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

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

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 $a_1 \geq a_2 \geq \cdots \geq a_n$ 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. □

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 $s_1^0s_2^2s_3^0 = s_2^2$:

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

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

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

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

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

Remark 2.20. *The same proof shows that the subring of symmetric polynomials of $\mathbb{Z}[X_1, \ldots, X_n]$ 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 $\alpha_1, \ldots, \alpha_n$. If $h(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$ is symmetric, then $h(\alpha_1, \ldots, \alpha_n) \in K$.*

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 $s_i(\alpha_1, \ldots, \alpha_n) \in K$ for all i. By Theorem 2.17, it follows that $h(\alpha_1, \ldots, \alpha_n) \in K$ for all symmetric polynomials $h(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$. □

Lecture 4

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 $\alpha_1, \ldots, \alpha_n$. If $h(X_1, \ldots, X_n) \in \mathbb{Z}[X_1, \ldots, X_n]$ is symmetric, then $h(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$. 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 $\beta_1 = \beta, \ldots, \beta_n$ be the conjugates of β. 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

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

Note that we obtain $h(t)$ by substituting $\beta_1, \ldots, \beta_n$ for $x_1, \ldots, x_n$ in (5), so we need to show that $u_i(\beta_1, \ldots, \beta_n) \in \mathbb{Q}$ for all $1 \le i \le mn$. Now as $f_\alpha \in \mathbb{Q}[t]$, it is clear that $u_i(x_1, \ldots, x_n) \in \mathbb{Q}[x_1, \ldots, x_n]$ 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

$$u_i(\beta_1, \ldots, \beta_n) \in \mathbb{Q} \qquad \forall 1 \le i \le mn,$$

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. □

Remark 2.23. *Using Remark 2.22, we see that the proof shows indeed something stronger: it proves that if both f_α and f_β have coefficients in $\mathbb{Z}$, then there exists a monic polynomial $h(t) \in \mathbb{Z}$ 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 $\sigma_1, \ldots, \sigma_n$ be the complex embeddings of K. Let $\alpha \in K$.

Definition 2.24. *Define the norm and trace of α by*

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

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: $\mathrm{Tr}(x+y) = \mathrm{Tr}(x) + \mathrm{Tr}(y)$.*

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

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

Proof. Let $\theta_i = \sigma_i(\theta)$, so $\theta_1, \theta_2, \ldots, \theta_n$ are the conjugates of θ. 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 θ_i and hence lies in $\mathbb{Q}$ by Corollary 2.21. The proof that $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Q}$ is similar. □

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

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

Example 2.28. Let $K = \mathbb{Q}(\zeta)$, where $\zeta = e^{\frac{2\pi i}{5}}$. Then the minimal polynomial of ζ 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 $\mathrm{Tr}(\alpha) = 5$.

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 $\alpha_1, \ldots, \alpha_n$ be elements of K. Define a matrix $A = (a_{ij})_{1 \leq i,j \leq n}$ by*

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

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

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 $\mathrm{Tr}_{K/\mathbb{Q}}(\sqrt{d}) = \sqrt{d} - \sqrt{d} = 0$, so

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

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

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

$$\mathrm{Tr}_{K/\mathbb{Q}}(\tau_d^2) = \mathrm{Tr}_{K/\mathbb{Q}}\left(\frac{1 + d + \sqrt{d}}{4}\right) = \frac{1+d}{2},$$

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 $\sigma_1, \ldots, \sigma_n$ 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*

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

Proof. Problem sheet 1. □

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

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

Then

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

Proof. Problem sheet 1. □

Note 2.33. *If $\beta_1, \ldots, \beta_n$ 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

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

Lecture 5

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

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

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

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* $X_1, \ldots, X_n$ *be indeterminates. Then*

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

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

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

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

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

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

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

Keep going, so in the end we get

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

It is now easy to calculate the determinant:

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

and we conclude by induction hypothesis. □

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

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

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

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

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

Then

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

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

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 θ has minimum polynomial $f(t)$ over $\mathbb{Q}$ of degree n. Then the $\mathbb{Q}$-basis $1, \theta, \ldots, \theta^{n-1}$ has discriminant*

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

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

Proof. Let $\sigma_1 = id, \sigma_2, \ldots, \sigma_n$ be theembeddings 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

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

Taking the norm, we see that

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

where the last equality follows from Proposition 2.35. □

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 θ over $\mathbb{Q}$ is of the form $g(t) = t^3 + at + b$ for some $a, b \in \mathbb{Q}$.*

Proof. Let α be a primitive element of K. Then the minimal polynomial of α 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 θ over $\mathbb{Q}$ is $f(t - \frac{c}{3})$, which is of the required form. □

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

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

Lecture 6

Proof. Let β, γ be the other two roots of $f(t)$, so over $\mathbb{C}$, $f(t)$ factorises as

$$f(t) = t^3 + at + b = (t - \alpha)(t - \beta)(t - \gamma),$$

which implies that

$$s_1(\alpha, \beta, \gamma) = 0, \quad s_1(\alpha, \beta, \gamma) = a, \quad s_2(\alpha, \beta, \gamma) = -b. \tag{6}$$

Now we know from Proposition 2.39 that

$$\Delta[1, \alpha, \alpha^2] = -N_{K/\mathbb{Q}}(Df(\alpha)).$$

We calculate $N_{K/\mathbb{Q}}(Df(\alpha))$ using the theory of symmetric polynomials: clearly $Df(\alpha) = 3t^2 + a$, so

$$\begin{aligned} N_{K/\mathbb{Q}}(Df(\alpha)) &= \sigma_1(3\alpha^2 + a) \cdot \sigma_2(3\alpha^2 + a) \cdot \sigma_3(3\alpha^2 + a) \\ &= (3\alpha^2 + a)(3\beta^2 + a)(3\gamma^2 + 3) \\ &= 27(\alpha\beta\gamma)^2 + 9a(\alpha^2\beta^2 + \beta^2\gamma^2 + \gamma^2\alpha^2) + 3a^2(\alpha^2 + \beta^2 + \gamma^2) + a^3 \end{aligned}$$

To evaluate the coefficients, we express them in terms of the $s_i(\alpha, \beta, \gamma)$. Applying the algorithm from Newton's theorem shows that

$$\begin{aligned} (\alpha\beta\gamma)^2 &= s_1(\alpha, \beta, \gamma)^2 = b^2, \\ \alpha^2\beta^2 + \beta^2\gamma^2 + \gamma^2\alpha^2 &= s_1(\alpha, \beta, \gamma)^2 - 2s_3(\alpha, \beta, \gamma)s_1(\alpha, \beta, \gamma) = a^2 \\ \alpha^2 + \beta^2 + \gamma^2 &= s_1(\alpha, \beta, \gamma)^2 - 2s_2(\alpha, \beta, \gamma) = -2a, \end{aligned}$$

so

$$N_{K/\mathbb{Q}}(Df(\alpha)) = 27b^2 + 4a^3.$$

□

3. Algebraic integers

3.1. Definition and basic properties.

Definition 3.1. *An* algebraic integer *is a root in $\mathbb{C}$ of a monic polynomial equation with integer coefficients. In other words, β is an algebraic integer if and only if there exist $b_0, \ldots, b_{n-1} \in \mathbb{Z}$ such that*

$$\beta^n + b_{n-1}\beta^{n-1} + \cdots + b_0 = 0.$$

Example 3.2. The algebraic number $\theta = \sqrt{-2}$ is an algebraic integer, since $\theta^2 + 2 = 0$. More surprisingly, $\tau = \frac{1+\sqrt{5}}{2}$ (the "Golden Ratio") is an algebraic integer, since it satisfies $\tau^2 - \tau - 1 = 0$. We will later determine all the algebraic integers in quadratic fields.

Clearly every algebraic integer is an algebraic number. The following proposition shows that there are algebraic integers which are not algebraic numbers.

