Number Fields

June 2, 2024

Contents

Lectures

Start of

lecture 1

1 Introduction

If $L \supset K$ are fields, then L is an extension of K. Notation L/K. We can think of L as a vector space over K. The dimension of L/K is called the degree of the field extension, and is written as $[L : K]$.

Definition (Number field)**.** A *number field* is a subfield K of $\mathbb{C}$ with $[K : \mathbb{Q}] < \infty$.

Example.

(1) $\mathbb{Q}$.

(2) Let $\alpha \in \mathbb{C}$ be algebraic, i.e. a root of a polynomial with integer coefficients. Then $\mathbb{Q}(\alpha)$ (this notation means the smallest subfield of $\mathbb{C}$ containing α) is a number field. $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg f_\alpha$, where f_α is the unique monic minimal polynomial of α over $\mathbb{Q}$. By the Primitive Element Theorem (see Galois Theory), all number fields are of this form.

(3) Quadratic fields: K with $[K : \mathbb{Q}] = 2$. $K = \mathbb{Q}(\sqrt{m})$ where $m \in \mathbb{Z}$, $m \neq 0, \pm 1$ and square-free.

(4) Cyclotomic fields. Let $n \in \mathbb{Z}_{\geq 3}$. Let $\theta_n = e^{2\pi i/n}$. This is an n-th root of unity, i.e. $\theta_n^n = 1$. Then $K = \mathbb{Q}(\theta_n)$ is a number field, with $[\mathbb{Q}(\theta_n) : \mathbb{Q}] = \varphi(n)$, where $\varphi(n)$ is the number of residue classes modulo n that are coprime to n.

Why study Number Fields?

Consider Fermat equation:

$$x^n + y^n = z^n, \qquad x, y, z \in \mathbb{Z}.$$

Consider the $n = 2$ case. We are interseted in primitive solutions (solutions with $\gcd(x, y, z) = 1$). Furthermore we assume $x, y, z \geq 0$.

Assume $2 \nmid y$. Note that $(z - x)(z + x) = z^2 - x^2 = y^2$.

Claim: $\gcd(z - x, z + x) = 1$. Indeed let $p \mid z - x, z + x$. Then $p \mid 2z, 2x, y^2$. But $\gcd(2x, 2z, y^2) = 1$ (since we assumed $2 \nmid y$ and $\gcd(x, y, z) = 1$), so no such p exists.

y^2 has all prime factors with even multiplicities, and these factors must go to either $(z - x)$ or $(z + x)$ with the multiplicity they occur in y^2. Conclusion: $z - x = n^2$,

$z + x = m^2$ for some $0 \leq n \leq m \in \mathbb{Z}$ and coprime and odd. We now have:

$$x = \frac{m^2 - n^2}{2}, \qquad z = \frac{m^2 + n^2}{2}, \qquad y = mn$$

All solutions must be of this form. Easy to check that these are all solutions. More customary to write

$$x = 2mn, \qquad y = m^2 - n^2, \qquad z = m^2 + n^2,$$

$m > n$, $\gcd(m, n) = 1$, and exactly one of them is even.

Fermat claimed: No solutions for $n \geq 3$ and $x, y, z \in \mathbb{Z}_{>0}$. First step is to factorize the equation. For $n = 2$, we used $X^2 - 1 = (X-1)(X+1)$. For general n, we have $X^n - 1 = \prod_{j=0}^{n-1}(X - \theta_n^j)$. Assume n is odd, then consider $X \to -X$: $X^n + 1 = \prod_{j=0}^{n-1}(X + \theta_n^j)$. Now substitute $X \leftarrow \frac{x}{y}$ to get

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

Next step: show that $(x + y\theta_n^j)$ is an n-th power.

Issues:

- Unique factorisation may fail. In fact, $\mathbb{Z}[\theta_n]$ is not a UFD for any prime $n \geq 23$.
- Even if it is a UFD, if α has all prime factors with multiplicity divisible by n, we can conclude only that $\alpha = u\beta^n$ for some $\beta \in \mathbb{Z}[\theta_n]$ and some unit $u \in \mathbb{Z}[\theta_n]^\times$ (reminder: $u \in R$ is a unit if there exists $u^{-1} \in R$ such that $uu^{-1} = 1$, and $R^\times$ denotes the set of units in R).

Theorem (Kummer 1850)**.** If p is a regular prime (not defined here), then

$$x^p + y^p = z^p$$

has no solutions with $x, y, z \in \mathbb{Z}_{\geq 1}$.

Aims of the course:

- Ring of integers in number fields
- Unique factorisation of ideals
- Units
- Fermat equation: prove Kummer's Theorem in the case $p \nmid xyz$

Start of

lecture 2

1.1 Ring of integers

Let $\alpha \in \mathbb{C}$ be algebraic. Then there is a unique monic irreducible polynomial $f \in \mathbb{Q}[X]$ of minimal degree such that $f(\alpha) = 0$. This is called the minimal polynomial.

Definition (Algebraic Integer)**.** $\alpha \in \mathbb{C}$ is an algebraic integer if it has minimal polynomial $f_\alpha \in \mathbb{Z}[X]$.

Remark. If α is a root of a monic polynomial $f \in \mathbb{Z}[X]$, then α is an algebraic integer. Indeed, then we can write $f = f_\alpha \cdot h$ with f_α the minimal polynomial of α, and $h \in \mathbb{Q}[X]$ monic. By Gauss's Lemma (see GRM), both $f_\alpha, h \in \mathbb{Z}[X]$.

Theorem. Algebraic integers form a ring.

Notation. The ring of algebraic integers is denoted by $\mathcal{O}$. If K is a number field, then $\mathcal{O}_K = \mathcal{O} \cap K$.

Example. If $K = \mathbb{Q}$, $\mathcal{O}_K = \mathbb{Z}$. Let $\frac{a}{b} \in \mathbb{Q}$. $f_\alpha = x - \frac{a}{b}$. So $\frac{a}{b} \in \mathcal{O}_K \iff \frac{a}{b} \in \mathbb{Z}$.

Example. Quadratic fields: Let $K = \mathbb{Q}(\sqrt{m})$, where $m \neq 0, 1 \in \mathbb{Z}$ is square-free. Then

$$\mathcal{O}_K = \begin{cases} a + b\sqrt{m} & a, b \in \mathbb{Z} \text{ if } m \equiv 2, 3 \pmod 4 \\ a + b\left(\frac{1+\sqrt{m}}{2}\right) & a, b \in \mathbb{Z} \text{ if } m \equiv 1 \pmod 4 \end{cases}$$

All elements of K are of the form $\alpha = a + b\sqrt{m}$ with $a, b \in \mathbb{Q}$. $\alpha \in \mathcal{O}_K \iff 2a \in \mathbb{Z}, a^2 - b^2 m \in \mathbb{Z}$.

$$f_\alpha = (x - (a + b\sqrt{m}))(x - (a - b\sqrt{m})) = x^2 - 2ax + a^2 - b^2 m.$$

Example. $n \in \mathbb{Z}_{\geq 3}$. $K = \mathbb{Q}(\underbrace{e^{2\pi i/n}}_{\theta_n})$. $\mathcal{O}_K = \mathbb{Z}[\theta_n] = \mathbb{Z} \oplus \theta_n\mathbb{Z} \oplus \cdots \oplus \theta_n^{\varphi(n)-1}\mathbb{Z}$.

Here, the direct sum notation ($\oplus$) means that each element of the ring $\mathcal{O}_K$ can be decomposed in a unique way, as opposed to if we used sum notation ($+$), where we would just assert that every element can be written in some way (but possibly multiple).

Why not work with $\mathbb{Z}[\alpha] \subset \mathbb{Q}[\alpha]$? Only $\mathcal{O}_K$ works.

Proposition. Let $\alpha \in \mathbb{C}$. Then the following are equivalent:

(i) $\alpha \in \mathcal{O}$.

(ii) $\mathbb{Z}[\alpha]$ is a finitely generated $\mathbb{Z}$-module, that is

$$\mathbb{Z}[\alpha] = \beta_1\mathbb{Z} + \beta_2\mathbb{Z} + \cdots + \beta_n\mathbb{Z}$$

for some $\beta_1, \ldots, \beta_n \in \mathbb{Z}[\alpha]$.

(iii) There is a finitely generated $\mathbb{Z}$-module $M \subset \mathbb{C}$ such that $\alpha M \subset M$.

Proof.

(1) $\implies$ (2) We show that

$$\mathbb{Z}[\alpha] = \underbrace{\mathbb{Z} + \alpha\mathbb{Z} + \cdots + \mathbb{Z}\alpha^{d-1}\mathbb{Z}}_{M}$$

where $d = \deg f_\alpha$. Enough to show that $\alpha^k \in M$ for all $n \in \mathbb{Z}_{\geq 0}$. Observe that for $n \geq d$:

$$\alpha^n = \underbrace{(\alpha^d - f_\alpha(\alpha))\alpha^{n-d}}_{\in \alpha^{n-1}\mathbb{Z} + \cdots + \mathbb{Z}}.$$

Using this and induction, the claim follows.

(2) $\implies$ (3) Trivial.

(3) $\implies$ (1) Let $M = \beta_1\mathbb{Z} + \cdots + \beta_k\mathbb{Z}$ be finitely generated, and suppose $\alpha M \subset M$. We exhibit a monic polynomial $f \in \mathbb{Z}[X]$ such that $f(\alpha) = 0$. There are $m_{ij} \in \mathbb{Z}$ such that

$$\alpha\beta_i = m_{i1}\beta_1 + \cdots + m_{in}\beta_n \qquad \forall i = 1, \ldots, n$$

Let A be the matrix with entries m_{ii}. Then

$$A \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} = \begin{pmatrix} \alpha\beta_1 \\ \vdots \\ \alpha\beta_n \end{pmatrix}$$

α is an eigenvalue of A. Then $f = \det(xI - A) \in \mathbb{Z}[X]$ is monic, and has the property that $f(\alpha) = 0$.

