one of the most important objects in the course, the *discriminant*. We will see later that the discriminant can tell us whether or not a given set of elements of a number field is a  $\mathbb{Q}$ -basis (c.f. Corollary 2.38).

**Definition 2.29.** Let  $K$  be a number field, and let  $\alpha_1, \dots, \alpha_n$  be elements of  $K$ . Define a matrix  $A = (a_{ij})_{1 \leq i, j \leq n}$  by

$$a_{ij} = \text{Tr}_{K/\mathbb{Q}}(\alpha_i \alpha_j).$$

Define the discriminant of the set  $\alpha_1, \dots, \alpha_n$  to be  $\Delta[\alpha_1, \dots, \alpha_n] = \det(A)$ .

**Example 2.30.** Let  $K = \mathbb{Q}(\sqrt{d})$ , and define

$$\tau_d = \begin{cases} \sqrt{d} & \text{if } d \not\equiv 1 \pmod{4} \\ \frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \pmod{4} \end{cases}$$

Note that  $\{1, \tau_d\}$  is a  $\mathbb{Q}$ -basis of  $K$ . (In fact, it is a very special basis, as we will see in the next section.) Let us calculate the discriminant of this basis.

(1) Suppose that  $d \not\equiv 1 \pmod{4}$ . Then we have  $\text{Tr}_{K/\mathbb{Q}}(\sqrt{d}) = \sqrt{d} - \sqrt{d} = 0$ , so

$$A = \begin{pmatrix} \text{Tr}_{K/\mathbb{Q}}(1) & \text{Tr}_{K/\mathbb{Q}}(\sqrt{d}) \\ \text{Tr}_{K/\mathbb{Q}}(\sqrt{d}) & \text{Tr}_{K/\mathbb{Q}}(d) \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix},$$

so  $\Delta[1, \sqrt{d}] = 4d$ .

(2) If  $d \equiv 1 \pmod{4}$ , then  $\tau_d = \frac{1+\sqrt{d}}{2}$ . We have  $\text{Tr}(\tau_d) = 1$  and

$$\text{Tr}_{K/\mathbb{Q}}(\tau_d^2) = \text{Tr}_{K/\mathbb{Q}}\left(\frac{1+d+\sqrt{d}}{2}\right) = \frac{1+d}{2},$$

so

$$A = \begin{pmatrix} 2 & 1 \\ 1 & \frac{1+d}{2} \end{pmatrix},$$

and  $\Delta[1, \tau_d] = \det(A) = d$ .

One can give an alternative characterisation of the discriminant as follows:

**Proposition 2.31.** Let  $K$  be a number field, and let  $\sigma_1, \dots, \sigma_n$  be the embeddings of  $K$  into  $\mathbb{C}$ , and define the matrix  $C = (c_{ij})_{1 \leq i, j \leq n}$  by  $c_{ij} = \sigma_i(\alpha_j)$ . Then

$$\Delta[\alpha_1, \dots, \alpha_n] = (\det(C))^2.$$

*Proof.* Problem sheet 1. □

**Corollary 2.32.** If  $\alpha_1, \dots, \alpha_n$  is a  $\mathbb{Q}$ -basis of  $K$  and  $\beta_1, \dots, \beta_n \in K$ . Define the matrix  $D = (d_{ij})$  with  $d_{ij} \in \mathbb{Q}$  by

$$\beta_j = \sum_{i=1}^n d_{ij} \alpha_i.$$

Then

$$\Delta[\beta_1, \dots, \beta_n] = \det(D)^2 \Delta[\alpha_1, \dots, \alpha_n].$$

*Proof.* Problem sheet 1. □

**Note 2.33.** If  $\beta_1, \dots, \beta_n$  is also a  $\mathbb{Q}$ -basis of  $K$ , then  $D$  is just the change-of-basis matrix.

**Example 2.34.** Consider  $\mathbb{Q}(\sqrt{-3})$ . We already know from above that  $\Delta[1, \sqrt{-3}] = -12$ . What is

$$\Delta\left[1 - \sqrt{-3}, \frac{1}{2}\sqrt{-3}\right]?$$

We have

$$\begin{pmatrix} 1 - \sqrt{-3} \\ 2\sqrt{-3} \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 0 & \frac{1}{2} \end{pmatrix} \begin{pmatrix} 1 \\ \sqrt{-3} \end{pmatrix},$$

so Corollary 2.32 implies that

$$\Delta\left[1 - \sqrt{-3}, \frac{1}{2}\sqrt{-3}\right] = \left(\frac{1}{2}\right)^2 \times \Delta[1, \sqrt{-3}] = -3.$$