Lemma 3.3. *If α is an algebraic integer and $\alpha \in \mathbb{Q}$, then $\alpha \in \mathbb{Z}$.*

Proof. Write $\alpha = a/b$ in lowest terms. Suppose α is not an integer, so $b \neq \pm 1$. As α is an algebraic integer, there are $c_0, \ldots, c_{n-1} \in \mathbb{Z}$ with

$$\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_0 = 0.$$

Clearing denominators,

$$a^n + c_{n-1}a^{n-1}b + \cdots + c_0 b^n = 0.$$

As $b \neq \pm 1$, b must have a prime factor, p say. Since a/b is in lowest terms, p doesn't divide a. But then we have

$$a^n = -(c_{n-1}a^{n-1}b + \cdots + c_0 b^n)$$

and the right-hand side is divisible by p but the left-hand side is not, a contradiction. □

The following fundamental result follows from our work on symmetric functions:

Theorem 3.4. *The algebraic integers form a subring $\mathbb{B}$ of $\mathbb{A}$.*

Proof. Let $\alpha, \beta \in \mathbb{B}$. Then Remark 2.23 shows that $\alpha + \beta$, $\alpha\beta$ and $-\alpha$ are in $\mathbb{B}$, so $\mathbb{B}$ is a ring. □

We now give an alternative description of algebraic integers, resembling Theorem 1.27. First recall the following definition:

Definition 3.5. *Let $(G, +)$ be an abelian group. Then we say G is* finitely generated *if there is a finite subset $x_1, \ldots, x_d$ of G such that every element $y \in G$ can be written in the form*

$$y = n_1 x_1 + \cdots + n_d x_d$$

for some $n_i \in \mathbb{Z}$. We call $x_1, \ldots, x_n$ generators of the group G.

Examples 3.6. (1) The additive group $\mathbb{Z}/N\mathbb{Z}$ for any $N \geq 1$ is finitely generated.
(2) The additive group $\left\{ \frac{a}{2^i} : i \geq 0 \right\}$ is not finitely generated.

Lemma 3.7. *A subgroup of a finitely generated abelian group is finitely generated.*

Proof. We won't prove this here, but it's not very hard to do (it suffices to check that any subgroup of $\mathbb{Z}^n$ is finitely generated, and this can be shown pretty easily by induction on n). □

Proposition 3.8. *A complex number α is an algebraic integer if and only if the additive group generated by the powers $1, \alpha, \alpha^2, \ldots$ is finitely generated.*

Remark 3.9. *Explicitly, this means that α is an algebraic integer if and only if there exists $N \geq 1$ such that for all $m > N$, there exist $c_0, \ldots, c_N \in \mathbb{Z}$ such that*

$$\alpha^m = c_0 + c_1\alpha + \cdots + c_N\alpha^N.$$

Proof. If α is an algebraic integer, then there exists a monic polynomial $f \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$. By polynomial division, any polynomial $g \in \mathbb{Z}[x]$ can be written in the form $g = qf + r$, with $\partial(r) < \partial(f)$; and, since f is monic, we have $r \in \mathbb{Z}[x]$. In particular, we can do this for $g(x) = x^n$ for any integer n. Then

$$\alpha^n = g(\alpha) = q(\alpha)f(\alpha) + r(\alpha) = r(\alpha),$$

since by assumption $f(\alpha) = 0$. Since r has degree $\leq n - 1$ and integer coefficients, this shows that $\alpha^n = r(\alpha)$ lies in the subgroup generated by $1, \ldots, \alpha^{n-1}$.