$\square$

Proof that algebraic integers form a ring. Let $\alpha, \beta \in \mathcal{O}$. We want to show that $\alpha - \beta$ and $\alpha\beta \in \mathcal{O}$. Let $M = \mathbb{Z}[\alpha, \beta]$. Clearly $(\alpha - \beta)M \subset M$ and $(\alpha\beta)M \subset M$. We show that M is a finitely generated $\mathbb{Z}$-module. Specifically

$$M = \sum_{i=1}^{n} \sum_{j=1}^{m} \alpha_i \beta_j \mathbb{Z},$$

where $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m$ are generators for $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ respectively. $\alpha, \beta \in M$, and M is a ring. $\square$

Additive structure of $\mathcal{O}_k$

Theorem. Let K be a number field. Then $\exists \beta_1, \dots, \beta_d \in \mathcal{O}_K$ such that

$$\mathcal{O}_K = \beta_1\mathbb{Z} \oplus \cdots \oplus \beta_d\mathbb{Z}$$

with $d = [K : \mathbb{Q}]$.

Definition. Such a tuple of β's is called an integral basis.

Suppose that we know that $\mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-module. By the structure theorem,

$$\mathcal{O}_K \cong \mathbb{Z}^r \oplus \cancel{\mathbb{Z}/m_1\mathbb{Z}} \oplus \cdots \oplus \cancel{\mathbb{Z}/m_s\mathbb{Z}}$$

Start of lecture 3

Let K be a number field, $\mathcal{O}_K$ the ring of integers. Let $[K : \mathbb{Q}] = d$.

Aim: $\exists$ an integral basis, that is $\alpha_1, \dots, \alpha_d \in \mathcal{O}_K$ such that

$$\mathcal{O}_K = \alpha_1\mathbb{Z} \oplus \cdots \oplus \alpha_d\mathbb{Z}$$

If $M \subset K$ is a finitely generated $\mathbb{Z}$-module, then

$$M = \alpha_1\mathbb{Z} \oplus \cdots \oplus \alpha_r\mathbb{Z}$$

Observe $r = \dim_{\mathbb{Q}} \operatorname{span}_{\mathbb{Q}}(M)$:

- $\alpha_1, \ldots, \alpha_r$ is linearly independent over $\mathbb{Q}$.
- $\operatorname{span}_{\mathbb{Q}}(M) = \operatorname{span}_{\mathbb{Q}}(\alpha_1, \ldots, \alpha_r)$.

Observe $\operatorname{span}_{\mathbb{Q}} \mathcal{O}_K = K$:

- If $\alpha \in K$, then $a\alpha \in \mathcal{O}_K$ for suitable a.

Discriminant of tuple

Recall Norm and Trace (from Galois Theory). Let L/K be a finite extension of fields. For $\alpha \in L$, we can associate $m_\alpha : x \mapsto \alpha x$ on L considered a vector space over K. The norm is $N_{L/K}(\alpha) = \det(m_\alpha) \in K$. The trace if $\operatorname{Tr}_{L/K}(\alpha) = \operatorname{Tr}(m_\alpha) \in K$. Recall the following properties:

- If $\alpha \in K$, $\operatorname{Tr}_{L/K}(\alpha) = [L : K]\alpha$, $N_{L/K}(\alpha) = \alpha^{[L:K]}$.
- $\alpha, \beta \in L$: $\operatorname{Tr}_{L/K}(\alpha + \beta) = \operatorname{Tr}_{L/K}(\alpha) + \operatorname{Tr}_{L/K}(\beta)$, $N_{L/K}(\alpha\beta) = N_{L/K}(\alpha)N_{L/K}(\beta)$.
- Let $M/L/K$: $\operatorname{Tr}_{M/K}(\alpha) = \operatorname{Tr}_{L/K}(\operatorname{Tr}_{M/L}(\alpha))$, similarly with norms.

Fix K. Let $d = [K : \mathbb{Q}]$. Then there exists d distinct embeddings $\sigma_1, \ldots, \sigma_d : K \to \mathbb{C}$ (if $K = \mathbb{Q}(\alpha)$, and f is the minimal polynomial of α, then $\sigma_1(\alpha), \ldots, \sigma_d(\alpha)$ are the roots of f).

We have:

$$N_{K/\mathbb{Q}}(\alpha) = \sigma_1(\alpha) \cdots \sigma_d(\alpha)$$
$$\operatorname{Tr}_{K/\mathbb{Q}}(\alpha) = \sigma_1(\alpha) + \cdots + \sigma_d(\alpha)$$

If $\alpha \in \mathcal{O}_K$, then $N_{K/\mathbb{Q}}(\alpha), \operatorname{Tr}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$. If α is such that $K = \mathbb{Q}(\alpha)$, and

$$f(X) = X^d + a_{d-1}x^{d-1} + \cdots + a_0$$

is its minimal polynomial, then

$$N_{K/\mathbb{Q}}(\alpha) = (-1)^d a_0, \qquad \operatorname{Tr}_{K/\mathbb{Q}}(\alpha) = -a_{d-1}.$$

Fix K. Write $N = N_{K/\mathbb{Q}}$, $\operatorname{Tr} = \operatorname{Tr}_{K/\mathbb{Q}}$.

Definition (Discriminant)**.** Let $\sigma_1, \dots, \sigma_d$ be the embeddings $K \to \mathbb{C}$. Let $\alpha_1, \dots, \alpha_d \in K$. Then we write

$$\operatorname{disc}(\alpha_1, \dots, \alpha_d) = \det(\sigma_i(\alpha_j)).$$

Note that $\det(\sigma_i(\alpha_j))$ denotes the determinant of the matrix whose ij-th entry is $\sigma_i(\alpha_j)$.

Example.

$$\operatorname{disc}(1, \alpha, \alpha^2, \dots, \alpha^{d-1}) = \prod_{1 \le i < j \le d} (\sigma_i(\alpha) - \sigma_j(\alpha))^2$$

If $K = \mathbb{Q}(\alpha)$ and f is the minimal polynomial, then this equals

$$(-1)^{\frac{d(d-1)}{2}} N(f'(\alpha)).$$

Note.

$$\mathbb{Z}[\alpha] = \mathbb{Z} + \alpha\mathbb{Z} + \cdots + \alpha^{d-1}\mathbb{Z}$$

for $\alpha \in \mathcal{O}_K$.

Lemma.

$$\operatorname{disc}(\alpha_1, \dots, \alpha_d) = \det(\operatorname{Tr}(\alpha_i\alpha_j))$$

Proof. Write $[x_{ij}]_{ij}$ for the $d \times d$ matrix with entries x_{ij}. Note

$$[\sigma_j(\alpha_i)]_{ij}[\sigma_j(\alpha_k)]_{jk} = \left[\sum_{j=1}^{d} \sigma_i(\alpha_i\alpha_j)\right] = [\operatorname{Tr}(\alpha_i\alpha_k)]_{ik}$$

Determinants are multiplicative and invariant under transpose. □

Lemma.

$$\operatorname{disc}(\alpha_1, \dots, \alpha_d) = 0 \iff \alpha_1, \dots, \alpha_d \text{ are linearly dependent over } \mathbb{Q}$$

Proof. If $\alpha_1, \dots, \alpha_d$ are linearly dependent, then the rows of $[\operatorname{Tr}(\alpha_i\alpha_j)]$ are also linearly dependent. Then $\det = 0$, so $\operatorname{disc} = 0$.

For the converse, suppose for the contrary that $\alpha_1, \dots, \alpha_d$ are linearly independent over $\mathbb{Q}$, and for sake of contradiction, assume disc $= 0$, so $\mathrm{disc}(\mathrm{Tr}(\alpha_i \alpha_j)) = 0$. Then there exists some $a_1, \dots, a_d$ not all 0 such that

$$\sum_{i=1}^{d} a_i \,\mathrm{Tr}(\alpha_i \alpha_j) = 0 \;\forall j$$

This is equivalent to (by additivity of Tr):

$$\mathrm{Tr}\left(\left(\sum_i a_i \alpha_i\right) \alpha_j\right) = 0 \;\forall j$$

By linear independence of $\alpha_1, \dots, \alpha_d$,

- $\sum_i a_i \alpha_i \neq 0$.
- $\exists b_1, \dots, b_d$ such that $\beta^{-1} = \sum_j b_j \alpha_j$.

Then

$$\sum_j b_j \,\mathrm{Tr}(\beta \cdot \alpha_j) = 0$$

hence

$$\mathrm{Tr}(\beta \cdot \beta^{-1}) = \mathrm{Tr}(1) = 0$$

which is a contradiction, since $\mathrm{Tr}(1) = d \neq 0$. □

Corollary. $\alpha_1, \dots, \alpha_d$ are linearly independent over $\mathbb{Q}$ if and only if the complex vectors $(\sigma_1(\alpha_j), \dots, \sigma_d(\alpha_j))^\top \in \mathbb{C}^d$ for $j = 1, \dots, d$ are linearly independent over $\mathbb{C}$.

Start of

lecture 4

Definition. Let K be a number field. Recall that we have d embeddings $\sigma_1, \dots, \sigma_d : K \to \mathbb{C}$, where $d = [K : \mathbb{Q}]$. We write r for the number of σ_j such that $\sigma_j(K) \subset \mathbb{R}$. Furthermore, we order the σ_i such that $\sigma_1, \dots, \sigma_r$ are precisely the real embeddings.

Write $s = \frac{d-r}{2}$. There are s pairs of complex conjugate embeddings. Denote them by $\tau_1, \overline{\tau_1}, \dots, \tau_s, \overline{\tau_s}$ (relabelling of $\sigma_{r+1}, \dots, \sigma_d$).

