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 $a_i \in \mathbb{Z}_{\geq 0}$ 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. □

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:

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

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 $1 \leq i \leq mn$. 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

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

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. □

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:

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

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. □

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 $1, \theta, \dots, \theta^{n-1}$ 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 Lecture 6

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

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*

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

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 $b_0, \dots, b_{n-1} \in \mathbb{Z}$ 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 $c_0, \dots, c_{n-1} \in \mathbb{Z}$ 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 $x_1, \dots, x_d$ 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 $x_1, \dots, x_n$ 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 $1, \alpha, \alpha^2, \dots$ 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 $c_0, \dots, c_N \in \mathbb{Z}$ 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 $1, \dots, \alpha^{n-1}$.

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

$$\beta = a_1w_1 + \cdots + a_nw_n$$

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

$$\psi_1 = \beta - aw_1, \quad \text{and} \quad \psi_i = w_i \quad \text{for } 2 \leq i \leq n.$$

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 $\pmod 2$ 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 $K = \mathbb{Q}(\sqrt{n})$.*

- *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 $\pmod 3$ 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.

Lecture 9

3.2.2. *Tricks for calculating integral bases.* Let $K = \mathbb{Q}(\theta)$, and let $f(t)$ be the minimal polynomial of θ over $\mathbb{Q}$. We assume without loss of generality that $\theta \in O_K$. If $f(t)$ satisfies Eisenstein's criterion, then there is a special trick for calculating integral bases. We start with the following two elementary observations.

Lemma 3.28. *Suppose that $f(t)$ satisfies Eisenstein's criterion for the prime p. We have $p|N(\theta)$, but $p^2 \nmid N(\theta)$.*

Proof. This is clear since

$$f(t) = \prod_{i=1}^{n}(t - \sigma_i(\theta)),$$

where $\sigma_1, \ldots, \sigma_n$ are the embeddings of K. □

Lemma 3.29. *Suppose that $f(t)$ satisfies Eisenstein's criterion for the prime p. Then $p|\Delta[1, \theta, \ldots, \theta^{n-1}]$.*

Proof. We use Proposition 2.39 to prove the lemma. By assumption, $f(t) \equiv t^n \pmod{p\mathbb{Z}[t]}$ so we have $Df(t) \equiv nt^{n-1} \pmod{p\mathbb{Z}[t]}$. Using the definition of the norm as a product over all the conjugates, we deduce that

$$N(Df(\theta)) \equiv N(n\theta^{n-1}) \pmod{p} \text{ in } \mathbb{Z}.$$

Now $N(n\theta^{n-1}) = N(n)N(\theta)^{n-1}$ and $p|N(\theta)$ by Lemma 3.28, which implies that

$$N(Df(\theta)) \equiv 0 \pmod{p}.$$

As $\Delta[1, \theta, \ldots, \theta^{n-1}] = (-1)^{\frac{n(n-1)}{2}}N(Df(\theta))$, this finishes the proof. □

So p could potentially make our life difficult when we calculate an integral basis. However the next result tells us that we will never need to worry about this factor.

Proposition 3.30. *Let $K = \mathbb{Q}(\theta)$; let $n = [K : \mathbb{Q}]$. Let $f(t)$ be the minimal polynomial of θ over $\mathbb{Q}$, and assume that $f(t)$ is Eisenstein for the prime p. Let*

$$\alpha = \frac{1}{p}\sum_{i=0}^{n-1} a_i\theta^i, \quad a_i \in \{0, \ldots, p-1\} \text{ not all } 0.$$

Then α is not an algebraic integer.

Before we give the proof, we studyan example to illustrate how useful Proposition 3.30 is.

Example 3.31. Let θ be a root of the polynomial $f(t) = t^p - p$, and let $K = \mathbb{Q}(\theta)$. Then $N(\theta) = -p$ and $Df(t) = pt^{p-1}$, and so

$$\begin{aligned}\Delta[1, \theta, \ldots, \theta^{p-1}] &= (-1)^{\frac{p(p-1)}{2}}N(p\theta^{p-1}) \\ &= p^{2p-1}.\end{aligned}$$

We have $N = p^{p-1}$, so according to the algorithm, we need to check whether any of the numbers

$$\frac{1}{p^{p-1}}\sum_{i=0}^{p-1} a_i\theta^i$$

with $0 \leq a_i < p^{p-1}$ are algebraic integers. We know from Proposition 3.30 that no element of the form

$$\frac{1}{p}(b_0 + \cdots + b_{p-1}\theta^{p-1}) \qquad b_i \in \{0, \ldots, p-1\}, \quad \text{not all zero} \tag{7}$$

is an algebraic integer.

If $x = \frac{1}{p^{p-1}} \sum_{i=0}^{p-1} a_i \theta^i$ for some $0 \leq a_i < p^{p-1}$, not all zero, write

$$x = \frac{1}{p^r} \sum_{i=0}^{p-1} a_i' \theta^i,$$

with $a_i' \in \mathbb{Z}$ for all i and $(a_j, p) = 1$ for at least one j. If x is an algebraic integer, then so is $p^{r-1}x$. But we have

$$p^{r-1}x = y + \frac{1}{p}(b_0 + \cdots + b_{p-1}\theta^{p-1}) \qquad b_i \in \{0, \ldots, p-1\}, \quad y \in \mathbb{Z}[\theta].$$

Note that of the b_i must be non-zero since $(a_j, p) = 1$ for at least one j. But if $p^{r-1}x \in O_K$ and $y \in \mathbb{Z}[\theta] \subset O_K$, then

$$\frac{1}{p}(b_0 + \cdots + b_{p-1}\theta^{p-1}) = p^{r-1}x - y \in O_K.$$

But this gives a contradiction by (7). Hence $1, \theta, \ldots, \theta^{n-1}$ is an integral basis of K.

We now prove Proposition Proposition 3.30:

Proof. Suppose $\alpha \in O_K$, and let a_d be the first non-zero coefficient. We therefore have

$$\alpha = \frac{1}{p} \sum_{i=d}^{n-1} a_i \theta^i \in O_K.$$

We can write this as

$$\alpha = \frac{1}{p}\left(a_d\theta^d + \theta^{d+1}\delta\right), \quad \delta \in O_K.$$

Multiplying through by θ^{n-1-d} we still have an element of O_K:

$$\theta^{n-1-d}\alpha = \frac{a_d\theta^{n-1}}{p} + \frac{\theta^n\delta}{p} \in O_K.$$

On the one hand, since $f(t)$ satisfies Eisenstein's criterion we have

$$\theta^n = pg(\theta), \quad \text{for some } g(t) \in \mathbb{Z}[t].$$

It follows that

$$\frac{a_d\theta^{n-1}}{p} + g(\theta)\delta \in O_K.$$

On the other hand since $g(\theta)\delta \in O_K$ we have

$$\frac{a_d\theta^{n-1}}{p} \in O_K.$$

We shall calculate the norm of this to get a contradiction:

$$N\left(\frac{a_d\theta^{n-1}}{p}\right) = \frac{a_d^n N(\theta)^{n-1}}{p^n}.$$

By Lemma 3.28, we have $N(\theta) = pr$, where $p \not| r$. Hence we have

$$N\left(\frac{a_d\theta^{n-1}}{p}\right) = \frac{a_d^n p^{n-1} r^{n-1}}{p^n} = \frac{a_d^n r^{n-1}}{p}.$$

However this cannot be an integer, since neither a_d nor r is a multiple of p. This gives the contradiction. □

3.3. **Example: cyclotomic fields.** In this section, we will use Proposition 3.30 to determine an integral basis of *cyclotomic fields*; these fields are of great importance in current reseach in algebraic number theory.

Definition 3.32. *A* cyclotomic field *is a field of the form $K = \mathbb{Q}(\zeta)$, where ζ is a primitive* m*th root of unity for some m.*

We will specialize to the case $K = \mathbb{Q}(\zeta)$, where p is an odd prime. We have already seen that the minimal polynomial of ζ over $\mathbb{Q}$ is

$$f(t) = t^{p-1} + \cdots + t + 1.$$

Let $\lambda = \zeta - 1$. Then the minimal polynomial of λ is

$$g(t) = t^{p-1} + \tbinom{p}{1}t^{p-2} + \cdots + \tbinom{p}{p-1}.$$

In particular, $g(t)$ is Eisenstein for p.

Lemma 3.33. *We have $N(\zeta) = 1$ and $N(\lambda) = p$.*

Proof. Clear. □

Theorem 3.34. *We have*

$$\Delta[1, \lambda, \ldots, \lambda^{p-2}] = (-1)^{\frac{p-1}{2}} p^{p-2},$$

and $\{1, \lambda, \ldots, \lambda^{p-2}\}$ is an integral basis in K.

Proof. By Proposition 2.39 we have

$$\Delta[1, \lambda, \ldots, \lambda^{p-2}] = (-1)^{\frac{(p-1)(p-2)}{2}} N(Dg(\lambda)).$$

To calculate $N(Dg(\lambda))$, we use a trick: recall that $g(t) = \frac{(t+1)^p - 1}{t}$. By the quotient rule, we have

$$Dg(t) = \frac{p(t+1)^{p-1}t - \big((t+1)^p - 1\big)}{t^2},$$

so $Dg(\lambda) = p\frac{\zeta^{p-1}}{\lambda}$. We deduce that

$$N(Dg(\lambda)) = N(p)N(\zeta)^{p-1}N(\lambda)^{-1} = p^{p-2}$$

by Lemma 3.33. Since p is odd, we have $(-1)^{\frac{(p-1)(p-2)}{2}} = (-1)^{\frac{p-1}{2}}$. Hence

$$\Delta[1, \lambda, \ldots, \lambda^{p-2}] = (-1)^{\frac{p-1}{2}} p^{p-2}$$

as claimed.

The only prime whose square divides this is p. However $g(t)$ satisfies Eisenstein's criterion at p, so we conclude by the same argument as in the example after Proposition 3.30. □

Remark 3.35. *If n is not prime and $K = \mathbb{Q}(\zeta)$, then it is still true that $O_K = \mathbb{Z}[\zeta]$, but the proof is harder. The degree of the extension is given by*

$$[K : \mathbb{Q}] = \#(\mathbb{Z}/n)^\times,$$

which is the same as the number of primitive n-th roots of unity in K. If $n = p^a$ for some prime p, then f_λ still satisfies Eisenstein's criterion for the prime p, and we again use this fact to prove that $\{\lambda^i\}$ is an integral basis. If n is not a power of a prime then f_λ does't satisfy Eisenstein's criterion, so the proof is quite different in this case.