Conversely, suppose that the abelian group generated by the powers of α is finitely generated. Then it has a finite generating set $x_1, \ldots, x_n$. Each of these generators can only mention finitely many powers of α, so there is some finite N such that the subgroup is generated by $1, \alpha, \ldots, \alpha^N$. But then α^{N+1} must be a linear combination, with integer coefficients, of $1, \ldots, \alpha^N$; so α satisfies a monic polynomial with integer coefficients of degree $N + 1$. □

We can now give a new proof of Theorem 3.4:

Proof. Let α, β be algebraic integers. We have to show that $\alpha\beta$ and $\alpha + \beta$ are also algebraic integers. By Proposition 2.11, all powers of α lie in a finitely generated additive subgroup Γ_α of $\mathbb{C}$ (with generators $v_1, \ldots, v_n$) and all powers of β lie in a finitely generated additive subgroup Γ_β of $\mathbb{C}$ (with generators $w_1, \ldots, w_m$).

Let Γ be the finitely generated additive group generated by $\{v_i\}_{1 \leq i \leq n}$, $\{w_j\}_{1 \leq j \leq m}$ and by the products $v_i w_j$ with $1 \leq i \leq n, 1 \leq j \leq m$. Then all powers of $\alpha + \beta$ and $\alpha\beta$ lie in Γ, so it follows from Proposition 3.8 that they are all algebraic integers. □

Lecture 7

We now want to give a criterion for an algebraic number to be an algebraic integer in terms of the minimal polynomial. We first rcall the following result:

Lemma 3.10 (Gauss' lemma)**.** *Let $f(t) \in \mathbb{Z}[t]$ and suppose $f = gh$ for some $g, h \in \mathbb{Q}[t]$. Then there exists $\lambda \in \mathbb{Q}$, $\lambda \neq 0$, such that both $\lambda g(t)$ and $\lambda^{-1}h(t)$ have coefficients in $\mathbb{Z}$. In particular, f is irreducible in $\mathbb{Q}[t]$ if and only if it is irreducible in $\mathbb{Z}[t]$.*

Proposition 3.11. *An algebraic number is an algebraic integer if and only if its minimal polynomial over $\mathbb{Q}$ has integer coefficients.*

Proof. If the minimal polynomial f of α has integral coefficients, then α is certainly an algebraic integer, since f is monic.

Conversely, suppose α is an algebraic integer. Then it satisfies some monic integral polynomial F with integer coefficients. So F is divisible by f, by the definition of the minimal polynomial; hence we can write $F = fg$ for some $f, g \in \mathbb{Q}[t]$. By Gauss's Lemma, we can find $\lambda \in \mathbb{Q}$ such that λf and $\lambda^{-1} g$ have integer coefficients.

Since f is monic, the leading coefficient of λf is just λ. In particular, $\lambda \in \mathbb{Z}$. But the leading coefficient of f must divide the leading coefficient of F, which is 1. So $\lambda = \pm 1$. Since f has integer coefficients if and only if $-f$ does, the result follows. □

Definition 3.12. *Let K be a number field. We define the* ring of integers *of K to be the ring $O_K = \mathbb{B} \cap K$.*

Example 3.13. Suppose that $\alpha = a + bi \in \mathbb{Q}(i)$ with $b \neq 0$. Then the minimal polynomial of α over $\mathbb{Q}$ is

$$f(t) = t^2 - 2at + (a^2 + b^2),$$

so α is an algebraic integer if and only if both $2a$ and $a^2 + b^2$ are in $\mathbb{Z}$. Hence the ring of integers of $\mathbb{Q}(i)$ is $\mathbb{Z}(i) = \{a + bi : a, b \in \mathbb{Z}\}$.

Let K be a number field. Given an element $\alpha \in K$, we can also use the norm and trace operators to test whether $\alpha \in O_K$:

Proposition 3.14. *Let $\alpha \in K$. If α is an algebraic integer, then* $\mathrm{Tr}(\alpha)$ *and* $N(\alpha) \in \mathbb{Z}$.

Proof. Example sheet. □

Example 3.15. Let $K = \mathbb{Q}(\sqrt[3]{2})$, and let $\alpha = \frac{1}{3}\sqrt[3]{2} + \frac{1}{2}\sqrt[3]{2^2}$. Is α an algebraic integer? An easy calcuation shows that $N(\alpha) = \frac{31}{54}$, so α is certainly not an algebraic integer.