Define $\Sigma : K \to \mathbb{R}^d$ by

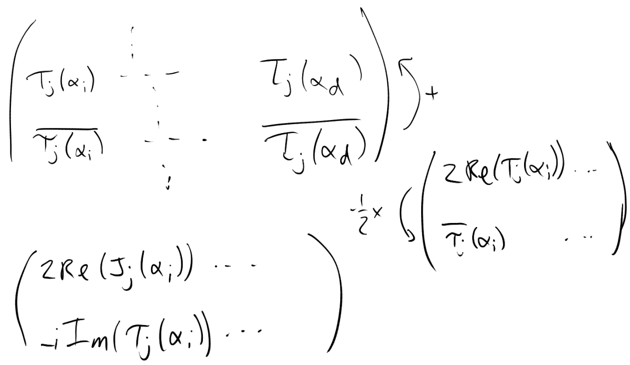
$$\Sigma(\alpha) = \begin{pmatrix} \sigma_1(\alpha) \\ \vdots \\ \sigma_r(\alpha) \\ \mathrm{Re}(\tau_1(\alpha)) \\ \mathrm{Im}(\tau_1(\alpha)) \\ \vdots \\ \mathrm{Re}(\tau_s(\alpha)) \\ \mathrm{Im}(\tau_s(\alpha)) \end{pmatrix}$$

This is $\mathbb{Q}$-linear.

Lemma. Let $\alpha_1, \dots, \alpha_d \in K$. Then

$$\mathrm{disc}(\alpha_1, \dots, \alpha_d) = (-4)^s \det(\Sigma(\alpha_1), \dots, \Sigma(\alpha_d))^2$$

Proof. The matrix $[\sigma_i(\alpha_j)]_{ij}$ has the following rows somewhere:



$\det(\sigma_i(\alpha_j)) = \pm(-2i)^s \det(\Sigma(\alpha_1), \dots, \Sigma(\alpha_d)))$. Squaring this we get the claim. □

Definition (Lattice)**.** A *lattice* in $\mathbb{R}^d$ is an additive subgroup of the form

$$\Lambda = v_1\mathbb{Z} \oplus \cdots \oplus v_d\mathbb{Z}$$

where $v_1, \dots, v_d \in \mathbb{R}^d$.

Definition (Fundamental domain)**.** A *fundamental domain* is a *Borel* set which contains exactly one point from each coset of some lattice Λ.

See Probability & Measure for a definition of Borel sets. The rough idea is that Borel sets are the sets for which we have a well-defined notion of volume.

Example. Fundamental parallelepiped:

$$[0,1) \cdot v_1 + \cdots + [0,1) \cdot v_d$$

Lemma. All fundamental domain have the same volume.

Proof. Out of the scope of this course (but should be fairly simple if you have studied Probability & Measure). □

Notation. We use $\mathrm{coVol}(\Lambda)$ to denote the volume of any fundamental domain of Λ (this is well-defined by the above lemma).

Observe:

$$\mathrm{Vol}([0,1)v_1 + \cdots + [0,1)v_d) = |\det(v_1, \dots, v_d)|$$

$$\mathrm{disc}(\alpha_1, \dots, \alpha_d) = (-4)^s \,\mathrm{coVol}(\Sigma(\alpha_1\mathbb{Z} + \cdots + \Sigma(\alpha_d)\mathbb{Z})^2.$$

Definition (Discriminant of a module)**.** The *discriminant* of a module of rank d is the discriminant of any basis of it (this is well-defined by part (3) of the following proposition).

Proposition. Let $\alpha_1, \dots, \alpha_d, \beta_1, \dots, \beta_d \in K$ which are linearly independent over $\mathbb{Q}$. Let $A \in \mathbb{Q}^{d \times d}$ such that

$$(\beta_1, \dots, \beta_d)^\top = A(\alpha_1, \dots, \alpha_d)^\top.$$

(1) Then
$$\operatorname{disc}(\beta_1, \dots, \beta_d) = \det(A)^2 \operatorname{disc}(\alpha_1, \dots, \alpha_d).$$

(2) If $\beta_1, \dots, \beta_d \in \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_d$, then

$$|\operatorname{disc}(\beta_1, \dots, \beta_d)| \geq |\operatorname{disc}(\alpha_1, \dots, \alpha_d)|.$$

(3) If the α's and β's generate the same module, then the discriminants are the same.

Proof.
$$[\sigma_j(\beta_i)]_{ij} = A[\sigma_j(\alpha_i)]$$

First claim (1) follows by the definition of discriminant and the properties of det.

For (2), there exists $A \in \mathbb{Z}^{d \times d}$ such that $(\beta_1, \dots, \beta_d)^\top = A(\alpha_1, \dots, \alpha_d)^\top$, and $|\det(A)| \geq 1$ since $\det(A) \neq 0$.

For (3), we already have $\geq$ by (2). For $\leq$, we can exchange the α's and β's. □

Proposition. Let $M_1 \subset M_2$ be two modules of rank d in K. Then

$$\operatorname{disc}(M_1) = |M_2/M_1|^2 \operatorname{disc}(M_2)$$

Recall from GRM:

Theorem. Let $M_1 \subset M_2$ be two free $\mathbb{Z}$-modules of rank d. Then M_2 has a basis $\alpha_1, \dots, \alpha_d$ and there are $\alpha_1, \dots, \alpha_d \in \mathbb{Z}$ such that $\alpha_1 \mid \alpha_2 \mid \cdots \mid \alpha_d$ and $a_1\alpha_1, \dots, a_d\alpha_d$ is a basis for M.

Start of lecture 5

Theorem. Let K be a number field. Then $\alpha_1, \dots, \alpha_d \in \mathcal{O}_K$ is integral basis if and only if $|\operatorname{disc}(\alpha_1, \dots, \alpha_d)|$ is minimal among all $\mathbb{Q}$-linear indepdendent tuples.

Proof. Let $\alpha_1, \dots, \alpha_d$ be such a tuple. Let $\beta \in \mathcal{O}_K$. We need to prove that $\beta \in M = \alpha_1\mathbb{Z} + \dots + \alpha_d\mathbb{Z}$. Then

$$\operatorname{disc}(M + \beta\mathbb{Z}) = |M + \beta\mathbb{Z}/M|^{-2} \operatorname{disc}(M) \implies |M + \beta\mathbb{Z}/M| = 1,$$

so $\beta \in M$. □

Definition (Discriminant of a number field)**.** The *discriminant* of a number field is the discriminant of any integral basis.

Example. Quadratic fields: $K = \mathbb{Q}(\sqrt{m})$, m square-free, $m \neq 0$. Two cases:

(1) $m \equiv 2, 2 \pmod 4$: $\mathcal{O}_K = \mathbb{Z} + \sqrt{m}\mathbb{Z}$,

$$\operatorname{disc}(K) = \begin{vmatrix} 1 & \sqrt{m} \\ 1 & -\sqrt{m} \end{vmatrix}^2 = 4m$$

(2) $m \equiv 1 \pmod 4$: $\mathcal{O}_K = \mathbb{Z} + \frac{1+\sqrt{m}}{2}\mathbb{Z}$,

$$\operatorname{disc}(K) = \begin{vmatrix} 1 & \frac{1+\sqrt{m}}{2} \\ 1 & \frac{1-\sqrt{m}}{2} \end{vmatrix}^2 = m$$

Proposition. Let $\alpha_1, \dots, \alpha_d \in \mathcal{O}_K$ be $\mathbb{Q}$-linearly independent. Then $\exists q \in \mathbb{Z}_{\geq 0}$ such that $q^2 \operatorname{disc}(\alpha_1, \dots, \alpha_d)$ and all $\beta \in \mathcal{O}_K$ can be written as

$$\beta = \frac{a_1\alpha_1 + \dots + a_d\alpha_d}{q}$$

with $a_1, \dots, a_d \in \mathbb{Z}$.

Proof. Set

$$q = \left(\frac{\operatorname{disc}(\alpha_1, \dots, \alpha_d)}{\operatorname{disc}(K)}\right)^{1/2}$$

Then

$$|\underbrace{\mathcal{O}_K/\alpha_1\mathbb{Z} \oplus \dots \oplus \alpha_d\mathbb{Z}}_{=M}| = q$$

$\beta \in \mathcal{O}_K$, $q\beta = 0$ in M, so $q\beta \in \alpha_1\mathbb{Z} \oplus \dots \oplus \alpha_d\mathbb{Z}$. □

Unique factorisation of ideals

Consider $K = \mathbb{Q}(\sqrt{-5})$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. We have

$$2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

In order to have unique factorisation, would have to have these elements split into smaller element. Say $2 = \pi_1\pi_2$. $N(2) = 4$, $N(1+\sqrt{-5}) = 1+5 = 6$. We would need $N(\pi_1) = \pm 2$. No such π_1, π_2.

Definition (Ideal)**.** A set $I \subset \mathcal{O}_K$ is an ideal if

$$\alpha, \beta \in I \implies \alpha + \beta \in I$$
$$\alpha \in I, \beta \in \mathcal{O}_K \implies \alpha\beta \in I$$

Example. The principal ideal generated by $\beta \in \mathcal{O}_K$ is

$$\{\beta \cdot \alpha : \alpha \in \mathcal{O}_K\} = \beta\mathcal{O}_K = \langle\beta\rangle = \langle\beta\rangle_{\mathcal{O}_K}$$

Observe that $\langle\beta\rangle = \langle\alpha\rangle$ if and only if $\beta = u\alpha$ for some unit $u \in \mathcal{O}_K^\times$.

Definition (Product of ideals)**.** Let $I, J \subset \mathcal{O}_K$ be two ideals. We define

$$IJ = \{\alpha_1\beta_1 + \cdots + \alpha_k\beta_k : \alpha_1, \ldots, \alpha_k \in I, \beta_1, \ldots, \beta_k \in J\}.$$

Remark.

- The set of ideals with this multiplication is a semi-group.
- $\alpha \mapsto \langle\alpha\rangle$ is a homomorphism.

Definition (Prime ideal)**.** An ideal $P \subsetneq \mathcal{O}_K$ is a prime ideal if the following holds: whenever $\alpha\beta \in P$ for some $\alpha, \beta \in \mathcal{O}_K$, then at least one of α, β is in P.