4. Factorisation in O_K

Lecture 10

4.1. **Units and irreducible elements in O_K.** Now let K be a number field. We first study the units in O_K.

Proposition 4.1. *An element $x \in O_K$ is a unit if and only if $|N(x)| = 1$.*

Proof. Since $N(x) \in \mathbb{Z}$ by Proposition 3.14 and N is multiplicative, it is clear that if $x \in O_K^\times$, then $|N(x)| = 1$. Suppose now that $N(x) = 1$. (The proof when $N(x) = -1$ is similar.) By definition, we have

$$N(x) = \prod_{i=1}^{n} \sigma_i(x),$$

where $\sigma_1, \ldots, \sigma_n$ are the different embeddings of K into $\mathbb{C}$. Without loss of generality, assume that $\sigma_1(x) = x$. Then

$$N(x) = 1 \quad \Leftrightarrow \quad x \cdot \big(\sigma_2(x) \cdots \sigma_n(x)\big) = 1,$$

so $\sigma_2(x) \cdots \sigma_n(x) = x^{-1} \in K$. It follows that $x \in O_K^\times$ if and only if $\sigma_2(x) \cdots \sigma_n(x) \in O_K$.

Now note that if $\sigma_i(x)$ is an algebraic integer for all i, since it has the same minimal polynomial as x. Hence $\sigma_2(x) \cdots \sigma_n(x)$ is an algebraic integer. But the algebraic integers in K are precisely the elements of O_K, so $\sigma_2(x) \cdots \sigma_n(x) \in O_K$, which finishes the proof. □

As a corollary, let us determine $O_K^\times$, where K is an imaginary quadratic field.

Proposition 4.2. *Let $K = \mathbb{Q}(\sqrt{-d})$, where $d > 0$. Then*

$$O_K^\times = \begin{cases} \{\pm 1, \pm i\} & \text{if } d = 1 \\ \{\pm 1, \pm\omega, \pm\omega^2 : \omega = e^{\frac{2\pi i}{3}}\} & \text{if } d = 3 \\ \{\pm 1\} & \text{for any other } d > 0 \end{cases}$$

Proof. Exercise sheet. □

Remark 4.3. *You see that in this example, all the units are in fact roots of unity. This is not true in general; you will see an example on problem sheet 3.*

Remark 4.4. *It is a natural question to ask whether one can say something in general about the unit group in the ring of integers of a number field. We will return to this question later.*

Suppose now that $x \in O_K$.

Lemma 4.5. *If $N(x) = \pm p$ for a prime number p then x is irreducible.*

Proof. Suppose that $x = yz$ for some $y, z \in O_K$. Then

$$N(x) = N(yz) = N(y)N(z),$$

so one of y, z must have norm of absolute value equal to 1. But any element of absolute norm equal to 1 is a unit by Proposition 4.1. Hence x is irreducible. □

The following theorem shows that one can factorise any non-zero element in O_K:

Theorem 4.6. *Let $x \in O_K$ be non-zero. Then there is a unit $u \in O_K^\times$ and irreducible elements $\pi_1, \ldots \pi_n$ such that*

$$x = u\pi_1 \cdots \pi_n.$$

Proof. We proceed by induction on $|N(x)|$. If $|N(x)| = 1$, then x is a unit by Proposition 4.1. Suppose therefore that the theorem is true for all elements $y \in O_K$ such that $|N(y)| < |N(x)|$. Then there are two possibilities: if x is irreducible, then the theorem is clearly true for x. If it is not irreducible, then there exist $y, z \in O_K$ which are not units such that $x = yz$. Note that Proposition 4.1 and the fact that the norm is multiplicative imply that $|N(y)|, |N(z)| < |N(x)|$. Hence both y and z can be factorized into irreducibles; therefore so can x. □

The problem with Theorem 4.6 is that O_K does usually *not* have unique factorisation! However, without this fact algebraic number theory would be pretty dull.

Example 4.7. Let $K = \mathbb{Q}(\sqrt{-10})$, so $O_K = \mathbb{Z}[\sqrt{-10}]$. We have two different factorizations of the number 10 in O_K, namely

$$10 = 2 \times 5 = -\sqrt{-10} \times \sqrt{-10}.$$

Furthermore the elements 2, 5 and $\sqrt{-10}$ are all irreducible. To see this we calculate their norms:

$$N(2) = 4, \quad N(5) = 25, \quad N(\sqrt{-10}) = 10.$$

The norm of a general element of the ring is

$$N(x + y\sqrt{-10}) = x^2 + 10y^2.$$

Since this is never equal to ± 2 or ± 5, it follows that the above elements are irreducible, and none of them is a unit multiple of another. Therefore O_K does not have unique factorization.

4.1.1. *Unique factorisation in imaginary quadratic fields.* The question of which imaginary quadratic fields have unique factorisation is quite subtle.

Theorem 4.8. *Let $K = \mathbb{Q}(\sqrt{d})$. Then O_K is UFD for*

$$d \in \{-1, -2, -3, -7, -11\}.$$

In order to prove Theorem 4.8, we show that under these assumptions $(O_K, |N(\sim)|)$ is a Euclidean domain. Recall Definition 1.12:

Definition 4.9. *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, ϕ) 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 $\phi(r) < \phi(y)$.*

Proof of Theorem 4.8. Claim. For $(O_K, |N(\sim)|)$ to be a Euclidean domain, it is sufficient to prove the following statement: for all $\alpha \in K$ there $\gamma \in O_K$ such that

$$|N(\alpha - \gamma)| < 1.$$

Proof of claim: let $\alpha = \frac{x}{y}$, and take $q = \gamma$ and $r = x - qy$. Then

$$|N(r)| = |N((\alpha - \gamma)y)| < |N(y),$$

which proves the claim.

Suppose now that $\alpha = r + s\sqrt{d} \in K$. If $d \not\equiv 1 \pmod 4$ (i.e. $d = -1, -2$), take $u, v \in \mathbb{Z}$ to be of minimal distance to r and s, respectively. Then

$$\left|(r-u)^2 - d(s-v)^2\right| \leq \left|\left(\frac{1}{2}\right)^2 + 2\left(\frac{1}{2}\right)^2\right| < 1.$$

In the remaining three cases we have $d \equiv 1 \pmod 3$, so we need to find

$$\gamma = u + v\left(\frac{1+\sqrt{d}}{2}\right) \qquad \text{with } u, v \in \mathbb{Z}$$

such that

$$\left|(r - u - \frac{1}{2}v)^2 - d(s - \frac{1}{2}v)^2\right| < 1.$$

Take v to be the integer closest to $2s$, so $|v - 2s| \leq \frac{1}{2}$; we can then find a $u \in \mathbb{Z}$ such that

$$\left|r - u - \frac{1}{2}v\right| \leq \frac{1}{2}.$$

For $d = -3, -7, -11$, this implies that

Lecture 11

$$\left|(r - u - \frac{1}{2}v)^2 - d(s - \frac{1}{2}v)^2\right| \leq \left|\frac{1}{4} + \frac{11}{16}\right| < 1.$$

□

Remark 4.10. *(1) One can show that if $d < -11$ is squarefree, then $\mathbb{Q}(\sqrt{d})$ is not Euclidean.*

(2) We call a number field K norm-Euclidean *if $|N(\sim)|$ is a Euclidean fuction on K. Thanks to the work of many mathematicians, we know that there are only finitely many* real-quadratic *fields which are norm-Euclidean. however, unlike in the imaginary quadratic case, it is not known whether a real-quadratic field can be Euclidean but not norm-Euclidean.*

The main insight concerning the problem of non-unique factorisation in number fields was that the irreducible elements are not the correct analogue of the prime numbers - the right thing to do is to factorise into *maximal ideals ideals.*

4.2. **Factorisation into ideals.**

Definition 4.11. *Let R be a ring. A subset I of R is an ideal if it satisfies the following properties:*

- *if $x, y \in I$, then $x + y \in I$;*
- *if $x \in I$ and $r \in R$, then $rx \in I$.*

An ideal I is proper *if $I \neq R$.*

Example 4.12. (1) The set $\{2x + t^2 y : x, y \in \mathbb{Z}[t]\}$ is an ideal in $\mathbb{Z}[t]$.

(2) Let R be the ring of continuous functions $\mathbb{R} \to \mathbb{R}$. Then

$$\{f \in R : f(1) = 0\}$$

is an ideal of R.

Example 4.13. More generally, if R is a ring and $a \in R$, then $\{ra : r \in R\}$ is an ideal in R. It is called the *ideal generated by a* and denoted by $\langle a \rangle$. An ideal I is *principal* if it is generated by one element. Similarly, if $a_1, \ldots, a_n \in R$, define the ideal generated by the a_i to be

$$\langle a_1, \ldots, a_n \rangle = \{r_1 a_1 + \cdots + r_n a_n : r_i \in R\}.$$

Thei definition generalizes in the obvious way to the ideal generated by an infinite number of elements.

Remark 4.14. *The ideal in example (2) above is equal to $\langle 2, t^2 \rangle$.*

Definition 4.15. *Let R be a ring and let I be a proper ideal of R. Then I is* maximal *if there is no other proper ideal J of R containing I.*

Example 4.16. The ideal $\langle 2 \rangle$ is maximal in $\mathbb{Z}$, but the ideal $\langle 6 \rangle$ is not. More generally, if $n \in \mathbb{Z}$ is non-zero, then $\langle n \rangle$ is a maximal ideal if and only if n is prime.

If R is a ring, we can define define the product of two ideals.

Definition 4.17. *Let I, J be ideals in a ring R. Define the product IJ by*

$$IJ = \langle xy : x \in I,\ y \in J \rangle.$$

I.e. IJ is the ideal generated by products of elements of I by elements of J.