**Proposition 2.35.** Suppose that  $K = \mathbb{Q}(\theta)$  is a number field of degree  $n$ , and let  $\theta = \theta_1, \theta_2, \dots, \theta_n$  be the conjugates of  $\theta$ . Then

$$\Delta[1, \theta, \dots, \theta^{n-1}] = \prod_{i>j} (\theta_i - \theta_j)^2.$$



**Corollary 2.36.** We have  $\Delta[1, \theta, \dots, \theta^{n-1}] \neq 0$ .

*Proof.* Immediate from Proposition 2.35 and the fact that  $\theta_i \neq \theta_j$  if  $i \neq j$  (why?). □

This proposition will follow immediately from Proposition 2.31 and the following result:

**Proposition 2.37.** Let  $X_1, \dots, X_n$  be indeterminates. Then

$$\det \begin{pmatrix} 1 & X_1 & \dots & X_1^{n-1} \\ 1 & X_2 & \dots & X_2^{n-1} \\ \dots & \dots & \dots & \dots \\ 1 & X_n & \dots & X_n^{n-1} \end{pmatrix} = \prod_{i>j} (X_i - X_j).$$

The matrix on the left is called the Vandermonde matrix.

*Proof.* We proceed by induction on  $n$ . The case for  $n = 2$  is clear by explicit computation. Suppose that it is true for  $n - 1$ . Now consider the matrix

$$A = \begin{pmatrix} 1 & X_1 & \dots & X_1^{n-2} & X_1^{n-1} \\ 1 & X_2 & \dots & X_2^{n-2} & X_2^{n-1} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & X_n & \dots & X_n^{n-2} & X_n^{n-1} \end{pmatrix}.$$

Recall that the determinant is invariant under row and column operations. Subtract  $X_1$ -times the  $(n - 1)$ st column from the  $n$ th column to get

$$\begin{pmatrix} 1 & X_1 & \dots & X_1^{n-2} & 0 \\ 1 & X_2 & \dots & X_2^{n-2} & (X_2 - X_1)X_2^{n-2} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & X_n & \dots & X_n^{n-2} & (X_n - X_1)X_n^{n-2} \end{pmatrix}.$$

Now subtract  $X_1$ -times the  $(n - 2)$ nd column from the  $(n - 1)$ st column to get

$$\begin{pmatrix} 1 & X_1 & \dots & 0 & 0 \\ 1 & X_2 & \dots & (X_2 - X_1)X_2^{n-3} & (X_2 - X_1)X_2^{n-2} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & X_n & \dots & (X_n - X_1)X_n^{n-3} & (X_n - X_1)X_n^{n-2} \end{pmatrix}.$$

Keep going, so in the end we get

$$\begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 1 & X_2 - X_1 & \dots & (X_2 - X_1)X_2^{n-3} & (X_2 - X_1)X_2^{n-2} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & X_n - X_1 & \dots & (X_n - X_1)X_n^{n-3} & (X_n - X_1)X_n^{n-2} \end{pmatrix}.$$

It is now easy to calculate the determinant:

$$\begin{aligned} \det(A) &= \det \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 1 & X_2 - X_1 & \dots & (X_2 - X_1)X_2^{n-3} & (X_2 - X_1)X_2^{n-2} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & X_n - X_1 & \dots & (X_n - X_1)X_n^{n-3} & (X_n - X_1)X_n^{n-2} \end{pmatrix} \\ &= \det \begin{pmatrix} X_2 - X_1 & \dots & (X_2 - X_1)X_2^{n-3} & (X_2 - X_1)X_2^{n-2} \\ \dots & \dots & \dots & \dots \\ X_n - X_1 & \dots & (X_n - X_1)X_n^{n-3} & (X_n - X_1)X_n^{n-2} \end{pmatrix} \\ &= (X_2 - X_1) \cdots (X_n - X_1) \det \begin{pmatrix} 1 & \dots & X_2^{n-3} & X_2^{n-2} \\ \dots & \dots & \dots & \dots \\ 1 & \dots & X_n^{n-3} & X_n^{n-2} \end{pmatrix}, \end{aligned}$$

and we conclude by induction hypothesis. □

**Corollary 2.38.** Let  $K$  be a number field of degree  $n$ , and let  $\alpha_1, \dots, \alpha_n \in K$ . Then  $\alpha_1, \dots, \alpha_n$  is a  $\mathbb{Q}$ -basis of  $K$  if and only if  $\Delta[\alpha_1, \dots, \alpha_n] \neq 0$ .