Fact: This is equivalent to $\mathcal{O}_K/P$ being an integral domain (recall that an integral domain is a commutative, unital ring without 0-divisors).

Fact: $\langle a\rangle$ is a prime ideal $\iff$ α is a prime in $\mathcal{O}_K$.

Theorem. Let K be a number field. Then all non-zero ideals in $\mathcal{O}_K$ are a product of non-zero prime ideals, and this factorisation is unique up to the order of the factors.

Remark. Addition on ideals can be defined as

$$I + J = \{\alpha + \beta : \alpha \in I, \beta \in J\}$$

But this does not make the set of ideals a ring. Also, $\langle \alpha \rangle + \langle \beta \rangle \neq \langle \alpha + \beta \rangle$ in general.

Lemma.

(1) All ideals in $\mathcal{O}_K$ are finitely generated. That is, they are of the form $\beta_1 \mathcal{O}_K + \cdots + \beta_k \mathcal{O}_K$ for some $\beta_1, \ldots, \beta_k \in \mathcal{O}_K$.

(2) If $I_1 \subset I_2 \subset I_3 \subset \cdots$ is a chain of ideals, then there exists k such that $I_k = I_{k+1} = I_{k+2} = \cdots$.

(3) Any collection of ideals contains a maximal one with respect to $\subset$.

This is called Noetherian property.

Proof.

(1) $I \subset \mathcal{O}_K$ is finitely generated as a $\mathbb{Z}$-module, which is even stronger than (1).

(2) $I = \bigcup_{i=1}^{\infty} I_j$ is an ideal, so $I = \beta_1 \mathcal{O}_K + \cdots + \beta_k \mathcal{O}_K$. Then there exists m such that $\beta_1, \ldots, \beta_k \in I_m$. Then $I = I_m = I_{m+1} = \cdots$.

(3) Suppose not. Then there is an infinite chain of ideals

$$I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots$$

contradicting (2). □

Start of lecture 6

Remarks:

- $\mathcal{O}_K$ is not a prime ideal.
- $\{0\}$ is not an integral domain (note that $\{0\}$ is a ring, with $1 = 0$).

- $\langle 0 \rangle \subset R$ is a prime ideal if and only if R is an integral domain.

- **$I \subset \mathcal{O}_K$ is a prime if it is a non-zero prime ideal.**

Definition (Maximal ideal)**.** An ideal $I \subsetneq \mathcal{O}_K$ is maximal if the only ideals J with $I \subset J \subset \mathcal{O}_K$ are I and $\mathcal{O}_K$.

Fact: I is maximal if and only if $\mathcal{O}_K/I$ is a field.

Lemma. In $\mathcal{O}_K$, primes and maximal ideals are the same.

Proof. First we prove that $\mathcal{O}_K/I$ is finite for all non-zero ideals. Enough to show that the rank of I is $d = [K : \mathbb{Q}]$ as a $\mathbb{Z}$-module. Take an integral basis $\alpha_1, \ldots, \alpha_d \in \mathcal{O}_K$. Let $0 \neq \beta \in I$. Then $\beta\alpha_1, \ldots, \beta\alpha_d \in I$ is linearly independent over $\mathbb{Q}$. Then $\mathrm{rank}(I) = d$. Now the lemma follows by the fact that finite integral domains are fields. Hint: Show that $\mathcal{O}_K/I$ is equal to its field of fractions. □

Lemma. Let $\alpha \in K$. Suppose that there is a finitely generated $\mathcal{O}_K$-module $M \subset K$ such that $\alpha M \subset M$. Then $\alpha \in \mathcal{O}_K$.

Remark. Integral domains that satisfy this property with the field of fractions playing the role of K are called integrally closed.

Proof. M is also finitely generated as a $\mathbb{Z}$-module, because $\mathcal{O}_K$ is finitely generated as a $\mathbb{Z}$-module. Then α is an algebraic integer, hence $\alpha \in \mathcal{O}_K$. □

An integral domain satisfying the conclusions of all 3 lemmas is called a Dedekind domain.

Let I be a non-zero ideal. By the Noetherian property, there exists a maximal ideal P such that $P \supset I$. Then P is a prime. It would be great if we had:

$$I \supset J \iff \exists I_2 \text{ ideal such that } II_2 = J.$$

Observe that:

- This holds for principal ideals:

$$\begin{aligned}\langle\beta\rangle \subset \langle\alpha\rangle &\iff \beta \in \langle\alpha\rangle \\ &\iff \beta = \gamma\alpha && \text{for some } \gamma \\ &\iff \langle\beta\rangle = \langle\gamma\rangle\langle\alpha\rangle\end{aligned}$$

- The $\Leftarrow$ direction is trivial. Indeed, if $\alpha \in I$, $\beta \in I_2$, then $\alpha\beta \in I$. The collection of all possible such $\alpha\beta$ generate J, so indeed $J \subset I$.

If this was true, we could write $I = PI_1$ for some ideal I_1.

Definition (Fractional Ideal)**.** A *fractional ideal* is a finitely generated $\mathcal{O}_K$-submodule of K.

Note. We extend the definition of multiplication of ideals to get multiplication of fractional ideals.

Lemma. If $I \subset K$ is a fractional ideal, then $\exists a \in \mathbb{Z}$ such that $a \cdot I$ is an ideal. Conversely, if $I \subset \mathcal{O}_K$ is an ideal, then $\alpha \cdot I$ is a fractional ideal for all $\alpha \in K$.

Proof. Let $\alpha_1, \dots, \alpha_k$ generate I as an $\mathcal{O}_K$-module. Write them as $\mathbb{Q}$-linear combinations of an integral basis. Take a to be a common denominator of all the coefficients. Then $a\alpha_j \in \mathcal{O}_K$. Hence $aI \subset \mathcal{O}_K$. Also, aI is an $\mathcal{O}_K$-module. Then aI is an ideal.

Conversely, if I is an ideal, then it is a finitely generated $\mathcal{O}_K$-module, then so is αI. □

Proposition. Let P be a prime. Then there exists a fractional ideal P' such that $PP' = \langle 1\rangle$.

Proof. Let $P' = \{\alpha \in K \mid \alpha P \subset \mathcal{O}_K\}$. This is an $\mathcal{O}_K$-module. Moreover, $\beta P' \subset \mathcal{O}_K$ for any $0 \neq \beta \in P$. Then $\beta P'$ is finitely generated as a $\mathbb{Z}$-module. Then P' is also finitely generated, so P' is a fractional ideal. Observe $P'P \subset \mathcal{O}_K$, hence it is an ideal (note that fractional ideals contained in $\mathcal{O}_K$ are always ideals). Also by $\mathcal{O}_K \subset P'$, $PP' \supset P\mathcal{O}_K = P$. $\mathcal{O}_K \supset P'P \supset P$, so $P'P$ is $\mathcal{O}_K$ or P. To exclude the second possibility, we show that there exists $\alpha \in P' \setminus \mathcal{O}_K$. Then we cannot have $\alpha P \subset P$, because that would imply $\alpha \in \mathcal{O}_K$, by $\mathcal{O}_K$ being integrally closed.

Let $0 \neq \beta \in P$. Let k be the smallest number such that there exists $Q_1, \dots, Q_k$ primes with $Q_1, \dots, Q_k \subset \langle \beta \rangle$ (see next lemma for existence of k). Note that $Q_1, \dots, Q_k \subset P$. Since P is a prime ideal, there exists j with $Q_j \subset P$ (we use the fact that $IJ \subset P \implies I \subset P$ or $J \subset P$). But Q_j is a maximal ideal, so $Q_j = P$. Let $\gamma \in Q_1 \cdots Q_{j-1} Q_{j+1} \cdots Q_k \setminus \langle \beta \rangle$. Such a γ exists by the minimality of k. Then $\gamma \notin \langle \beta \rangle \implies \frac{\gamma}{\beta} \notin \mathcal{O}_K$. Then $P\gamma \in \langle \beta \rangle \implies \frac{\gamma}{\beta} P \subset \mathcal{O}_K$. So we can take $\alpha = \frac{\gamma}{\beta}$. □

Start of lecture 7

Lemma. Let $0 \neq I \subset \mathcal{O}_K$ be an ideal. Then there are primes $P_1, \dots, P_k \subset \mathcal{O}_K$ such that $I \supset P_1 P_2 \cdots P_k$.

Proof. Trivial if I is a prime. Suppose that the lemma is false. Let I be maximal among the ideals for which it fails (since $\mathcal{O}_K$ is Noetherian). Then I is not a prime. Then there exists $\alpha, \beta \in \mathcal{O}_K \setminus I$ such that $\alpha\beta \in I$. Then

$$\underbrace{(I + \langle \alpha \rangle)}_{\supsetneq I} \underbrace{(I + \langle \beta \rangle)}_{\supsetneq I} \subset I$$

By hypothesis, there exists $Q_1, \dots, Q_l, R_1, \dots, R_m \subset \mathcal{O}_K$ primes such that

$$Q_1 \cdots Q_l \subseteq I + \langle \alpha \rangle \qquad \text{and} \qquad R_1 \cdots R_m \subseteq I + \langle \beta \rangle.$$

Multiplying these together, we see that the lemma holds for I also. □

Theorem. Non-zero ideals in $\mathcal{O}_K$ are products of primes in a unique way up to the order of the factors.