Example 4.18. Let $x, y \in R$. Then

$$\langle x \rangle \langle y \rangle = \langle xy \rangle.$$

More generally, if $x, y, u, v \in R$, then

$$\langle x, y \rangle \langle u, v \rangle = \langle xu, xv, yu, yv \rangle.$$

Remark 4.19. *The ideal IJ is not necessarily equal to the set $\{xy : x \in I,\ y \in J\}$: if $R = \mathbb{Z}[t]$ and $I = \langle 2, t \rangle$, $J = \langle 3, t \rangle$. Then $IJ = \langle 6, t \rangle$, even though t cannot be written of the form ij with $i \in I$ and $j \in J$.*

Later in the course, we shall prove the following theorem, which takes the place of uniqueness of factorization of elements:

Theorem 4.20. *Let K be a number field, and let $I \subset O_K$ be a non-zero ideal. Then there are maximal ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ in O_K such that*

$$I = \mathfrak{p}_1 \cdots \mathfrak{p}_n.$$

Furthermore this factorisation is unique up to reordering of the factors.

Remark 4.21. *This theorem generalizes the uniqueness of factorisation of the integers: if $n = p_1 \cdots p_n$ for some prime numbers p_i, then*

$$\langle n \rangle = \langle p_1 \rangle \cdots \langle p_n \rangle.$$

We us now see how Theorem 4.20 solves the problem of factorising the number 10 in $\mathbb{Z}[\sqrt{-10}]$.

Example 4.22. Consider the ideals

$$\mathfrak{p} = \langle 2, \sqrt{-10} \rangle, \quad \mathfrak{q} = \langle 5, \sqrt{-10} \rangle.$$

Then

$$\begin{aligned}
\mathfrak{pq} &= \langle 2, \sqrt{-10}\rangle\langle 5, \sqrt{-10}\rangle \\
&= \langle 10, 2\sqrt{-10}, 5\sqrt{-10}, -10\rangle \\
&= \langle 10, 2\sqrt{-10}, 5\sqrt{-10}, -10, \sqrt{-10}\rangle \\
&= \langle \sqrt{-10}\rangle \\
\mathfrak{p}^2 &= \langle 2, \sqrt{-10}\rangle\langle 2, \sqrt{-10}\rangle \\
&= \langle 4, 2\sqrt{-10}, -10\rangle \\
&= \langle 4, 2\sqrt{-10}, -10, 2\rangle \\
&= \langle 2\rangle \\
\mathfrak{q}^2 &= \langle 5, \sqrt{-10}\rangle\langle 5, \sqrt{-10}\rangle \\
&= \langle 25, 5\sqrt{-10}, -10\rangle \\
&= \langle 25, 5\sqrt{-10}, -10, 5\rangle \\
&= \langle 5\rangle.
\end{aligned}$$

So our two distinct factorizations into elements can both be refined to the same factorization into ideals:

$$\langle 10\rangle = \langle 2\rangle \times \langle 5\rangle = \mathfrak{p}^2\mathfrak{q}^2 = \langle\sqrt{-10}\rangle^2 = (\mathfrak{pq})^2.$$

Remark 4.23. *In general, if we have a number field K and $x \in O_K$ is non-zero, then we can factorise $\langle x\rangle$ uniquely into a product of maximal ideals,*

$$\langle x\rangle = \mathfrak{p}_1 \cdots \mathfrak{p}_n. \tag{8}$$

We can also factorise x (not necessarily uniquely) into a product of irreducibles,

$$x = y_1 \cdots y_r,$$

which induces a factorisation into ideals

$$\langle x\rangle = \langle y_1\rangle \cdots \langle y_r\rangle. \tag{9}$$

The factorisations (8) *and* (9) *agree if and only if $n = r$ and (after some permutation of the indices) we have $\mathfrak{p}_i = \langle y_i\rangle$; i.e. the unique factorisation of $\langle x\rangle$ into maximal ideals induces a factorisation of x into irreducibles if and only if each maximal ideal is principal.*

Hence, in order to understand 'how far away' the ring O_K is from having unique factorisation into irreducibles, we need to understand 'how far away' a general ideal is from being principal. For this purpose we define the class group *of K to be the group*

$$\mathrm{Cl}(K)\text{" = "}\mathcal{I}(K)/\mathcal{P}(K),$$

where $\mathcal{I}(K)$ is the set of ideals of K, and $\mathcal{P}(K)$ is the set of principal ideals. (In fact these sets are semi-groups, although the quotient is a group.) The class group measure how far away O_K is from having unique factorisation into irreducibles: Cl_k is trivial if and only if O_K is a principal ideal domain, and has unique factorization. We shall prove that $\mathrm{Cl}(K)$ is always a finite group (i.e. the failure of unique factorisation into irreducibles is never too bad), and calculate it in a lot of examples.

*(*This is a vague sketch of what we are going to do. The definition of the class group does not make sense the way it is stated, because neither $\mathcal{I}(K)$ nor $\mathcal{P}(K)$ have the structure of a group. We will discuss this issue at a later stage.*)*

4.3. **Prime ideals.**

Definition 4.24. *Let R be a ring, and let $\mathfrak{p}$ be an ideal in R. Then $\mathfrak{p}$ is* prime *if it is a proper ideal and for $x, y \in R$*

$$xy \in \mathfrak{p} \Rightarrow (x \in \mathfrak{p} \text{ or } y \in \mathfrak{p}).$$

Remark 4.25. *A ring R is an* integral domain *if and only if (0) is a prime ideal.*

We can give an alternative characterisation of a prime ideal, which is closer in spirits to the properties of prime numbers.

Lemma 4.26. *Let $\mathfrak{p}$ be an ideal of a ring R. Then $\mathfrak{p}$ is prime if and only if the following condition is satisfied: if I, J are ideals of R such that $IJ \subset \mathfrak{p}$, then $I \subset \mathfrak{p}$ or $J \subset \mathfrak{p}$.*

Lecture 12

Proof. Assume $\mathfrak{p}$ is prime and suppose $IJ \subseteq \mathfrak{p}$. We'll assume that $I \not\subseteq \mathfrak{p}$ and prove that $J \subseteq \mathfrak{p}$. Let $x \in I \setminus \mathfrak{p}$. For every $y \in J$ we have $xy \in IJ$. Therefore $xy \in \mathfrak{p}$. Since $x \notin \mathfrak{p}$ and $\mathfrak{p}$ is prime, it follows that $y \in \mathfrak{p}$. Hence $J \subseteq \mathfrak{p}$.

Conversely, assume that $\mathfrak{p}$ satisfies the condition and suppose $xy \in \mathfrak{p}$. This implies $\langle xy \rangle \subseteq \mathfrak{p}$. Therefore $\langle x \rangle \langle y \rangle \subseteq \mathfrak{p}$. By the assumption, we have $\langle x \rangle \subseteq \mathfrak{p}$ or $\langle y \rangle \subseteq \mathfrak{p}$. This implies $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$. □

Example 4.27. Let p be a prime number, and let $n \in \mathbb{Z}$ be non-zero. Then $p|n$ if and only if $\langle n \rangle \subset \langle p \rangle$, and the fundamental property of primes numbers

$$p|mn \quad \Rightarrow \quad p|m \text{ or } p|n$$

is equivalent to the statement of Lemma 4.26.

Recall that if I is an ideal in a ring R, then we can look at the *quotient ring* R/I:

Definition 4.28. *The elements of R/I are the cosets of I in R. Addition and multiplication are defined as follows:*

$$(a + I) + (b + I) = a + b + I$$
$$(a + I)(b + I) = ab + I.$$

The unit element in R/I is the coset $1 + I$.

Lemma 4.29. *Let $\mathfrak{p}$ be an ideal in a ring R. Then*

- *$\mathfrak{p}$ is a maximal ideal if and only if $R/\mathfrak{p}$ is a field.*
- *$\mathfrak{p}$ is a prime ideal if and only if $R/\mathfrak{p}$ is an integral domain.*

Proof. Problem sheet 4. □

Corollary 4.30. *Every maximal ideal is prime.*

Proof. Since every field is an integral domain, this shows that $\mathfrak{p}$ is prime. □

Warning 1. *The converse of Corollary 4.30 is false! For example if R is an integral domain but not a field, then (0) is a prime ideal but is not maximal.*

However, we have a partial converse to Corollary 4.30.

Proposition 4.31. *Let $\mathfrak{p}$ be a prime ideal in a ring R, and suppose that $R/\mathfrak{p}$ is finite. Then $\mathfrak{p}$ is maximal.*

Proof. Proposition 4.31 follows immediately from Lemma 4.29 and the fact that a finite integral domain is a field: Let A be a finite integral domain, and let $x \in A$ be non-zero. We have to show that there exists $y \in A$ such that $xy = 1$. Consider the map $\times x : A \to A$. As A is an integral domain, the map is injective. As A is finite, this implies that the map is also surjective, so there exists $y \in A$ such that $xy = 1$. □

We now return to the case when $R = O_K$ for some number field K.

Proposition 4.32. *If $\mathfrak{a}$ is any non-zero ideal in O_K, then $O_K/\mathfrak{a}$ is finite.*

Before we prove this, we note the following consequence:

Corollary 4.33. *Every non-zero prime ideal in O_K is maximal.*

Proof. Immediate from Propositions 4.31 and 4.32. □

We now prove Proposition 4.32.

Proof. Let $\mathfrak{a}$ be a non-zero ideal, and choose a non-zero element $x \in \mathfrak{a}$. Let $N = N(x)$. Let $\sigma_1 = \mathrm{id}, \sigma_2, \ldots, \sigma_n$ be the embeddings of K into $\mathbb{C}$. By definition, we have

$$N(x) = x\sigma_2(x) \cdots \sigma_n(x) \in \mathbb{Z} \subset O_K.$$

As $x \in \mathfrak{a} \subset O_K$, we have $\sigma_2(x) \cdots \sigma_n(x) \in O_K$, which - by the property of an ideal - implies that $N \in \mathfrak{a}$, and hence $\langle N \rangle \subseteq \mathfrak{a}$. It follows that we have a quotient map (which is surjective by construction)

$$O_K/\langle N \rangle \to O_K/\mathfrak{a},$$

which identifies $O_K/\mathfrak{a}$ with a quotient of $O_K/\langle N\rangle$. Now the fact the O_K has an integral basis implies that $O_K \cong \mathbb{Z}^n$ as an additive group (here $n = [K : \mathbb{Q}]$), so

$$O_K/\langle N\rangle \cong (\mathbb{Z}/N\mathbb{Z})^n,$$

which is finite, which implies that $O_K/\mathfrak{a}$ is finite as well. □

Definition 4.34. *Let K be a number field, and let $\mathfrak{a}$ be a non-zero ideal in O_K. Define the* norm of $\mathfrak{a}$ *to be $N(\mathfrak{a}) = |O_K/\mathfrak{a}|$. This is finite by Proposition 4.32.*

Remark 4.35. *We will return later to the question of how to calculate the norm of an ideal. Before that, we want to prove Theorem 4.20.*

4.4. **Uniqueness of Factorization into ideals.** The aim of this section is the proof of Theorem 4.20, which states that if K is a number field, then every non-zero ideal in O_K has a unique factorisation into maximal ideals. We start by recalling the following definition.