Warning. Proposition 3.14 is not an if-and-only-if criterion!

3.2. **Integral bases.** Let K be a number field of degree n. Recall that a $\mathbb{Q}$-basis of K is a basis for K as a $\mathbb{Q}$-vector space. We now want to define a 'basis' for the ring of integers of K. Recall that O_K is an Abelian group.

Definition 3.16. *An* integral basis *of K is a $\mathbb{Q}$-basis of K which is also a $\mathbb{Z}$-basis for O_K. In other words, a $\mathbb{Q}$-basis $x_1, ..., x_n$ of K is an integral basis of K if for every $\alpha \in O_K$ there exist unique $a_1, \ldots, a_n \in \mathbb{Z}$ such that*

$$\alpha = a_1 x_1 + \cdots + a_n x_n.$$

Example 3.17. 1 is an integral basis of $\mathbb{Q}$; $\{1, i\}$ is an integral basis of $\mathbb{Q}(i)$. But $\{1, \sqrt{5}\}$ is *not* an integral basis of $\mathbb{Q}(\sqrt{5})$, since we know that $\frac{1+\sqrt{5}}{2}$ is an algebraic integer.

It is not immediately clear that every number field has an integral basis.

3.2.1. *Existence of integral bases.* The aim of this section is to show that every number field has an integral basis. We start with the following elementary observation:

Lemma 3.18. *Let α be an algebraic number. Then there is a nonzero integer c such that $c\alpha$ is an algebraic integer.*

Proof. Exercise. □

As a corollary, we get the following result:

Corollary 3.19. *Let K be a number field. Then there exists a $\mathbb{Q}$-basis $\{\alpha_1, \ldots, \alpha_n\}$ of K such that $\alpha_i \in O_K$ for all $1 \leq i \leq n$.*

The following observation will be useful:

Lemma 3.20. *If $\{\alpha_1, \ldots, \alpha_n\}$ is a $\mathbb{Q}$-basis of K such that $\alpha_i \in O_K$ for all $1 \leq i \leq n$, then $\Delta[\alpha_1, \ldots, \alpha_n] \in \mathbb{Z}$.*

Proof. Since O_K is a ring, it is clear that $\alpha_i \alpha_j \in O_K$ for all i, j. Then Proposition 3.14 implies that $\mathrm{Tr}(\alpha_i \alpha_j) \in \mathbb{Z}$. As $\Delta[\alpha_1, \ldots, \alpha_n]$ is by definition the determinant of the matrix with entries $\mathrm{Tr}(\alpha_i \alpha_j)$, this finishes the proof. □

We can now prove the main result of this section:

Theorem 3.21. *Every number field K has an integral basis. More precisely, if $\alpha_1, \ldots, \alpha_n \in O_K$ is a $\mathbb{Q}$-basis of K such that $|\Delta[\alpha_1, \ldots, \alpha_n]|$ is minimal, then it is an integral basis.*

Proof. By Corollary 3.19, there exists a $\mathbb{Q}$-basis of K consisting of algebraic integers. Let $w_1, \ldots, w_n$ be such a basis with $\Delta[w_1, \ldots, w_n]$ minimal. We now argue by contradiction: suppose that $w_1, \ldots, w_n$ is not an integral basis. Then there exists an algebraic integer $\beta \in O_K$ such that

$$\beta = a_1 w_1 + \cdots + a_n w_n$$

for some $a_i \in \mathbb{Q}$, not all of which are in $\mathbb{Z}$. Suppose without loss of generality that $a_1 \notin \mathbb{Z}$. Then

$$a_1 = a + r,$$

where $a \in \mathbb{Z}$ and $0 < r < 1$. Define

Lecture 8

$$\psi_1 = \beta - a w_1, \quad \text{and} \quad \psi_i = w_i \quad \text{for } 2 \leq i \leq n.$$