Proof. Let i be a non-zero ideal. Let $P_1 \subsetneq \mathcal{O}_K$ be an ideal that is maximal among those that contain I. Then P_1 is a maximal ideal, hence prime. Let $I_1 = I \cdot P^{-1}$ (P^{-1} is notation for P' from the Proposition about $PP' = \langle 1 \rangle$). Observe that $I_1 P = I$ and $I_1 \subset \mathcal{O}_K$ is an ideal. This is because $I_1 = I \cdot P^{-1} \subset PP^{-1} = \langle 1 \rangle = \mathcal{O}_K$. Also, $I_1 \supsetneq I$, for otherwise we would have $\alpha I \subset I$ for all $\alpha \in P^{-1}$, and this would imply $P' \subset \mathcal{O}_K$. Keep going with this, and we get sequences $P_1, P_2, \dots$ and $I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots$ such that $I_{j-1} = I_j P_j$. This must terminate, so $I_k = \mathcal{O}_K$ for some k. Then

$$I = P_1 I_1 = P_1 P_2 I_2 = \cdots = P_1 P_2 \cdots P_k I_k = P_1 \cdots P_k.$$

We now show that $P_1 \cdots P_k = Q_1 \cdots Q_l$ implies $k = l$ and $P_j = Q_{\sigma(j)}$ for some permutation σ. It is enough to show that $P_1 = Q_j$ for some j, because then the claim follows by induction on $k + l$. Observe that $P_1 \supset P_1 \cdots P_k = Q_1 \cdots Q_l$. By the argument for the proof of the lemma, P_1 must be equal to one of the Q_j's. □

Corollary. For all non-zero fractional ideals $I \subset K$, there exists $I^{-1} \subseteq K$ a fractional ideal such that $II^{-1} = \langle 1 \rangle$. That is, fractional ideals form a group.

Proof. If $I \subset \mathcal{O}_K$ is an ideal, then $I = P_1 \cdots P_k$ for some primes. We can use the lemma and take: $I^{-1} = P_1^{-1} \cdots P_k^{-1}$. In the general case, $I = J_1 \cdots J_2^{-1}$, where $J_1, J_2 \subseteq \mathcal{O}_K$. In fact we can take $J_2 = \langle a \rangle$ for some $a \in \mathbb{Z}$. Then use the special case, and take $I^{-1} = J^{-1} J_2$. □

Corollary. Let $0 \neq I, J \subset \mathcal{O}_K$ be ideals. Then

$$I \supset J \iff \exists I_2 \subset \mathcal{O}_K \text{ such that } II_2 = J.$$

Proof. Take $I_2 = J \cdot I^{-1}$. We need to show that $J \cdot I^{-1} \subseteq \mathcal{O}_K$. Let $\alpha \in J \cdot I^{-1}$. Then $\alpha I \subset J \subset I$, so by integrally closedness, $\alpha \in \mathcal{O}_K$ as needed. □

Corollary. $\mathcal{O}_K$ is a UFD if and only if it is a PID.

Proof. PID $\implies$ UFD holds in general.

Suppose it is a UFD. All elements $\alpha \in \mathcal{O}_K$ are the product of primes. All principal ideals are products of principal prime ideals. Let I be an ideal, and let $\beta \in I$. $\langle \beta \rangle \subset I \implies I \mid \langle \beta \rangle$. So all prime factors of I are prime factors of $\langle \beta \rangle$, hence principal. □

Start of lecture 8

Recall $J \mid I \iff J \supset I$, by a Corollary from last time.

Definition (gcd and lcm)**.** $\gcd(I_1, I_2)$ is the smallest ideal J such that $J \mid I_1$, $J \mid I_2$.

$\operatorname{lcm}(I_1, I_2)$ is the largest ideal J such that $I_1, I_2 \mid J$.

Fact:

$$\gcd(I_1, I_2) = I_1 + I_2 = \{\alpha + \beta : \alpha \in I, \beta \in J\}$$
$$\operatorname{lcm}(I_1, I_2) = I_1 \cap I_2$$

Norm of ideals

Definition (Norm of an ideal)**.** Let $I \subset \mathcal{O}_K$ be an ideal. Then $N(I) = |\mathcal{O}_K/I|$.

Recall: If $I \neq \langle 0 \rangle$, then $N(I) < \infty$. If $\alpha_1, \dots, \alpha_d$ generate I as a free $\mathbb{Z}$-module, then

$$N(I) = \left(\frac{\mathrm{disc}(\alpha_1, \dots, \alpha_d)}{\mathrm{disc}(K)} \right)^{1/2}$$

Proposition. Let $I, J \subset \mathcal{O}_K$ be non-zero ideals. Then

$$N(IJ) = N(I) \cdot N(J).$$

Proof. Enough to prove when J is a prime. This special case implies that

$$N(P_1 \cdots P_k) = N(P_1) \cdots N(P_k)$$

for primes $P_1, \dots, P_k$. Apply this to the factorisation of I, J, IJ to deduce the general case.

Now let J be a prime. Observe $\mathcal{O}_K/I \cong (\mathcal{O}_K/IJ)/(I/IJ)$. So

$$N(I) = N(IJ)/|I/IJ|.$$

So it is enough to show $N(J) = |I/IJ|$.

Let $\alpha_1, \dots, \alpha_{N(J)}$ be representatives for the cosets in $\mathcal{O}_K/J$. Let $\beta \in I \setminus IJ$.

Claim: $\beta\alpha_1, \dots, \beta\alpha_{N(J)}$ are representatives for I/IJ.

Proof:

(1) Show $\forall \gamma \in I$, $\exists \alpha_j$ such that $\gamma \equiv \beta\alpha_j \pmod{IJ}$. Enough to show that $\exists \alpha \in \mathcal{O}_K$ such that $\gamma \equiv \beta\alpha \pmod{IJ}$, because $\exists \alpha_j \equiv \alpha \pmod{J}$. Need to find α such that $\gamma - \beta\alpha \in IJ$. This is the same as showing that $\gamma \in IJ + \langle \beta \rangle$. Note $\langle \beta \rangle = I \cdot P_1 \cdots P_k$, where none of the P_j's are J. Now

$$\begin{aligned} IJ + \langle \beta \rangle &= \gcd(IJ, \langle \beta \rangle) \\ &= I \end{aligned}$$

That is good because $\gamma \in I$.

(2) Want to show $\beta\alpha_i \equiv \beta\alpha_j \pmod{IJ}$ implies $i = j$. We have $IJ \mid \langle\beta\rangle\langle\alpha_i - \alpha_j\rangle$. This is

$$\begin{aligned} & IJ \mid I \cdot P_1 \cdots P_k \langle\alpha_i - \alpha_j\rangle \\ \implies & IJ \mid P_1 \cdots P_k \langle\alpha_i - \alpha_j\rangle \\ & J \mid \langle\alpha_i - \alpha_j\rangle \\ \implies & i = j \end{aligned}$$

□

Lemma. Let $\alpha \neq 0 \in \mathcal{O}_K$. Then $N(\langle\alpha\rangle) = |N_{K/\mathbb{Q}}(\alpha)|$.

Proof. Let $\alpha_1, \dots, \alpha_d$ be an integral basis. Then

$$\langle\alpha\rangle = \alpha\alpha_1\mathbb{Z} \oplus \cdots \oplus \alpha\alpha_d\mathbb{Z}.$$

Now we can calculate:

$$N(\langle\alpha\rangle)^2 = \frac{\operatorname{disc}(\alpha\alpha_1, \dots, \alpha\alpha_d)}{\operatorname{disc}(\alpha_1, \dots, \alpha_d)}$$

and

$$\begin{aligned} \operatorname{disc}(\alpha\alpha_1, \dots, \alpha\alpha_d) &= \det(\sigma_i(\alpha\alpha_j))^2 \\ \sigma_1(\alpha)^2 \cdots \sigma_d(\alpha)^2 \cdot \det(\sigma_i(\alpha_j))^2 & \\ &= N_{K/\mathbb{Q}}(\alpha)^2 \operatorname{disc}(K) \end{aligned}$$

□

Let L/K be an extension of number fields. Given an ideal $I \subset \mathcal{O}_K$, we can associate to it an ideal in $\mathcal{O}_L$:

$$I \cdot \mathcal{O}_L = \{\alpha_1\beta_1 + \cdots + \alpha_k\beta_k : \alpha_i \in I, \beta_i \in \mathcal{O}_L\}$$

This is indeed an ideal in $\mathcal{O}_L$.

It is the smallest ideal that contains I.

Fact:

$$(I_1\mathcal{O}_L) \cdot (I_2\mathcal{O}_L) = (I_1I_2)\mathcal{O}_L$$

Given an ideal $I \subset \mathcal{O}_L$, we can associate to it one in $\mathcal{O}_K$: $I \cap \mathcal{O}_K$. Again this is an ideal. In general:

$$(I \cap \mathcal{O}_K)(I_2 \cap \mathcal{O}_K) \neq (I_1I_2 \cap \mathcal{O}_K)$$

Lemma. The following are equivalent for $P \subset \mathcal{O}_K$ and $Q \subset \mathcal{O}_L$ primes:

(1) $Q \mid P\mathcal{O}_L$.

(2) $Q \cap \mathcal{O}_K = P$.

Proof.

(1) $\implies$ (2) $Q \supset P\mathcal{O}_L \supset P$. So $Q \cap \mathcal{O}_K \supset P$. But P is a maximal ideal, so enough to show that $Q \cap \mathcal{O}_K \subsetneq \mathcal{O}_K$. And this follows by $1 \notin Q$.

(2) $\implies$ (1) (2) implies $Q \supset P$ and hence $Q \supset P\mathcal{O}_L$ because Q is an ideal. Then $Q \mid P\mathcal{O}_L$. □

Definition (Lying above)**.** Let $P \subset \mathcal{O}_K$, $Q \subset \mathcal{O}_L$ be primes. If $Q \mid P\mathcal{O}_L$ (or equivalently $Q \cap \mathcal{O}_K = P$), we say that Q lies above or over P, and P lies under or below Q.

Lemma. For all primes $Q \subset \mathcal{O}_L$, there is a unique prime in $\mathcal{O}_K$ that lies under it. For all primes $P \subset \mathcal{O}_K$, there is at least one in $\mathcal{O}_L$ that lies over it.

Proof.