Definition 4.36. *A ring R is called a Noetherian ring if it satisfies the following condition (called the* ascending chain condition*): For every ascending sequence of ideals of R:*

$$I_1 \subseteq I_2 \subseteq \dots,$$

there is an $N \in \mathbb{N}$ such that

$$I_N = I_{N+1} = I_{N+1} = \dots,$$

i.e. every ascending chain of ideals stabilizes eventually.

Lemma 4.37. *Let K be any number field. Then O_K is noetherian.*

Proof. If we have a sequence of (non-zero) ideals

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \dots,$$

then by the 3rd isomorphism theorem, we have an isomorphism of additive groups:

$$O_K/\mathfrak{a}_{i+1} \cong (O_K/\mathfrak{a}_i)/(\mathfrak{a}_{i+1}/\mathfrak{a}_i).$$

for all $i \geq 1$. Hence

$$N(\mathfrak{a}_{i+1}) = N(\mathfrak{a}_i)/|\mathfrak{a}_{i+1}/\mathfrak{a}_i|. \tag{10}$$

(Note that $|\mathfrak{a}_{i+1}/\mathfrak{a}_i| < \infty$ since $\mathfrak{a}_{i+1}/\mathfrak{a}_i \subset O_K/\mathfrak{a}_i$ and $O_K/\mathfrak{a}_i$ is finite by Proposition 4.32.) It follows that $N(\mathfrak{a}_{i+1}) < N(\mathfrak{a}_i)$ with equality if and only if $\mathfrak{a}_{i+1} = \mathfrak{a}_i$. Hence we have a decreasing sequence of natural numbers:

$$N(\mathfrak{a}_1) \geq N(\mathfrak{a}_2) \geq \dots.$$

Clearly there is an N such that

$$N(\mathfrak{a}_N) = N(\mathfrak{a}_{N+1}) = \dots,$$

so $\mathfrak{a}_N = \mathfrak{a}_{N+1} = \dots$. □

Remark 4.38. *If R is a Noetherian ring then there is a strategy for proving results about ideals of R as follows: assume that the result if false, and suppose I_1 is a counterexample. We call I_1 a* maximal counterexample *if every ideal containing I_1 satisfies the theorem. If I_1 is not a maximal counterexample then choose a bigger counterexample I_2. If I_2 is not a maximal counterexample then choose a bigger counterexample I_3 etc. In this way we obtain a sequence of ideals which must end in a maximal counterexample. So we may always assume that if a theorem about ideals is false then there is a maximal counterexample.*

An example of this method is the following:

Lemma 4.39. *Let $\mathfrak{a} \subseteq O_K$ be a non-zero ideal. Then there are maximal ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ such that*

Lecture 13

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathfrak{a}.$$

Proof. Suppose not and let $\mathfrak{a}$ be a maximal counterexample. Clearly $\mathfrak{a}$ is not a maximal ideal; otherwise we could take $\mathfrak{p}_1 = \mathfrak{a}$. Since $\mathfrak{a}$ is non-zero, we know that $\mathfrak{a}$ is not prime. By Lemma 4.26, it follows that there are ideals $\mathfrak{b}, \mathfrak{c}$ such that $\mathfrak{bc} \subset \mathfrak{a}$ but neither $\mathfrak{b}$ nor $\mathfrak{c}$ is a subset of $\mathfrak{a}$. By replacing $\mathfrak{b}$ and $\mathfrak{c}$ by

$$\langle \mathfrak{b}, \mathfrak{a}\rangle = \{b + a : b \in \mathfrak{b}, a \in \mathfrak{a}\}$$
$$\langle \mathfrak{c}, \mathfrak{a}\rangle = \{c + a : c \in \mathfrak{c}, a \in \mathfrak{a}\}$$

we may assume that $\mathfrak{b}$ and $\mathfrak{c}$ both contain $\mathfrak{a}$. By the maximality of our counterexample, it follows that we can find maximal ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ and $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ such that

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathfrak{b}, \quad \mathfrak{q}_1 \cdots \mathfrak{q}_s \subseteq \mathfrak{c}.$$

Hence

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \mathfrak{q}_1 \cdots \mathfrak{q}_s \subseteq \mathfrak{bc} \subseteq I\mathfrak{a},$$

which gives the required contradiction. □

We also need the following technical lemma:

Lemma 4.40. *Let $\mathfrak{a}$ be a non-zero ideal of O_K. If $x \in K$ satisfies $x\mathfrak{a} \subset \mathfrak{a}$ then $x \in O_K$.*

Proof. Recall that O_K is a free finitely generated $\mathbb{Z}$-module. Hence $\mathfrak{a} \subset O_K$ is also a finitely generated free $\mathbb{Z}$-module[1], say

$$\mathfrak{a} = \mathrm{Span}_{\mathbb{Z}}\{\alpha_1, \ldots, \alpha_r\}.$$

Multiplication by x takes $\mathfrak{a}$ to $\mathfrak{a}$, so we have

$$x\alpha_i = \sum_{j=1}^{n} c_{i,j}\alpha_j, \quad c_{i,j} \in \mathbb{Z}.$$

Hence if we let $C = \{c_{i,j}\}$, then

$$(C - xI_r)\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_r \end{pmatrix} = 0$$

This means that x is an eigenvalue of C and hence a root of the polynomial $f(t) = \det(tI_r - C)$, so is an algebraic integer. □

Definition 4.41. *A* fractional ideal *of O_K is a subset of the form $c^{-1}\mathfrak{a}$, where $\mathfrak{a}$ is an ideal in O_K and $c \in O_K$ is non-zero.*

Example 4.42. For any $r \in \mathbb{Q}$, $r\mathbb{Z}$ is a fractional ideal of $\mathbb{Z}$. However, the set

$$\{\frac{n}{5^m} : n \in \mathbb{Z}, m \geq 0\}$$

is not a fractional ideal of $\mathbb{Z}$.

Lemma 4.43. *(i) Every ideal in O_K is a fractional ideal.*

(ii) A subset $\mathfrak{b}$ of K is a fractional ideal if and only if (a) if $x, y \in \mathfrak{b}$, then $x + y \in \mathfrak{b}$ ($\mathfrak{b}$ is closed under addition), (b) $\mathfrak{b}O_K \subset \mathfrak{b}$, and (c) there exists $c \in O_K$ such that $c\mathfrak{b} \subseteq O_K$.

Proof. (i) is clear. (ii) is on Course work 4.

□

Note 4.44. *It is in fact clear that $\mathfrak{b}O_K = \mathfrak{b}$.*

Lemma 4.45. *If $\mathfrak{b}$ and $\mathfrak{c}$ are fractional ideals in K, then*

$$\mathfrak{bc} = \{x_1y_1 + \cdots + x_ny_n : x_i \in \mathfrak{b}, y_i \in \mathfrak{c}\}$$

is a fractional ideal.

Proof. By definition, there exist ideals $\mathfrak{a}$,$\mathfrak{d}$ in O_K and non-zero elements $b, c \in O_K$ such that $\mathfrak{b} = b^{-1}\mathfrak{a}$ and $\mathfrak{c} = d^{-1}\mathfrak{d}$. By definition, $\mathfrak{bc} = (bc)^{-1}\mathfrak{ad}$, so $\mathfrak{bc}$ is a fractional ideal. □

Definition 4.46. *Let $\mathfrak{a}$ be a non-zero ideal in O_K. Define*

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

Example 4.47. Let $\mathfrak{a} = \langle 2 \rangle$ in $\mathbb{Z}$. Then

$$\mathfrak{a}^{-1} = \frac{1}{2}\mathbb{Z}.$$

[1] of the same rank, as $O_K/\mathfrak{a}$ is finite by Proposition 4.32

Example 4.48. Let $K = \mathbb{Q}(\sqrt{6})$, so $O_K = \mathbb{Z}[\sqrt{6}]$, i.e. $1, \sqrt{6}$ is an integral basis of K. Let $\mathfrak{p} = \langle 2, \sqrt{6}\rangle$. Then

$$\begin{aligned}
\mathfrak{p}^{-1} &= \{\alpha : \alpha\mathfrak{p} \subset \mathbb{Z}[\sqrt{6}]\} \\
&= \{x + y\sqrt{6} : x, y \in \mathbb{Q}, (x + y\sqrt{6})\langle 2, \sqrt{6}\rangle \subset \mathbb{Z}[\sqrt{6}]\} \\
&= \{x + y\sqrt{6} : x, y \in \mathbb{Q}, 2(x + y\sqrt{6}) \in \mathbb{Z}[\sqrt{6}] \quad \text{and} \quad \sqrt{6}(x + y\sqrt{6}) \in \mathbb{Z}[\sqrt{6}]\} \\
&= \{x + y\sqrt{6} : x, y \in \mathbb{Q}, 2x \in \mathbb{Z}, 2y \in \mathbb{Z}, x \in \mathbb{Z}, 6y \in \mathbb{Z}\} \\
&= \{x + y\sqrt{6} : x \in \mathbb{Z}, 2y \in \mathbb{Z}\}.
\end{aligned}$$

Example 4.49. We have $O_K^{-1} = O_K$.

Remark 4.50. *(i) If $\mathfrak{a} \subset \mathfrak{b}$, then $\mathfrak{b}^{-1} \subset \mathfrak{a}^{-1}$.*
(ii) It is clear from the definition that $O_K \subset \mathfrak{a}^{-1}$.