Then $\psi_1, \ldots, \psi_n$ is a $\mathbb{Q}$-basis of K consisting of integers, and the determinant of the change of basis matrix from $\{w_1, \ldots, w_n\}$ to $\{\psi_1, \ldots, \psi_n\}$ is

$$\begin{vmatrix} a_1 - a & a_2 & a_3 & \ldots & a_n \\ 0 & 1 & 0 & \ldots & 0 \\ & & \ldots & & \\ 0 & 0 & 0 & \ldots & 1 \end{vmatrix} = r,$$

and hence Corollary 2.32 implies that

$$\Delta[\psi_1, \ldots, \psi_n] = r^2 \Delta[w_1, \ldots, w_n],$$

and $|\Delta[\psi_1, \ldots, \psi_n]| < |\Delta[w_1, \ldots, w_n]|$ since $0 < r < 1$. This gives a contradiction by the choice of $w_1, \ldots, w_n$. □

Corollary 3.22. *Suppose that $\alpha_1, \ldots, \alpha_n \in O_K$ are a $\mathbb{Q}$-basis of K. If $\Delta[\alpha_1, \ldots, \alpha_n]$ is square-free, then $\{\alpha_1, \ldots, \alpha_n\}$ is an integral basis of K.*

Proof. Let $\beta_1, \ldots, \beta_n$ be an integral basis. Then there exist $c_{ij} \in \mathbb{Z}$ for $1 \leq i, j \leq n$ such that $\alpha_i = \sum_{j=1}^n c_{ij} \beta_j$. Let $C = (c_{ij})_{1 \leq i,j \leq n}$. By Corollary 2.32 this implies that

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

Since the left-hand side is square-free, we must have $\det(C) = \pm 1$, so that the matrix C is uni- modular, i.e. its inverse also has entries in $\mathbb{Z}$. Hence $\alpha_1, \ldots, \alpha_n$ is also a $\mathbb{Z}$-basis of O_K, which finishes the proof. □

However, this corollary is **NOT** an *if and only if* criterion!

Example 3.23. Recall that if $K = \mathbb{Q}(i)$, then we know that $\{1, i\}$ is an integral basis. However, $\Delta[1, i] = -4$, which is certainly not square-free.

Example 3.24. Let $f(t) = t^3 - t - 1$. We first note that f is irreducible in $\mathbb{Z}[t]$ (and hence in $\mathbb{Q}[t]$, by Gauss' lemma), as is reduction (mod 2) has no root and is hence irreducible. Let α be a root of $f(t)$ (it is clearly an algebraic integer), and let $K = \mathbb{Q}(\alpha)$. Then $1, \alpha, \alpha^2$ is a $\mathbb{Q}$-basis of K by Theorem 1.27, and Corollary 2.42 shows that

$$\Delta[1, \alpha, \alpha^2] = -23.$$

As 23 is prime, we deduce from Theorem 3.22 that $\{1, \alpha, \alpha^2\}$ is an integral basis of O_K .

So given a general number field, how do we find an integral basis? The proof of Theorem 3.21 gives an algorithm:

- Start with any $\mathbb{Q}$-basis $\alpha_1, \ldots, \alpha_n$ of K consisting of algebraic integers.
- Calculate $\Delta[\alpha_1, \ldots, \alpha_n]$, and let N be the largest integer whose square divides N.
- If $N = 1$, the basis $\alpha_1, \ldots, \alpha_n$ is integral by Corollary 3.22.
- If $N > 1$, then for each element of the form

  $$\theta = \frac{1}{N} \sum_{i=1}^n a_i \alpha_i, \qquad \text{with } 1 \leq a_i < N$$

  determine whether θ is an algebraic integer. If it is, then replace one of the α_i for which $a_i \neq 0$ by θ to get a new basis with discriminant of smaller absolute value, and start again with step 2.
- If none of the θ are algebraic integers (or $N = 1$), you have found an integral basis.