(i) Need to show $Q \cap \mathcal{O}_K$ is a prime. Observe that $1 \notin Q \cap \mathcal{O}_K$, so is a proper ideal. Since $\mathcal{O}_L/Q$ is finite, the image of $\mathcal{O}_K$ ($\mathcal{O}_K/Q \cap \mathcal{O}_K$) in it is also finite. Since $\mathcal{O}_K$ is infinite, $Q \cap \mathcal{O}_K \neq \langle 0 \rangle$. Suppose that $\alpha, \beta \in \mathcal{O}_K$ and $\alpha\beta \in Q \cap \mathcal{O}_K$. Then $\alpha\beta \in Q$, a prime ideal, hence $\alpha \in Q$ or $\beta \in Q$. So $\alpha \in Q \cap \mathcal{O}_K$ or $\beta \in Q \cap \mathcal{O}_K$. So $Q \cap \mathcal{O}_K$ is indeed a prime.

(ii) We only need to show that $P\mathcal{O}_L$ is a proper ideal, because then it has prime factors. To that end: $\mathcal{O}_L = (P\mathcal{O}_L)(P^{-1}\mathcal{O}_L)$. If $\mathcal{O}_L = P\mathcal{O}_L$, then

$$\mathcal{O}_L = \mathcal{O}_L(P^{-1}\mathcal{O}_L) = P^{-1}\mathcal{O}_L$$

so $P^{-1} \subset \mathcal{O}_L$. But we have seen that P^{-1} contains elements which are not algebraic integers.

□

Start of

lecture 9

Definition (Ramification index)**.** Given an extension of number fields L/K, and primes $P \subset \mathcal{O}_K$, $Q \subset \mathcal{O}_L$ such that P lies over Q, we define $e(Q \mid P)$ to be the largest $e \in \mathbb{Z}$ such that $Q^e \mid P\mathcal{O}_L$.

Observe: $\mathcal{O}_L \to \mathcal{O}_L/Q$ sends $\mathcal{O}_K$ to $\mathcal{O}_K/P$ because $Q \cap \mathcal{O}_K = P$, so $\mathcal{O}_L/Q \mid \mathcal{O}_K/P$.

Definition (Inertial degree)**.** If P lies over Q, we define the *inertial degree*

$$f(Q \mid P) = [\mathcal{O}_L/Q : \mathcal{O}_K/P].$$

Let M/L, let $R \subset \mathcal{O}_M$ be a prime that lies over Q. Then R lies over P, and

$$\begin{aligned} e(R \mid P) &= e(R \mid Q)e(Q \mid P) \\ f(R \mid P) &= f(R \mid Q)f(Q \mid P) \end{aligned}$$

Lemma. For all ideals I, $\exists k \in \mathbb{Z}_{>0}$ such that I^k is a principal ideal.

Proof. Later. This Lemma is only stated now so that we can use it in the following proofs. □

Proposition. Let L/K. Let $I \subset \mathcal{O}_K$. Then $N(I\mathcal{O}_L) = N(I)^{[L:K]}$.

Proof. True for principal ideals. Indeed, if $I = \alpha\mathcal{O}_K$ for some $\alpha \in \mathcal{O}_K$, then

$$\begin{aligned} I\mathcal{O}_L &= \alpha\mathcal{O}_L \\ N(\alpha\mathcal{O}_K) &= N_{K/\mathbb{Q}}(\alpha) \\ N(\alpha\mathcal{O}_L) &= N_{L/\mathbb{Q}}(\alpha) = N_{K/\mathbb{Q}}(\alpha)^{[L:K]} \end{aligned}$$

Now to prove for a general ideal I, pick $k > 0$ such that I^k is principal. Then by the above, the equality holds for I^k. Hence it holds for I, by multiplicativity of $N(I)$ (since $N(I)$ is a positive integer). □

Theorem. Let $Q_1, \ldots, Q_r$ be the primes in $\mathcal{O}_L$ that lies above $P \subset \mathcal{O}_K$. Then:

$$[L : K] = \sum_{j=1}^{r} e(Q_j \mid P)f(Q_j \mid P).$$

Proof. $P\mathcal{O}_L = Q_1^{e(Q_1|P)} \cdots Q_r^{e(Q_r|P)}$ (by the definition of ramification index). Then

$$N(P\mathcal{O}_L) = N(Q_1)^{e(Q_1|P)} \cdots N(Q_r)^{e(Q_r|P)} = N(P)^{\sum_{i=1}^r e(Q_i|P) f(Q_j|P)}.$$

By the above Proposition,

$$N(P\mathcal{O}_L) = N(P)^{[L:K]}.$$

So the desired equality follows, since $N(P) > 1$. □

Theorem (Dedekind)**.** Let K be a number field. Let $P \subset \mathcal{O}_K$ a prime. Let p be the rational prime below P. Let $g \in \mathcal{O}_K[X]$ be monic and irreducible. Let α be a root of g, and let $L = K(\alpha)$. Assume $p \nmid [\mathcal{O}_L : \mathcal{O}_K[\alpha]]$. Let $\overline{g}$ be the image of g in $(\mathcal{O}_K/P)[X]$. Let

$$\overline{g} = \overline{g}_1^{e_1} \cdots \overline{g}_r^{e_r}$$

be the factorisation of $\overline{g}$ into irreducibles in the $(\mathcal{O}_K/P)[X]$. Let $g_j \in \mathcal{O}_K[X]$ monic such that $g_j \equiv \overline{g}_j \pmod{P}$ for all j. Then $Q_j = P\mathcal{O}_L + g_j(\alpha)\mathcal{O}_L$ is a prime in $\mathcal{O}_L$ with $f(Q_j \mid P) = \deg g_j$, and

$$P\mathcal{O}_L = Q_1^{e_1} \cdots Q_r^{e_r}.$$

Definition (Monogenic)**.** A number field K is *monogenic* if there is α such that $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

Proposition.

$$Q_1^{e_1} \cdots Q_r^{e_r} \subset P\mathcal{O}_L$$

Proof. Pick e_j elements (not necessarily distrinct) from each $P\mathcal{O}_L \cup \{g_j(\alpha)\}$, and multiply them together. Collect all such products in a set A. By definition, $Q_1^{e_1} \cdots Q_r^{e_r}$ is generated by A. So it is enough to show that $A \subset P\mathcal{O}_L$. All but one element in A has a factor in $P\mathcal{O}_L$. The exception is $g_1(\alpha)^{e_1} \cdots g_r(\alpha)^{e_r} \equiv g(\alpha) = 0 \pmod{P\mathcal{O}_L}$. Hence $g_1(\alpha)^{e_1} \cdots g_r(\alpha)^{e_r} \in P\mathcal{O}_L$. □

Start of lecture 10

Proposition. $P\mathcal{O}_L/Q_j$ is a factor of $(\mathcal{O}_K/P)[X]/\langle \overline{g}_j \rangle$ ("factor" is another way of saying "quotient of").

Two possible factors (since $\overline{g}_j$ is irreducible, so $(\mathcal{O}_K/P)[X]/\langle \overline{g}_j \rangle$ is a field): $P\mathcal{O}_L/Q_j \cong \{0\}$, so $Q_j = P\mathcal{O}_L$, or $P\mathcal{O}_L/Q_j \cong (\mathcal{O}_K/P)[X]/\langle \overline{g}_j \rangle$, in which case Q_j is a prime and $f(Q_j \mid P) = \deg g_j$.

For $A \subset R$, we use $\langle A \rangle_R$ to denote the ideal generated by A in R.

Lemma. Let $R_1 \overset{\varphi_1}{\to} R_2 \overset{\varphi_2}{\to} R_3$ be surjective homomorphisms of rings. Let $A \subset R_1$ such that $\langle \varphi_1(A) \rangle_{R_2} = \ker(\varphi_2)$. Then:

$$\ker(\varphi_2 \circ \varphi_1) = \langle A \rangle_{R_1} + \ker(\varphi_1).$$

Key point is to show:

$$\varphi_1(\langle A \rangle_{R_1}) = \langle \varphi_1(A) \rangle_{R_2}.$$

This uses the surjectivity of φ_1.

Proof of Proposition. First we prove

$$(\mathcal{O}_K/\underline{P})[X]/\langle \overline{g}_i \rangle \cong \mathcal{O}_K[\alpha]/\langle \underline{P}, g_j(\alpha) \rangle$$

$$\begin{array}{ccccc} & & (\mathcal{O}_K/\underline{P})[X] & \xrightarrow{\varphi_2} & (\mathcal{O}_K/\underline{P})[X]/\langle \overline{g}_j \rangle \\ & \overset{\varphi_1}{\nearrow} & & & \\ \mathcal{O}_K[X] & & & & \\ & \underset{\chi_1}{\searrow} & & & \\ & & \mathcal{O}_K[\alpha] & \xrightarrow{\chi_2} & \mathcal{O}_K[\alpha]/\langle \underline{P}, g_j(\alpha) \rangle \end{array}$$

$\varphi_2 \circ \varphi_1$: Let $A = \{g_j\}$. Then $\varphi_1(g_j) = \overline{g}_j$ generates $\langle \overline{g}_j \rangle = \ker(\varphi_2)$.

$$\ker(\varphi_2 \circ \varphi_1) = \langle g_j \rangle \mathcal{O}_K[X] + P\mathcal{O}_K[X].$$

$\chi_2 \circ \chi_1$: Let $A = \underline{P} \cup \{g_j\}$. $\chi_1(A) = \underline{P} \cup \{g_j(\alpha)\}$ generates $\ker(\chi_2)$.

$$\ker(\chi_2 \circ \chi_1) = \underline{P}\mathcal{O}_K[X] + \langle g_j \rangle \mathcal{O}_K[X] + \langle g \rangle \mathcal{O}_K[X].$$

Noet $g \equiv g_j \circ h \pmod{\underline{P}}$ (where h is the product of the other g_i's).

$$\begin{cases} g_j h \in \langle g_j \rangle_{\mathcal{O}_K[X]} \\ g - g_j h \in \underline{P}\mathcal{O}_K[X] \end{cases} \implies g \in \underline{P}\mathcal{O}_K[X] + \langle g_j \rangle_{\mathcal{O}_K[X]}$$

So the RHS of the two earlier equations are equal, so $\varphi_2 \circ \varphi_1$ and $\chi_2 \circ \chi_1$ have the same kernel.