Lemma 4.51. *If $\mathfrak{a}$ is any non-zero ideal in O_K, then $\mathfrak{a}^{-1}$ is a fractional ideal. Moreover, if $\mathfrak{a} \neq O_K$, then $\mathfrak{a}^{-1} \neq O_K$ (i.e. $\mathfrak{a}^{-1}$ is strictly bigger than O_K).*

Proof. Let $c \in \mathfrak{a}$ be non-zero. Then $c\mathfrak{a}^{-1} \subset O_K$, and $\mathfrak{a}^{-1}$ is clearly closed under addition and under multiplication by O_K, so $\mathfrak{a}^{-1}$ is a fractional ideal by Lemma 4.43 (ii). Lecture 14

Suppose now that $\mathfrak{a} \neq O_K$. By Remark 4.50, it is sufficient to prove that $\mathfrak{a}^{-1} \not\subset O_K$ when $\mathfrak{a}$ is maximal. Let $c \in \mathfrak{a} \setminus \{0\}$. Then by Lemma 4.39, there exist prime ideals $\mathfrak{p}_i$ such that $(c) \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r$. We take r to be as small as possible. As $\mathfrak{a} \supset (c)$, it follows that $\mathfrak{a} \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r$. Since $\mathfrak{a}$ is maximal (and hence prime), it follows that there exists i such that $\mathfrak{a} \supset \mathfrak{p}_i$. Since $\mathfrak{p}_i$ is maximal by Corollary 4.33, we know that in fact $\mathfrak{a} = \mathfrak{p}_i$. Without loss of generality $i = 1$.

There are now two cases:

(1) $r = 1$: then
$$\mathfrak{a} = (c) = \mathfrak{p}_1,$$
so $\mathfrak{a}^{-1} = c^{-1} \cdot O_K$, which is clearly bigger than O_K since c is not a unit.

(2) $r > 1$: Since r was chosen to be minimal, we know that $(c) \not\supseteq \mathfrak{p}_2 \cdots \mathfrak{p}_r$, so we can choose a $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r \setminus (c)$. We'll show that $\frac{b}{c} \in \mathfrak{a}^{-1} \setminus O_K$.
First note that
$$(b)\mathfrak{a} \subset \mathfrak{p}_1 \cdots \mathfrak{p}_r \subset (c).$$
As $(c) = cO_K$, this shows that $\frac{b}{c}\mathfrak{a} \subset O_K$ and hence $\frac{b}{c} \in \mathfrak{a}^{-1}$ by definition. As $b \notin (c)$, we have $\frac{b}{c} \notin O_K$, which finishes the proof.

□

Proposition 4.52. *Let $\mathfrak{p}$ be any maximal ideal in O_K. Then $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}^{-1}\mathfrak{p} = O_K$.*

Proof. Clearly $\mathfrak{p}^{-1}\mathfrak{p} \subset O_K$ by definition of $\mathfrak{p}^{-1}$. Therefore $\mathfrak{p}^{-1}\mathfrak{p}$ is an (integral) ideal. On the other hand, since $O_K \subset \mathfrak{p}^{-1}$ by Remark 4.50 it follows that $\mathfrak{p} \subseteq \mathfrak{p}^{-1}\mathfrak{p}$. By maximality of $\mathfrak{p}$ we have either $\mathfrak{p}^{-1}\mathfrak{p} = O_K$ or $\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}$. If the latter is the case then we have $\mathfrak{p}^{-1} \subset O_K$ by Lemma 4.40, but this contradicts Lemma 4.51. □

We can now prove Theorem 4.20.

Proof. Suppose that the statement of the theorem is not true, and let $\mathfrak{a}$ be a maximal counterexample in the sense of Remark 4.38. Clearly $\mathfrak{a}$ is not a maximal ideal, and hence not prime. On the other hand $\mathfrak{a}$ is contained in some maximal ideal $\mathfrak{p}$. As $O_K \subset \mathfrak{p}^{-1}$ by Remark 4.50, we have
$$\mathfrak{a} \subset \mathfrak{p}^{-1}\mathfrak{a} \subset \mathfrak{p}^{-1}\mathfrak{p} = O_K.$$
Hence $\mathfrak{p}^{-1}\mathfrak{a}$ is an (integral) ideal containing $\mathfrak{a}$. Furthermore, $\mathfrak{p}^{-1}\mathfrak{a} \neq \mathfrak{a}$, since otherwise we would have $\mathfrak{p}^{-1} \subset O_K$ by Lemma 4.40. Since $\mathfrak{a}$ was chosen to be a maximal counterexample, it follows that $\mathfrak{p}^{-1}\mathfrak{a}$ can be factorized into prime ideals:
$$\mathfrak{p}^{-1}\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r.$$
Hence by Proposition 4.52, we have
$$\mathfrak{a} = \mathfrak{p}\mathfrak{p}_1 \cdots \mathfrak{p}_r,$$
which gives a contradiction. Hence every non-zero ideal can be factorised into a product of maximal ideals. It remains to show that the factorisation is unique. Suppose that
$$\mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s.$$

Clearly $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathfrak{q}_1$. Since $\mathfrak{q}_1$ is prime it follows that $\mathfrak{p}_i \subset \mathfrak{q}_1$ for some i. After reordering we may assume $i = 1$. By maximality of $\mathfrak{p}_1$ we have $\mathfrak{p}_1 = \mathfrak{q}_1$. Multiplying both sides by $\mathfrak{p}^{-1}$ we have

$$\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_2 \cdots \mathfrak{q}_s.$$

We can now proceed by induction. □

In view of Theorem 4.20, it is natural to make the following definition:

Definition 4.53. *Let $\mathfrak{a}, \mathfrak{b}$ be ideals of O_K. Then $\mathfrak{a}$ is a factor of $\mathfrak{b}$ (write $\mathfrak{a}|\mathfrak{b}$) if there is an ideal $\mathfrak{c}$ such that $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$.*

Corollary 4.54. *If $\mathfrak{a}, \mathfrak{b}$ are ideals in O_K, then $\mathfrak{a}|\mathfrak{b}$ if and only if $\mathfrak{a} \supseteq \mathfrak{b}$.*

Proof. If $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$, then it is clear that $\mathfrak{b} \subseteq \mathfrak{a}$. Conversely suppose that $\mathfrak{b} \subseteq \mathfrak{a}$. Then there is a fractional ideal $\mathfrak{c}$ such that $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$. Since $\mathfrak{a}\mathfrak{c} = \mathfrak{b} \subseteq \mathfrak{a}$ it follows from Lemma 4.40 that $\mathfrak{c} \subseteq O_K$, so $\mathfrak{c}$ is an ideal. □

We can summarize the properties of the fractional ideals as follows:

Proposition 4.55. *The non-zero fractional ideals of O_K form an abelian group under multiplication; the identity element is the trivial ideal O_K. We denote this group by $\mathcal{I}(K)$.*

In order to prove this proposition, we need the following lemma:

Lemma 4.56. *If $\mathfrak{a}$ is a non-zero ideal of O_K, we have $\mathfrak{a}\mathfrak{a}^{-1} = O_K$. Moreover, if $\mathfrak{a}$ factorises as*

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_n'$$

where the $\mathfrak{p}_i$ are maximal, then

$$\mathfrak{a}^{-1} = \mathfrak{p}_1^{-1} \cdots \mathfrak{p}_n^{-1}.$$

Proof. Suppose that there exists a non-zero ideal $\mathfrak{a}$ such that $\mathfrak{a}\mathfrak{a}^{-1} \neq O_K$. Assume that $\mathfrak{a}$ is a maximal counterexample. Let $\mathfrak{p}$ be a maximal ideal such that $\mathfrak{a} \subset \mathfrak{p}$. The

Lecture 15

$$\begin{aligned} & O_K \subset \mathfrak{p}^{-1} \subseteq \mathfrak{a}^{-1}, \\ \Rightarrow \quad & \mathfrak{a} \subseteq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{a}\mathfrak{a}^{-1} \subseteq O_K. \end{aligned}$$

In particular, the fact that $\mathfrak{a}\mathfrak{p}^{-1} \subseteq O_K$ inplies that $\mathfrak{a}\mathfrak{p}^{-1}$ is an ideal. Now we cannot have $\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}$ by Lemma 4.40 and Lemma 4.51. Hence $\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{p}^{-1}$, and the maximality condition on $\mathfrak{a}$ implies that

$$\mathfrak{a}\mathfrak{p}^{-1}(\mathfrak{a}\mathfrak{p}^{-1})^{-1} = O_K.$$

By the definition of $\mathfrak{a}^{-1}$, this means that

$$\mathfrak{p}^{-1}(\mathfrak{a}\mathfrak{p}^{-1})^{-1} \subseteq \mathfrak{a}^{-1},$$

so

$$O_K = \mathfrak{a}\mathfrak{p}^{-1}(\mathfrak{a}\mathfrak{p}^{-1})^{-1} \subseteq \mathfrak{a}\mathfrak{a}^{-1} \subseteq O_K,$$

from which the result follows.

Suppose now that $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_n'$. Multiplying both sides with $\mathfrak{a}^{-1}\mathfrak{p}_1^{-1} \cdots \mathfrak{p}_n^{-1}$ and using that

$$\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{p}_1\mathfrak{p}_1^{-1} = \cdots = \mathfrak{p}_n\mathfrak{p}_n^{-1} = O_K,$$

we deduce that

$$\mathfrak{a}^{-1} = \mathfrak{p}_1^{-1} \cdots \mathfrak{p}_n^{-1}.$$

□

We can now prove Proposition 4.55.

Proof. By Lemma 4.45, the product of two fractional ideals is a fractional ideal, and multiplication is clearly associative, with O_K being the identity element. Hence we just have to show that every element has an inverse. Note that by Lemma 4.56, every ideal has a multiplicative inverse.