Example 3.25. Let $K = \mathbb{Q}(\sqrt{5})$. We start with the $\mathbb{Q}$-basis $1, \sqrt{5}$ of K. The two embeddings of K are determined by $\sqrt{5} \mapsto \pm\sqrt{5}$, so we have

$$\Delta[1, \sqrt{5}] = \det \begin{pmatrix} 1 & \sqrt{5} \\ 1 & -\sqrt{5} \end{pmatrix}^2 = 2^2 \cdot 5.$$

Hence $N = 2$, and we need to check whether any of the elements $\frac{1}{2}$, $\frac{1+\sqrt{5}}{2}$, $\frac{\sqrt{5}}{2}$ are algebraic integers. We know from Lemma 3.3 that $\frac{1}{2}$ is not an algebraic integer.

What about $\alpha = \frac{1}{2}(1 + \sqrt{5})$? Its minimal polynomial is $t^2 - t - 1$, so α is an algebraic integer. We calculate the discriminant of the new basis:

$$\Delta[1, \alpha] = \det \begin{pmatrix} 1 & \frac{1+\sqrt{5}}{2} \\ 1 & \frac{1-\sqrt{5}}{2} \end{pmatrix}^2 = 5,$$

which is square-free, so $1, \alpha$ is an integral basis of K.

Theorem 3.26. *Let $d \in \mathbb{Z} \setminus \{0, 1\}$ be square-free and let $K = \mathbb{Q}(\sqrt{d})$.*

- *If $d \not\equiv 1 \bmod 4$ then $\{1, \sqrt{d}\}$ is an integral basis of K.*
- *If $d \equiv 1 \bmod 4$ then $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$ is an integral basis of K.*

Proof. Course work 3. □

Example 3.27. Let α be a root of the polynomial $f(t) = t^3 + 11t + 4$. Note that $f(t)$ is irreducible in $\mathbb{Q}[t]$ as its reduction (mod 3) has no root. It follows from Theorem 1.27 that if we let $K = \mathbb{Q}(\alpha)$, then $[K : \mathbb{Q}] = 3$, and $1, \alpha, \alpha^2$ is a $\mathbb{Q}$-basis of K. Corollary 2.42 implies that

$$\Delta[1, \alpha, \alpha^2] = -1439 \cdot 2^2.$$

As 1439 is prime, we have $N = 2$, and we need to check whether any of the numbers $\frac{1}{2}(a + b\alpha + c\alpha^2)$, $a, b, c \in \{0, 1\}$ are algebraic integers. Let us start with $\frac{1}{2}(\alpha + \alpha^2)$. In order to see whether this element is an algebraic integer, we determine its minimal polynomial, using the theory of symmetric polynomials. Let $\alpha = \alpha_1, \alpha_2\alpha_3$ be the roots of $f(t)$. Then the polynomial

$$g(t) = \left(t - \frac{\alpha_1 + \alpha_1^2}{2}\right)\left(t - \frac{\alpha_2 + \alpha_2^2}{2}\right)\left(t - \frac{\alpha_3 + \alpha_3^2}{2}\right)$$

has $\frac{\alpha+\alpha^2}{2}$ as a root, and as it is symmetric in $\alpha_1, \alpha_2, \alpha_3$, it is coefficients in $\mathbb{Q}$ by Corollary 2.21. Explicitly, if we write

$$g(t) = t^3 + at^2 + bt + c,$$

then one can show (after a long and messy calculation) that $a = 11$, $b = 36$ and $c = 4$. Hence $\frac{\alpha+\alpha^2}{2}$ is an algebraic integer.

We now have a new basis of K consisting of algebraic integers, namely $1, \alpha, \frac{\alpha+\alpha^2}{2}$. Is it an integral basis? We have

$$\begin{aligned} \Delta\left[1, \alpha, \frac{\alpha + \alpha^2}{2}\right] &= \begin{vmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & \frac{1}{2} & \frac{1}{2} \end{vmatrix}^2 \times \Delta[1, \alpha, \alpha^2] \\ &= \frac{1}{4}\Delta[1, \alpha, \alpha^2] \\ &= -1439, \end{aligned}$$

which is prime, so $1, \alpha, \frac{\alpha+\alpha^2}{2}$ is an integral basis by Corollary 3.22.