Observe $Q_j \cap \mathcal{O}_K[\alpha] \supset \langle \underline{P}, g_j(\alpha) \rangle_{\mathcal{O}_K[\alpha]}$. $\mathcal{O}_K[\alpha]/Q_j \cap \mathcal{O}_K[\alpha]$ is a quotient of $\mathcal{O}_K[\alpha]/\langle \underline{P}, g_j(\alpha) \rangle$. Enough to show that

$$\mathcal{O}_L/Q_j \cong \mathcal{O}_K[\alpha]/(Q_j \cap \mathcal{O}_K[\alpha])$$

$\mathcal{O}_L \xrightarrow{\varphi} \mathcal{O}_L/Q_j$, $\varphi(\mathcal{O}_K[\alpha]) \cong \mathcal{O}_K[\alpha]/(Q_j \cap \mathcal{O}_K[\alpha])$. Enough to show: $\mathcal{O}_K[\alpha] + Q_j = \mathcal{O}_L$. Look at $\mathcal{O}_L/(\mathcal{O}_K[\alpha] + Q_j)$ in the category of abelian groups. This is a quotient of both $\mathcal{O}_L/\mathcal{O}_K[\alpha]$ and $\mathcal{O}_L/Q_j$.

$$[\mathcal{O}_L : \mathcal{O}_K[\alpha] + Q_j] \mid \gcd(\underbrace{[\mathcal{O}_L : \mathcal{O}_K[\alpha]]}_{p\nmid}, \underbrace{[\mathcal{O}_L : Q_j]}_{=N(Q_j)}) = 1$$

where $N(Q_j)$ is a power of p because Q_j lies above $\underline{P}$ that lies above p. □

Proposition. If $i \neq j$, then $Q_i + Q_j = \mathcal{O}_L$.

Proof. $\overline{g}_i, \overline{g}_j$ are two distinct irreducible polynomials in $(\mathcal{O}_K/\underline{P})[X]$, a Euclidean domain. By Euclidean algorithm, there exists $\overline{h}_i, \overline{h}_j \in (\mathcal{O}_K/\underline{P})[X]$ such that

$$\overline{h}_i\overline{g}_i + \overline{h}_j\overline{g}_j = 1.$$

Let h_i, h_j be lifts of h_i and h_j in $\mathcal{O}_K[X]$.

$$h_i g_i + h_j g_j \equiv 1 \pmod{\underline{P}}.$$

There exists $f \in \underline{P}\mathcal{O}_K[X]$ such that

$$\underbrace{h_i(\alpha)g_i(\alpha)}_{\in Q_i} + \underbrace{h_j(\alpha)g_j(\alpha)}_{\in Q_j} + \underbrace{f(x)}_{\in \underline{P}} = 1$$

So $1 \in Q_i + Q_j$, so $Q_i + Q_j = \mathcal{O}_L$. □

Proof of Dedekind. Recall: $P\mathcal{O}_L \ supset Q_1^{e_1} \cdots Q_r^{e_r}$.

□

Start of lecture 11

We will use the notation of Legendre symbols:

$$\left(\frac{m}{p}\right) = \begin{cases} 0 & \text{if } p \mid m \\ 1 & \text{if } \exists a \neq 0 \in \mathbb{Z}/p\mathbb{Z} \text{ with } a^2 \equiv m \pmod{p} \\ -1 & \text{otherwise} \end{cases}$$

See Number Theory for some properties.

Theorem. Let $K = \mathbb{Q}(\sqrt{m})$. Let $p \in \mathbb{Z}$ be prime and suppose m is square-free, with $m \neq 0, 1$. Then:

(1) p is ramified in K, that is $\exists P \subset \mathcal{O}_K$ such that $p\mathcal{O}_K = P^2$, if and only if p is od and $p \mid m$, or p is even and $m \equiv 2, 3 \pmod 4$.

(2) p is split in K, that is $\exists P_1, P_2 \subset \mathcal{O}_K$ such that $p\mathcal{O}_K = P_1 P_2$, if and only if p is odd and $\left(\frac{m}{p}\right) = 1$ or $p = 2$ and $m \equiv 1 \pmod 8$.

(3) p is inert, that is $p\mathcal{O}_K$ is a prime, if and only if p is odd and $\left(\frac{m}{p}\right) = -1$ or $p = 2$ and $m \equiv 5 \pmod 8$.

Proof. If p is odd or if $p = 2$ and $m \equiv 2, 3 \pmod 4$, then we can apply Dedekind with $g(x) = x^2 - m$, because $p \nmid [\mathcal{O}_K : \mathbb{Z}[\sqrt{m}]]$. If $p = 2$ and $m \equiv 1 \pmod 4$, then we can apply Dedekind with $g(x) = x^2 - m + \frac{1-m}{4}$, which is the minimal polynomial of $\frac{1+\sqrt{m}}{2}$. □

Definition (Class group)**.** Write $\mathcal{I}$ for the set of fractional ideals in K, which form an abelian group under multiplication. Let $\mathcal{P}$ denote the principal fractional ideals, which form a subgroup. The class group of K is

$$\mathrm{Cl}(K) = \mathcal{I}/\mathcal{P}.$$

We have seen that for all $I \in \mathcal{I}$, there exists $a \in \mathbb{Z}$ such that $aI \subset \mathcal{O}_K$, that is aI is an integral ideal. Thus each class in $\mathrm{Cl}(K)$ contains integral ideals.

Alternatively, $\mathrm{Cl}(K)$ can be defined as equivalence classes of integral ideals under $I \sim J$, where $I \sim J$ if and only if $\exists \alpha \in K$ such that $I = \alpha J$.

Definition (Class number)**.** The *class number* of K is $h(K) = |\,\mathrm{Cl}(K)|$.

$h(K) = 1$ if and only if $\mathcal{O}_K$ is a PID (which we also showed before happens if and only if $\mathcal{O}_K$ is a UFD).

Theorem. For all number fields, $h(K) < \infty$.

In order to prove this, we need a couple of results:

Theorem (Minkowski's bound)**.** Let K be a number field, let $I \subset \mathcal{O}_K$ be an ideal. Write s for the number of pairs of complex embeddings of K. Then $\exists \alpha \in I$ such that

$$|N(\alpha)| \leq \frac{d^1}{d^d}\left(\frac{4}{\pi}\right)^s N(I)\sqrt{\operatorname{disc}(K)}.$$

Then by Stirling's Approximation,

$$\frac{d^1}{d^d} = (1+\sigma(1))\sqrt{2\pi d}e^{-d}.$$

Corollary (Minkowski's bound 2)**.** Let K be a number field, and let s be the number of pairs of complex embeddings of K. Then every ideal class in $\operatorname{Cl}(K)$ contains an integral ideal I with

$$N(I) \leq \frac{d^1}{d^d}\left(\frac{4}{\pi}\right)^s \sqrt{\operatorname{disc}(K)}.$$

Proof. Let I be an ideal. Let $J \subset \mathcal{O}_K$ be an ideal in the class of I^{-1}. We apply the Minkowski's bound to J, so there is $\alpha \in J$ such that $N(\alpha) \leq \cdots N(J)\sqrt{\operatorname{disc}(K)}$. Since $\alpha \in J$, $J \mid \langle\alpha\rangle$, so $\alpha J^{-1} \subset \mathcal{O}_K$ is an ideal in the class of I. Also,

$$N(\alpha J^{-1}) = |N(\alpha)|N(J)^{-1} \leq \frac{d^1}{d^d}\left(\frac{4}{\pi}\right)^s \sqrt{\operatorname{disc}(K)}.$$

□

This implies $h(K) < \infty$ because of:

Lemma. Let $X \in \mathbb{R}_{>0}$. Then there are only finitely many ideals in $\mathcal{O}_K$ of norm $\leq X$.

Proof. Each ideal of norm $\leq X$ is the product of at most $\log_2(X)$ primes. The primes in those decompositions lie over rational primes $\leq X$. For each such prime, there at most d primes of $\mathcal{O}_K$ lying over it. □

Computation of $\operatorname{Cl}(K)$:

(1) Calculate $X = \frac{d^1}{d^d}\left(\frac{4}{\pi}\right)^s\sqrt{\mathrm{disc}(K)}$. For $K = \mathbb{Q}(\sqrt{m})$, we get:

$$X = \begin{cases} \frac{\sqrt{m}}{2} & \text{if } m > 1 \text{ and } m \equiv 1 \pmod 4 \\ \sqrt{m} & \text{if } m > 1 \text{ and } m \equiv 2,3 \pmod 4 \\ \frac{2\sqrt{-m}}{\pi} & \text{if } m < 0 \text{ and } m \equiv 1 \pmod 4 \\ \frac{4\sqrt{-m}}{\pi} & \text{if } m < 0 \text{ and } m \equiv 2,3 \pmod 4 \end{cases}$$

(2) List all rational primes $\leq X$.

(3) Split all of these rational primes in $\mathcal{O}_K$, and make a list of all prime ideals with norm $\leq X$, say $P_1, \ldots, P_k$.

(4) Figure out when $P_1^{m_1} \cdots P_k^{m_k}$ is principal for some $m_1, \ldots, m_k \in \mathbb{Z}$.

Corollary (Minkowski bound 3)**.**

$$\mathrm{disc}(K) \geq \frac{d^{2d}}{(d^1)^2}\left(\frac{\pi}{4}\right)^{2s}.$$

This follows from $N(I) \geq 1$ and Minkowski's bound 2.