Let $\mathfrak{a}$ be a fractional ideal. There is an $x \in O_K$ such that $(x)\mathfrak{a}$ is an ideal. By Theorem 4.20 we have $(x)\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ for some maximal ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$. We can also factorise (x) as

$$(x) = \mathfrak{q}_1 \cdots \mathfrak{q}_d$$

for some maximal ideals $\mathfrak{q}_j$. Using Proposition 4.52, we see that

$$\mathfrak{a} = \mathfrak{q}_1^{-1} \cdots \mathfrak{q}_s^{-1}\mathfrak{p}_1 \cdots \mathfrak{p}_r,$$

so if we put

$$\mathfrak{a}^{-1} = \mathfrak{q}_1 \cdots \mathfrak{q}_s \mathfrak{p}_1^{-1} \cdots \mathfrak{p}_r^{-1},$$

then $\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{a}^{-1}\mathfrak{a} = O_K$. (Note that the definition of $\mathfrak{a}^{-1}$ for a fractional ideal agrees reduces to the formula in Lemma 4.56 when $\mathfrak{a}$ is an ideal.) □

4.5. **The norm of ideals.** We now want to develop some algorithms for factorising ideals in practise. We start by learning how to calculate the norm of an ideal. Recall the definition: if $\mathfrak{a}$ is a non-zero ideal in O_K, define $N(\mathfrak{a}) = |O_K/\mathfrak{a}|$. We first collect some properties of the norm.

Lemma 4.57. *Let $\mathfrak{a}$ be a non-zero ideal in O_K. Then $N(\mathfrak{a}) \subset \mathfrak{a}$, i.e. $\mathfrak{a} | \langle N(\mathfrak{a}) \rangle$.*

Proof. Course work 4. □

As a corollary, we obtain the following result:

Proposition 4.58. *Let K be a number field. For any given positive integer n, there are only finitely many ideals in O_K of norm n.*

Proof. It follows from Lemma 4.57 that if $N(\mathfrak{a}) = n$, then $\langle n \rangle \subseteq \mathfrak{a}$, i.e. $\mathfrak{a} | \langle n \rangle$ by Corollary 4.54. Now $\langle n \rangle$ factorises as

$$\langle n \rangle = \mathfrak{p}_1 \cdots \mathfrak{p}_k,$$

so $\mathfrak{a}$ must factorise as the product of some of the $\mathfrak{p}_i$. □

Remark 4.59. *We will learn later how to determine all the ideals of a given norm. However, we first need to develop some tools for calculating the norm of an ideal.*

Proposition 4.60. *If $\mathfrak{a}, \mathfrak{b}$ are any two non-zero ideals in O_K, then*

$$N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b}).$$

Proof. Since $\mathfrak{b}$ may be factorized into maximal ideals, it is sufficient to prove this in the case when $\mathfrak{b}$ is maximal. We have an isomorphism of additive groups:

$$O_K/\mathfrak{a} \cong (O_K/\mathfrak{a}\mathfrak{b})/(\mathfrak{a}/\mathfrak{a}\mathfrak{b}).$$

Hence

$$N(\mathfrak{a}) = N(\mathfrak{a}\mathfrak{b})/|\mathfrak{a}/\mathfrak{a}\mathfrak{b}|.$$

It is therefore sufficient to show that

$$N(\mathfrak{b}) = |\mathfrak{a}/\mathfrak{a}\mathfrak{b}|.$$

Choose $\alpha \in \mathfrak{a} \setminus \mathfrak{a}\mathfrak{b}$ and consider the map

$$\Phi : O_K \to \mathfrak{a}/\mathfrak{a}\mathfrak{b}, \quad \Phi(x) = \alpha x + \mathfrak{a}\mathfrak{b}.$$

We claim that this map induces an isomorphism

$$O_K/\mathfrak{b} \cong \mathfrak{a}/\mathfrak{a}\mathfrak{b}.$$

Since $\mathfrak{b}$ is maximal, there are no ideals between $\mathfrak{a}$ and $\mathfrak{a}\mathfrak{b}$. Hence $\mathfrak{a}$ is generated by α and $\mathfrak{a}\mathfrak{b}$ and Φ is surjective. On the other hand if $x \in \mathfrak{b}$ then $\alpha x \in \mathfrak{a}\mathfrak{b}$, so $\Phi(x) = 0 + \mathfrak{a}\mathfrak{b}$. This shows that $\mathfrak{b} \subset \ker(\Phi)$. Since $\mathfrak{b}$ is maximal, the kernel is either $\mathfrak{b}$ or O_K. However $\Phi(1) = \alpha + \mathfrak{a}\mathfrak{b} \neq 0 + \mathfrak{a}\mathfrak{b}$, so $\ker(\Phi) = \mathfrak{b}$. It follows from the first isomorphism theorem that there is an isomorphism of additive groups

$$O_K/\mathfrak{b} \cong \mathfrak{a}/\mathfrak{a}\mathfrak{b}.$$

Hence $N(\mathfrak{b}) = |\mathfrak{a}/\mathfrak{a}\mathfrak{b}|$, which finishes the proof. □

Now recall the following theorem proved in another course:

Theorem 4.61. *Let H be a subgroup of $\mathbb{Z}^d$ such that $|\mathbb{Z}^d/H| < \infty$. Then there exist $c_1, \ldots, c_d \in \mathbb{Z}^d$ linearly independent such that*

$$H = \mathrm{Span}_{\mathbb{Z}}\{c_1, \ldots, c_d\}.$$

Furthermore $|\mathbb{Z}^d/H| = |\det(c_1, \ldots, c_d)|$.

Corollary 4.62. *Suppose that K is a number field of degree n. Let $\mathfrak{a}$ be a non-zero ideal in O_K. Then there exist $a_1, \ldots, a_n$ such that*

$$\mathfrak{a} = \mathrm{Span}_{\mathbb{Z}}(a_1, \ldots, a_n).$$

We call $a_1, \ldots, a_n$ a $\mathbb{Z}$-basis of $\mathfrak{a}$.

Warning 2. *A $\mathbb{Z}$-basis of an ideal is* not *the same as a set of generators!*

Example 4.63. Consider the ideal $\langle 2\rangle$ in $\mathbb{Z}[\sqrt{3}]$. Then 2, $2\sqrt{3}$ is a $\mathbb{Z}$-basis of $\langle 2\rangle$.

Example 4.64. Consider the ideal $\mathfrak{p} = \langle 2, 1-\sqrt{-17}\rangle$ in $\mathbb{Z}[\sqrt{-17}]$. By definition, the elements of $\mathfrak{p}$ are of the form $2(a+b\sqrt{-17}) + (1-\sqrt{-17})(c+d\sqrt{-17})$, where $a,b,c,d \in \mathbb{Z}$. Now

$$\begin{aligned} 2(a+b\sqrt{-17}) + (1-\sqrt{-17})(c+d\sqrt{-17}) &= (2a+c+17d) + (2b-c+d)\sqrt{-17}) \\ &= r + s\sqrt{-17}, \end{aligned}$$

where $r - s \in 2\mathbb{Z}$, so $r \equiv s \pmod 2$. Clearly r can be any integer, and s can be any integer of the same parity as r. It follows that

Lecture 16

$$\begin{aligned} \mathfrak{p} &= \{r + s\sqrt{-17} : r,s \in \mathbb{Z},\ r \equiv s \pmod 2\} \\ &= \{r + (r+2c)\sqrt{-17} : r,c \in \mathbb{Z}\} \\ &= \{r(1+\sqrt{-17}) + 2c\sqrt{-17} : r,c \in \mathbb{Z}\}, \end{aligned}$$

so $1+\sqrt{-17}, 2\sqrt{-17}$ is a $\mathbb{Z}$-basis of $\mathfrak{p}$.

Proposition 4.65. *Let $\mathfrak{a}$ be a non-zero ideal in O_K and let $a_n, \dots, a_n$ be a $\mathbb{Z}$-basis of $\mathfrak{a}$. Let $b_1, \dots, b_n$ be an integral basis of O_K. Let M be the change-of-basis matrix from $a_1, \dots, a_n$ to $b_1, \dots b_n$. Then*

$$N(\mathfrak{a}) = |\det(M)| = \sqrt{\frac{\Delta[a_1, \dots, a_n]}{\Delta[b_1, \dots, b_n]}}.$$

Proof. By Theorem 4.61, we have

$$N(\mathfrak{a}) = |O_K/\mathfrak{a}| = |\det M|.$$

On the other hand, we have $\Delta[a_1, \dots, a_n] = (\det M)^2 \Delta[b_1, \dots, b_n]$ by Corollary 2.32, which implies the result. □

Example 4.66. Let $\mathfrak{p}$ be as in the example above. What is $N(\mathfrak{p})$? We know that $1, \sqrt{-17}$ is an integral basis of $\mathbb{Z}[\sqrt{-17}]$. The base-change matrix from $1, \sqrt{-17}$ to $1+\sqrt{-17}, 2\sqrt{-17}$ is

$$M = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix},$$

so by Proposition 4.65, we have

$$N(\mathfrak{p}) = |\det(M)| = 2.$$

We can also see this directly: if $x \in O_K - \mathfrak{p}$, then $x = r + s\sqrt{-17}$, where $r \not\equiv s \pmod 2$, so $x + 1 \in \mathfrak{p}$. It follows that $O_K/\mathfrak{p}$ has two elements, i.e. $N(\mathfrak{p}) = 2$.

Proposition 4.65 has the following useful consequence:

Corollary 4.67. *For any non-zero element $a \in O_K$, we have $N(\langle a\rangle) = |N(a)|$.*

Proof. Course work 5. □

Example 4.68. Let $\sigma : K \hookrightarrow \mathbb{C}$ is an embedding, and suppose that $\sigma(K) = K$. Clearly σ restricts to a map $O_K \to O_K$ and maps ideals to ideals. It follows that if $\mathfrak{a}$ is an ideal then

$$N(\sigma\mathfrak{a}) = |O_K/\sigma\mathfrak{a}| = |(O_K/\sigma\mathfrak{a}| = |\sigma(O_K/\mathfrak{a})| = |O_k/\mathfrak{a}| = N(\mathfrak{a}).$$

For example, if $K = \mathbb{Q}(\sqrt{-3})$, then

$$N\big(\langle 2, 1+\sqrt{3}\rangle\big) = N\big(\langle 2, 1-\sqrt{3}\rangle\big).$$

Hence

$$\begin{aligned} N\big(\langle 2, 1+\sqrt{3}\rangle\big)^2 &= N\big(\langle 2, 1+\sqrt{3}\rangle\big) N\big(\langle 2, 1-\sqrt{3}\rangle\big) \\ &= N\big(\langle 2, 1+\sqrt{3}\rangle\langle 2, 1-\sqrt{3}\rangle\big) \\ &= N\big(\langle 4, 2+2\sqrt{3}, 2-2\sqrt{3}, -2\rangle\big) \\ &= N\big(\langle 2\rangle\big) \\ &= 4, \end{aligned}$$

and so $N\big(\langle 2, 1+\sqrt{3}\rangle\big) = 2$. We can often use this method to calculate norms.