*Proof.* By Theorem 2.5, we can choose  $\theta \in K$  such that  $K = \mathbb{Q}(\theta)$ . Then  $1, \theta, \dots, \theta^{n-1}$  is a  $\mathbb{Q}$ -basis of  $K$  by Theorem 1.27, and

$$\Delta[1, \theta, \dots, \theta^{n-1}] \neq 0$$

by Corollary 2.36. Let  $D = (d_{ij})$  be the matrix defined by

$$\alpha_j = \sum_{i=1}^n d_{ij} \theta^i.$$

Then

$$\Delta[\alpha_1, \dots, \alpha_n] = \det(D)^2 \Delta[1, \theta, \dots, \theta^{n-1}]$$

by Lemma 2.32. As  $\det(D) \neq 0$  if and only if  $\alpha_1, \dots, \alpha_n$  is also a  $\mathbb{Q}$ -basis of  $K$ , this implies the result.  $\square$

In other words, the discriminant can be used to detect whether a given set of elements of a number field is a  $\mathbb{Q}$ -basis. However, it is not easy from the definitions to calculate the discriminant. The following result shows that in special circumstance we can use the norm to calculate the discriminant:

**Proposition 2.39.** *Let  $K = \mathbb{Q}(\theta)$ , where  $\theta$  has minimum polynomial  $f(t)$  over  $\mathbb{Q}$  of degree  $n$ . Then the  $\mathbb{Q}$ -basis  $1, \theta, \dots, \theta^{n-1}$  has discriminant*

$$\Delta[1, \theta, \dots, \theta^{n-1}] = (-1)^{\frac{1}{2}n(n-1)} N_{K/\mathbb{Q}}(Df(\theta)),$$

where  $Df(t) \in \mathbb{Q}[t]$  is the formal derivative of  $f(t)$ .

*Proof.* Let  $\sigma_1 = id, \sigma_2, \dots, \sigma_n$  be the embeddings of  $K$ , and let  $\theta_i = \sigma_i(\theta)$ , so in particular  $\theta_1 = \theta$ . Over  $\mathbb{C}$ , the polynomial  $f(t)$  factorises as

$$f(t) = (t - \theta_1) \cdots (t - \theta_n).$$

If we define

$$g_i(t) = \prod_{j \neq i} (t - \theta_j),$$

then  $f(t) = (t - \theta_i)g_i(t)$  for all  $1 \leq i \leq n$ , and

$$\sigma_i(g_1(t)) = \frac{f(t)}{\sigma_i(t - \theta_1)} = \frac{f(t)}{t - \theta_i} = g_i(t).$$

Then

$$\begin{aligned} Df(t) &= g_1(t) + (t - \theta)Dg_1(t), \\ \Rightarrow Df(\theta) &= g_1(\theta) = \prod_{i=2}^n (\theta - \theta_i). \end{aligned}$$

Taking the norm, we see that

$$\begin{aligned} N_{K/\mathbb{Q}}(Df(\theta)) &= N_{K/\mathbb{Q}}(g_1(\theta)) \\ &= \prod_{j=1}^n \sigma_j(g_1(\theta)) \\ &= \prod_{j=1}^n g_j(\theta_j) \\ &= \prod_{i \neq j} (\theta_j - \theta_i) \\ &= \prod_{i < j} (\theta_j - \theta_i)(\theta_i - \theta_j) \\ &= (-1)^{\frac{n(n-1)}{2}} \prod_{i < j} (\theta_i - \theta_j)^2 \\ &= (-1)^{\frac{n(n-1)}{2}} \Delta[1, \theta, \dots, \theta^{n-1}], \end{aligned}$$

where the last equality follows from Proposition 2.35.  $\square$

To give an example of how to use Proposition 2.39, let us look at cubic fields:

**Definition 2.40.** *A number field  $K$  is cubic if  $[K : \mathbb{Q}] = 3$ .*

**Lemma 2.41.** *Let  $K$  be a cubic field. Then there exists  $\theta \in K$  such that  $K = \mathbb{Q}(\theta)$  and the minimal polynomial of  $\theta$  over  $\mathbb{Q}$  is of the form  $g(t) = t^3 + at + b$  for some  $a, b \in \mathbb{Q}$ .*

*Proof.* Let  $\alpha$  be a primitive element of  $K$ . Then the minimal polynomial of  $\alpha$  over  $\mathbb{Q}$  is of the form

$$f(t) = t^3 + ct^2 + dt + e$$

for some  $c, d, e \in \mathbb{Q}$ . Let  $\theta = \alpha + \frac{c}{3}$ . Then clearly  $K = \mathbb{Q}(\theta)$ , and the minimal polynomial of  $\theta$  over  $\mathbb{Q}$  is  $f(t - \frac{c}{3})$ , which is of the required form.  $\square$

**Corollary 2.42.** *Let  $K$  be a cubic field, and let  $\alpha$  be a primitive element of  $K$  whose minimal polynomial over  $\mathbb{Q}$  is of the form  $f(t) = t^3 + at + b$ . Then*

$$\Delta[1, \alpha, \alpha^2] = -27b^2 - 4a^3.$$