4.6. **The norm of prime ideals.** Let K be a number field, and let $\mathfrak{a} \subset O_K$ be a non-zero ideal. Then we can factorise $\mathfrak{a}$ as a product of prime ideals,

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_n.$$

As the norm is multipliciative, we have

$$N(\mathfrak{a}) = N(\mathfrak{p}_1) \cdots N(\mathfrak{p}_n).$$

The aim of this chapter is to develop some tools for calculating the norm of prime ideals. We start with the following elementary observation:

Lemma 4.69. *Let $R \subset S$ be commutative rings with 1 and let $\mathfrak{p}$ be a prime ideal of S. Then $\mathfrak{p} \cap R$ is a prime ideal of R.*

Proof. Immediate from the definition. □

Definition 4.70. *Suppose now that $\mathfrak{p}$ is a non-zero prime ideal in O_K. The by Lemma 4.69, $\mathfrak{p} \cap \mathbb{Z}$ is a prime ideal in $\mathbb{Z}$, so it is of the form $\mathfrak{p} \cap \mathbb{Z} = (p)$ for some prime number p. We say that* $\mathfrak{p}$ lies above p.

Proposition 4.71. *If $\mathfrak{p}$ is prime, then $N(\mathfrak{p}) = p^f$ for some $1 \leq f \leq d = [K : \mathbb{Q}]$.*

Furthermore, there exist prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ of O_K such that

$$pO_K = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_r^{e_r}$$

with $N(\mathfrak{p}_i) = p^{f_i}$. Moreover, we have

$$d = \sum_{i=1}^{r} e_i f_i.$$

Proof. If $\mathfrak{p}$ lies above p then $p \in \mathfrak{p}$. Hence $\langle p \rangle \subseteq \mathfrak{p}$, i.e. $\mathfrak{p} | \langle p \rangle$, and it follows that $N(\mathfrak{p}) | N(\langle p \rangle) = p^d$. □

Definition 4.72. *In the notation of the proposition, the integer e_i is the ramification index of $\mathfrak{p}_i$, and f_i is the residue degree of $\mathfrak{p}_i$.*

(1) p is ramified in K if $e_i \geq 2$ for some i.
(2) p is totally ramified if there is a unique prime $\mathfrak{p}$ of O_K above p with ramification index $d = [K : \mathbb{Q}]$, i.e. $\langle p \rangle = \mathfrak{p}^d$.
(3) p is inert in K if $\langle p \rangle$ is a prime ideal of O_K.
(4) p splits completely in K if $\langle p \rangle$ is the product of d distinct prime ideals of O_K.

Lecture 17

Theorem 4.73. *(Dedekind's Criterion) Let K be a number field, and suppose that $O_K = \mathbb{Z}[\alpha]$ for some element α. Let $f(t) \in \mathbb{Z}[t]$ be the minimal polynomial of α over $\mathbb{Q}$. Let p be a prime number, and let $\bar{f} = f \pmod{p}$. Suppose that $\bar{f}(t)$ factorizes over $\mathbb{F}_p[t]$ as*

$$\bar{f} \equiv \bar{f}_1^{e_1} \cdots \bar{f}_r^{e_r},$$

with $\bar{f}_i(t) \in \mathbb{F}_p[t]$ monic and irreducible, and $\bar{f}_i \neq \bar{f}_j$ unless $i = j$. Let $f)_i(t) \in \mathbb{Z}[t]$ be a left of $\bar{f}_i(t)$. Then the ideal (p) in O_K factorizes as

$$\langle p \rangle = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}, \qquad \mathfrak{p}_i = \langle p, f_i(\alpha) \rangle.$$

Each ideal $\mathfrak{p}_i$ is maximal and has norm $p^{\deg \bar{f}_i}$. If $i \neq j$ then $\mathfrak{p}_i \neq \mathfrak{p}_j$.

Remark 4.74. *The condition $O_K = \mathbb{Z}[\alpha]$ is equivalent to saying that $\{1, \alpha, \ldots, \alpha^{d-1}\}$ is an integral basis. There is not always such an α, but often there is in the examples which we've seen.*

The theorem can be generalized as follows: if $K = \mathbb{Q}(\alpha)$ with α an algebraic integer, and p is a prime which does not divide $|O_K/\mathbb{Z}[\alpha]$, then the conclusion of the theorem holds.

Proof. First note that since $O_K = \mathbb{Z}[\alpha]$, we have an isomorphism

$$O_K \equiv \mathbb{Z}[t]/\langle f \rangle, \qquad \alpha \mapsto t + \langle f \rangle.$$

This implies that there is an isomorphism

$$O_K/\mathfrak{p}_i \equiv \mathbb{Z}[t]/\langle f, p, f_i \rangle \equiv \mathbb{F}_p[t]/\langle \bar{f}, \bar{f}_i \rangle \equiv \mathbb{F}_p[t]/\langle \bar{f}_i \rangle. \tag{11}$$

Since $\bar{f}_i$ is irreducible in $\mathbb{F}_p[t]$, it follows that $\langle \bar{f}_i \rangle$ is a maximal ideal in $\mathbb{F}_p[t]$. Hence $\mathbb{F}_p[t]/\langle \bar{f}_i \rangle$ is a field. On the other hand this implies that $O_K/\mathfrak{p}_i$ is a field, so $\mathfrak{p}_i$ is a maximal ideal of O_K.

The norm of $\mathfrak{p}_i$ is the number of elements of $\mathbb{F}_p[t]/(\bar{f}_i)$, which is equal to

$$p^{[\mathbb{F}_p[t]/\langle \bar{f}_i \rangle : \mathbb{F}_p]} = p^{\partial(\bar{f}_i)}$$

by Theorem 1.27. Next note that

$$\prod_{i=1}^{r} \mathfrak{p}_i^{e_i} \subseteq \left\langle p, \prod_{i=1}^{r} f_i(\alpha)^{e_i} \right\rangle.$$

On the other hand

$$\prod_{i=1}^{r} f_i(\alpha)^{e_i} \equiv f(\alpha) \equiv 0 \bmod p,$$

so we have

$$\prod_{i=1}^{r} \mathfrak{p}_i^{e_i} \subseteq \langle p \rangle.$$

To prove that we have equality here, it is sufficient to prove that both sides of the equation have the same norm. This is true since

$$\begin{aligned} N\left(\prod_{i=1}^{r} \mathfrak{p}_i^{e_i}\right) &= \prod_{i=1}^{r} N(\mathfrak{p}_i)^{e_i} \\ &= \prod_{i=1}^{r} p^{e_i \deg \bar{f}_i} \\ &= p^{\sum_{i=1}^{r} e_i \deg \bar{f}_i} \\ &= p^{\partial(\prod_{i=1}^{r} \bar{f}_i^{e_i})} \\ &= p^{\partial\langle f \rangle} \\ &= p^{[K:\mathbb{Q}]} \\ &= N(\langle p \rangle). \end{aligned}$$

It remains to show that the maximal ideals $\mathfrak{p}_i$ are distinct. Suppose that $\mathfrak{p}_i = \mathfrak{p}_j$. Then $O_K/\mathfrak{p}_i = O_k/\mathfrak{p}_j$, which by (11) is equivalent to

$$\mathbb{F}_p[t]/\langle \bar{f}_i \rangle \cong \mathbb{F}_p[t]/\langle \bar{f}_j \rangle.$$

In other words, them image of $\bar{f}_i(t)$ in $\mathbb{F}_p[t]/\langle \bar{f}_j \rangle$ is zero (and of course vice versa), i.e. $\bar{f}_j | \bar{f}_i$. As both $\bar{f}_i$ and $\bar{f}_j$ are monic and irreducible, this implies that $f_i = f_j$ and hence $i = j$. □

Corollary 4.75. *Let K be a number field (of degree d) with ring of integers $O_K = \mathbb{Z}[\theta]$, and assume that the minimal polynomial of θ is Eisenstein at p. Then p is totally ramified in K.*

Proof. Let $f(t)$ be the minimal polynomial of θ over $\mathbb{Q}$. Then $f(t) \equiv t^d \pmod p$, so we deduce from Theorem 4.73 that $\langle p \rangle = \mathfrak{p}^d$, where $\mathfrak{p} = \langle p, \theta \rangle$. □

Example 4.76. Let $K = \mathbb{Q}(\sqrt{6})$, so $O_K = \mathbb{Z}[\sqrt{6}]$. The minimal polynomial of $\sqrt{6}$ over $\mathbb{Q}$ is $f(t) = t^2 - 6$. Here are some values of f:

t	t^2-6
0	-6
± 1	-5
± 2	-2
± 3	3
± 4	10
± 5	19

From the table we see that $f(t)$ factorizes modulo small primes as

$$\begin{aligned} t^2 - 6 &\equiv t^2 \bmod 2 \\ &\equiv t^2 \bmod 3 \\ &\equiv (t+1)(t-1) \bmod 5 \\ &\equiv t^2 - 6 \bmod 7 \\ &\equiv t^2 - 6 \bmod 11. \end{aligned}$$

By Theorem 4.73, the small primes factorize in O_K as follows:

$$\begin{aligned} \langle 2 \rangle &= \mathfrak{p}_2^2, & \mathfrak{p}_2 &= \langle 2, \sqrt{6} \rangle, \\ \langle 3 \rangle &= \mathfrak{p}_3^2, & \mathfrak{p}_3 &= \langle 3, \sqrt{6} \rangle, \\ \langle 5 \rangle &= \mathfrak{p}_5 \mathfrak{p}_5', & \mathfrak{p}_5 &= \langle 5, \sqrt{6}+1 \rangle, \quad \mathfrak{p}_5' = \langle 5, \sqrt{6}-1 \rangle. \end{aligned}$$

On the other hand $\langle 7\rangle$ and $\langle 11\rangle$ are prime in O_K. The norms of the ideals are also given by the theorem:

$$N(\mathfrak{p}_2)=2,\quad N(\mathfrak{p}_3)=3,\quad N(\mathfrak{p}_5)=N(\mathfrak{p}_5')=5,\quad N(\langle 7\rangle)=49,\quad N(\langle 11\rangle)=121.$$

Example 4.77. Let $K=\mathbb{Q}(\sqrt[3]{2})$; we have already seen that then $O_K=\mathbb{Z}[\sqrt[3]{2}]$, so we can apply Theorem 4.73. The minimal polynomial of $\sqrt[3]{2}$ is $f(t)=t^3-2$. To factorize this modulo primes p, we make a table of values of f:

t	t^3-2
0	-2
1	-1
-1	-3
2	6
-2	-10
3	25
-3	-29

$$\begin{aligned} t^3-2 &\equiv t^3 \bmod 2\\ &\equiv (t+1)^3 \bmod 3\\ &\equiv (t+2)(t^2+3t+4) \bmod 5\\ &\equiv t^3-2 \bmod 7 \end{aligned}$$

$$\begin{array}{lll} \langle 2\rangle=\mathfrak{p}_2^3, & \mathfrak{p}_2=\langle 2,\sqrt[3]{2}\rangle, & N(\mathfrak{p}_2)=2\\ \langle 3\rangle=\mathfrak{p}_3^3, & \mathfrak{p}_2=\langle 3,\sqrt[3]{2}+1\rangle, & N(\mathfrak{p}_3)=3\\ \langle 5\rangle=\mathfrak{p}_5\mathfrak{p}_{25}, & \mathfrak{p}_5=\langle 5,\sqrt[3]{2}+2\rangle, & N(\mathfrak{p}_5)=5\\ & \mathfrak{p}_{25}=\left\langle 5,\sqrt[3]{2}^2+3\sqrt[3]{2}+4\right\rangle, & N(\mathfrak{p}_{25})=25,\\ \langle 7\rangle \text{ is maximal} & & N(\langle 7\rangle)=7^3. \end{array}$$

Lecture 18

4.7. **Factorisation of ideals.** We are now able to factorize an ideal $\mathfrak{a}$ of O_K into maximal ideals:

- Calculate $N(\mathfrak{a})$ and factorize it into primes.
- For each prime p dividing $N(\mathfrak{a})$, factorize $\langle p\rangle$ into maximal ideals of O_K;
- Write down all ideals whose norm is equal to the norm of $\mathfrak{a}$ (this is a finite list);
- To find out which factorization is correct, use the principle: $\mathfrak{p}|\mathfrak{a}$ if and only if the generators of $\mathfrak{a}$ are in $\mathfrak{p}$.

Example 4.78. Again let $K=\mathbb{Q}(\sqrt{6})$ as above. We factorize the ideal $\langle 12+7\sqrt{6}\rangle$. First note that

$$N(12+7\sqrt{6})=144-6\times 49=144-294=-150,$$

so Corollary 4.67 implies that

$$N\big(\langle 12+7\sqrt{6}\rangle\big)=150=2\times 3\times 5^2.$$

However we already calculated the maximal ideals above 2, 3 and 5, namely

$$\begin{array}{lll} \langle 2\rangle = \mathfrak{p}_2^2, & \mathfrak{p}_2=\langle 2,\sqrt{6}\rangle,\\ \langle 3\rangle = \mathfrak{p}_3^2, & \mathfrak{p}_3=\langle 3,\sqrt{6}\rangle,\\ \langle 5\rangle = \mathfrak{p}_5\mathfrak{p}_5', & \mathfrak{p}_5=\langle 5,\sqrt{6}+1\rangle, \quad \mathfrak{p}_5'=\langle 5,\sqrt{6}-1\rangle \end{array}$$

where

$$N(\mathfrak{p}_2)=2,\qquad N(\mathfrak{p}_3)=3,\qquad N(\mathfrak{p}_5)=N(\mathfrak{p}_5')=5.$$

Hence there are three ideals of norm 150:

$$\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5^2,\quad \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5\mathfrak{p}_5',\quad \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5'^2.$$

Since $\mathfrak{p}_5\mathfrak{p}_5'=\langle 5\rangle$ and $12+7\sqrt{6}$ is not a multiple of 5, is follows that $\langle 12+7\sqrt{6}\rangle\neq\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5\mathfrak{p}_5'$. We are left with two possibilities. Since $12+7\sqrt{6}=5+7(1+\sqrt{6})$, it follows that $12+7\sqrt{6}\in\mathfrak{p}_5$, and so $\mathfrak{p}_5|\langle 12+7\sqrt{5}\rangle$. Hence

$$\langle 12+7\sqrt{6}\rangle=\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5^2.$$

Example 4.79. Consider $K=\mathbb{Q}(\sqrt{3})$, so $O_K=\mathbb{Z}[\sqrt{3}]$. We want to factorise the ideals $\langle 3\rangle$ and $\langle 10\rangle$ into irreducibles. The minimal polynomial of $\sqrt{3}$ is $f(t)=t^2-3$, so

$$f(t)\equiv t^2 \pmod 3.$$

By Theorem 4.73, it follows that $\mathfrak{p}=\langle 3\rangle+\langle\sqrt{3}\rangle=\langle\sqrt{3}\rangle$ is prime in O_K, and

$$\langle 3\rangle=\langle\sqrt{3}\rangle^2.$$

Now $10 = 2 \cdot 5$, so $\langle 10\rangle = \langle 2\rangle\langle 5\rangle$. Let us decompose $\langle 2\rangle$ and $\langle 5\rangle$ into irreducibles. We have

$$f(t) \equiv t^2 + 1 = (t+1)^2 \pmod 2,$$

so if we let $g(t) = t + 1$, then Dedekind's criterion states that the ideal

$$\mathfrak{q} = \langle 2\rangle + \langle \sqrt{3} + 1\rangle$$

is prime in O_K. Now

$$\begin{aligned}\mathfrak{q} &= \{2x + (1+\sqrt{3})y : x, y \in O_K\} \\ &= \langle 2, 1+\sqrt{3}\rangle.\end{aligned}$$

We therefore deduce from Theorem 4.73 that

$$\langle 2\rangle = \mathfrak{q}^2 \quad \Rightarrow \quad N\big(\langle 2\rangle\big) = 4 = N(\mathfrak{q})^2,$$

so $N(\mathfrak{q}) = 2$. Finally, $f(t)$ is irreducible $\pmod 5$, so Dedekind's criterion implies that $\langle 5\rangle$ is a prime ideal in O_K. Hence

$$\langle 10\rangle = \langle 2\rangle\langle 5\rangle = \mathfrak{q}^2\langle 5\rangle.$$

We want to determine all ideals in $\mathbb{Z}[\sqrt{3}]$ which have norm 50. By Corollary 4.67, we have $N(\langle 5\rangle) = 25$. Suppose now that $N(\mathfrak{b}) = 50$. By Lemma 4.57, this implies that

$$\mathfrak{b} | \langle 50\rangle = \langle 2\rangle\langle 5\rangle^2 = \mathfrak{q}^2\langle 5\rangle^2,$$

so

$$\mathfrak{b} = \mathfrak{q}^r\langle 5\rangle^s$$

for some $r, s \in \{0, 1, 2\}$. Now

$$N(\mathfrak{b}) = N(\mathfrak{q})^r N\big(\langle 5\rangle\big)^s = 2^r 25^s,$$

so we deduce that $r = s = 1$, and the only ideal in $\mathbb{Z}[\sqrt{3}]$ of norm 50 is $\mathfrak{b} = \langle 2, 1+\sqrt{3}\rangle\langle 5\rangle$.

5. An extended example: ramification in quadratic fields

5.1. The Legendre symbol.

Definition 5.1. *Let $p \geq 3$ be a prime number, and let $a \in \mathbb{Z}$ be comprime to p. Then a is a quadratic residue* $\pmod p$ *if there exists $x \in \mathbb{Z}$ such that $x^2 \equiv a \pmod p$.*

Example 5.2.

- 3 is a quadratic residue $\pmod{13}$, since $4^2 = 16 \equiv 3 \pmod{13}$.
- 2 is not a quadratic residue $\pmod 3$.

Lemma 5.3. *Let $p \geq 3$ be a prime number, and let $a \in \mathbb{Z}$ be comprime to p. Then the following are equivalent:*

(1) a is a quadratic residue $\pmod p$
(2) $a^{\frac{p-1}{2}} \equiv 1 \pmod p$.

Proof. Suppose first that a is a quadratic residue $\pmod p$, so $x^2 = a \pmod p$ for some $x \in \mathbb{Z}$. Then Fermat's little theorem implies that $x^{p-1} = 1 \pmod p$, and hence

$$a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \equiv 1 \pmod p.$$

Conversely, assume that $a^{\frac{p-1}{2}} \equiv 1 \pmod p$. Now the group $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic, and let $g \in \mathbb{Z}$ be a generator, so $a \equiv g^r \pmod p$ for some $r \geq 0$. Then

$$(g^r)^{\frac{p-1}{2}} \equiv 1 \pmod p.$$

Since g has order $p-1$ in $(\mathbb{Z}/p\mathbb{Z})^\times$, we have $(p-1) | r\frac{p-1}{2}$, so $r/2$ is an integer, which implies that

$$a \equiv (g^{\frac{r}{2}})^2 \pmod p,$$

i.e. a is a quadratic residue. □

Definition 5.4. *Let p be a prime, and let $a \in \mathbb{Z}$. Define the* Legendre symbol

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } p \nmid a \text{ and } a \text{ is a quadratic residue} \pmod p \\ -1 & \text{if } p \nmid a \text{ and } a \text{ is not a quadratic residue} \pmod p \\ 0 & \text{if } p \mid a \end{cases}$$

Example 5.5. We have $\left(\frac{3}{13}\right) = 1$ and $\left(\frac{2}{3}\right) = -1$.

Lemma 5.6. *Let $p \geq 3$ be prime, and let $a, b \in \mathbb{Z}$.*

(1) (Euler's lemma) $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$*;*

(2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$*;*

(3) if $a \equiv b \pmod{p}$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

Proof. (i) By Fermat's little theorem, we have $a^{p-1} \equiv 1 \pmod{p}$, so p divides

$$a^{p-1} - 1 = \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right),$$

i.e. $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$. But by Lemma 5.3, a is a quadratic residue $\pmod{p}$ if and only if $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, which finishes the proof. Lecture 19

(ii) Since

$$(ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}},$$

part (i) implies that $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}$. But both sides are in $\{\pm 1\}$, so they must be equal.

(iii) Clear. □