Start of lecture 12

Recall: $\sigma_1, \ldots, \sigma_r$ are the embeddings $K \to \mathbb{C}$ with real image, $\tau_1, \overline{\tau_1}, \ldots, \tau_s, \overline{\tau_s}$ are the other embeddings, $d = r + 2s$. We defined

$$\Sigma : K \to \mathbb{R}^d$$
$$\Sigma(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_r(\alpha), \mathrm{Re}(\tau_1(\alpha)), \mathrm{Im}(\tau_1(\alpha)), \ldots, \mathrm{Re}(\tau_s(\alpha)), \mathrm{Im}(\tau_s(\alpha)))$$

$\Sigma(\mathcal{O}_K) \subset \mathbb{R}^d$ is a lattice, i.e. it is an additive subgroup of $\mathbb{R}^d$ generated by d linearly independent elements.

$$\mathrm{coVol}(\Sigma(\mathcal{O}_K)) = 2^{-s}\sqrt{\mathrm{disc}(K)}.$$

Let $I \subset \mathcal{O}_K$ be an ideal, then $\Sigma(I) \subset \Sigma(\mathcal{O}_K)$ is a sublattice, and

$$\mathrm{coVol}(\Sigma(I)) = 2^{-s}\sqrt{\mathrm{disc}(I)} = 2^{-s}N(I)\sqrt{\mathrm{disc}(K)}.$$

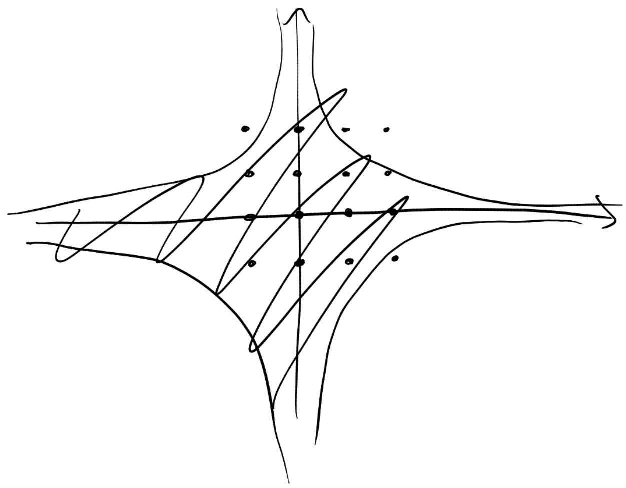
(where $\mathrm{disc}(I)$ is the discriminant of a generating tuple).

$\mathcal{N} : \mathbb{R}^d \to \mathbb{R}$,

$$\mathcal{N}(x_1, \ldots, x_d) = \prod_{j=1}^{r} |x_j| \prod_{j=1}^{s} (|x_{r+j}|^2 + |x_{r+j+1}|^2).$$

Note $\alpha \in K$, $\mathcal{N}(\Sigma(\alpha)) = |N(\alpha)|$. Need to prove that the lattive $\Sigma(\mathcal{O}_K)$ contains a non-zero element in the region:

$$\{x \in \mathbb{R}^d : \mathcal{N}(x) \leq N(I)\sqrt{\mathrm{disc}(K)}\}$$



Geometry of numbers

Convex means that if $x, y \in S$ and $a \in (0,1)$, then $ax + (1-a)y \in S$.

Symmetric to 0 means that if $x \in S$, then $-x \in S$.

Lemma. Let $\Lambda \subset \mathbb{R}^d$ be a lattice, and let $S \subset \mathbb{R}^d$ be a Borel set with $\text{Vol}(S) > \text{coVol}(\Lambda)$, then there exists $x \neq y$ in S such that $x - y \in \Lambda$.

Proof. Let F be a fundamental domain for Λ. Note that $\mathbb{R}^d$ is the disjoint union of

$$\{F + a : a \in \Lambda\}.$$

Define: $S(a) = (S \cap (F + a)) - a$ for $a \in \Lambda$. Observe that $S(a) \subset F$.

$$\text{Vol}(S) = \sum_{a \in \Lambda} \text{Vol}(S \cap (F + a)) = \sum_{a \in \Lambda}$$

Then $\exists a \neq b \in \Lambda$ and $x \in S(a) \cap S(b)$. Then $x + a \neq x + b \in S$, and $(x + a) - (x + b) = a - b \in \Lambda$. $\square$

Theorem (Minkowski's theorem)**.** Let $\Lambda \in \mathbb{R}^d$ be a lattice, and let $S \subset \mathbb{R}^d$ be convex and symmetric to 0. Suppose $\text{coVol}(S) > 2^d \, \text{coVol}(\Lambda)$. Then $\exists x \in \Lambda \cap S$ such that $x \neq 0$.

Proof. We apply the lemma for the set

$$\frac{1}{2}S = \left\{\frac{1}{2}x : x \in S\right\}.$$

Then $\mathrm{Vol}\left(\frac{1}{2}S\right) = 2^{-d}\,\mathrm{Vol}(S)$. We get $x \neq y \in \frac{1}{2}S$ such that $x - y \in \Lambda$. THen $2x, -2y \in S$, and by symmetry, $x - y = \frac{1}{2}(2x) + \frac{1}{2}(-2y) \in S$ by convexity. □

Example (non-example)**.** $\Lambda = \mathbb{Z}^d$, $S = (-1,1)^d$, $\mathrm{coVol}(S) = 2^d = 2^d\,\mathrm{coVol}(\Lambda)$, $S \cap \Lambda = \{0\}$.

Is S is closed in addition, then $>$ can be replaced by $\geq$.

Proof of Minkowski's bound. Consider $S = [-Y, Y]^d$ for some $Y \in \mathbb{R}$. Then $\mathrm{Vol}(S) = 2^d Y^d$, and $|\mathcal{N}(x)| \leq 2^s Y^d$ for $x \in S$. Minkowski's theorem gives $S \cap \Lambda \neq \{0\}$ if $\mathrm{Vol}(S) > 2^s\,\mathrm{coVol}(\Lambda)$.

□

Start of lecture 13

Note that for $I \subset \mathcal{O}_K$, there exists $k > 0$ such that I^k is principal if and only if the order of I in $\mathrm{Cl}(K)$ is finite. But we now that $\mathrm{Cl}(K)$ is finite, hence the order is always finite, so there always exists some $k > 0$ such that I^k is principal.

Units: $\alpha \in \mathcal{O}_K$ is a unit if $\alpha^{-1} \in \mathcal{O}_K$. Notation:

$$\mathcal{O}_K^\times := \{u \in \mathcal{O}_K \mid u \text{ is a unit}\}.$$

Lemma. The following are equivalent for $\alpha \in \mathcal{O}_K$:

(1) $\alpha \in \mathcal{O}_K^\times$.

(2) $N(\alpha) = \pm 1$.

(3) $\langle \alpha \rangle = \mathcal{O}_K$.

Proof.

(1) ⇒ (2) $N(\alpha) \in \mathbb{Z}$ and

$$N(\alpha)N(\alpha^{-1}) = N(\alpha\alpha^{-1}) = N(1) = 1$$

with both $N(\alpha), N(\alpha^{-1}) \in \mathbb{Z}$ since $\alpha, \alpha^{-1} \in \mathcal{O}_K$. Hence $N(\alpha) = \pm 1$.

(2) $\Rightarrow$ (3) Note:

$$N(\langle\alpha\rangle) = |N(\alpha)| = 1 \implies |\mathcal{O}_K/\langle\alpha\rangle| = 1 \implies \langle\alpha\rangle = \mathcal{O}_K.$$

(3) $\Rightarrow$ (1) If $\langle\alpha\rangle = \mathcal{O}_K$, then $1 = \alpha \cdot \beta$ for some $\beta \in \mathcal{O}_K$. Hence $\alpha \in \mathcal{O}_K^\times$.

□

Quadratic fields

Let $m \neq 0, 1$, m square-free, $K = \mathbb{Q}(\sqrt{m})$. Recall:

$$\mathcal{O}_K = \begin{cases} a + b\sqrt{m} : a, b \in \mathbb{Z} & \text{if } m \equiv 2, 3 \pmod 4 \\ \frac{a+b\sqrt{m}}{2} : a, b \in \mathbb{Z}, 2 \mid a + b & \text{if } m \equiv 1 \pmod 4 \end{cases}$$

We have

$$N(a + b\sqrt{m}) = (a + b\sqrt{m})(a - b\sqrt{m}) = a^2 - mb^2.$$

There are 2 cases:

- $m \equiv 2, 3 \pmod 4$: $\mathcal{O}_K^\times$ is the elements $u = a + b\sqrt{m}$ with $a, b \in \mathbb{Z}$ such that
$$a^2 - mb^2 = \pm 1 \tag{$*$}$$
- $m \equiv 1 \pmod 4$: $\mathcal{O}_K^\times$ is the elements $u = \frac{a+b\sqrt{m}}{2}$ with $a, b \in \mathbb{Z}$ such that
$$a^2 - mb^2 = \pm 4 \tag{$**$}$$

First consider $m < 0$. If $m \leq -5$, then

$$-mb^2 = \pm 4 - a^2 \leq 4 \implies |b| \leq \frac{4}{5} \implies b = 0.$$

Then $u = \pm 1$. We can go over the cases $m = -1, -2, -3, -4$ by hand:

- $m = -1$, the units are ± 1, $\pm\sqrt{-1}$.
- $m = -2, -4$ the units are ± 1.
- $m = -3$, the units are ± 1, $\frac{\pm 1 \pm \sqrt{-3}}{2}$.

Now move onto $m \geq 2$.

Theorem. Let $K = \mathbb{Q}(\sqrt{m})$, $m \geq 2$, squarefree. Then there is a unit $u > 1$ that is smallest, and all units are of the form:

$$\mathcal{O}_K^\times = \{\pm u^n : n \in \mathbb{Z}\}.$$

Proof. We first show that all units $u > 1$ are of the form $u = a + b\sqrt{m}$ with $a, b > 0$. Note:

$$N(u) = \pm 1 = (a + b\sqrt{m})(a - b\sqrt{m})$$

hence

$$\{\pm u^{\pm 1}\} = \{\pm a \pm \sqrt{m}b\}.$$

If $u > 1$, then these are distinct, and $a + \sqrt{m}b$ are the largest among them. Therefore $a, b > 0$ indeed. The fact that u with $u > 1$ exists is not examinable, but there are two ways to see this:

(1) The Pell equation $a^2 - mb^2 = 1$ always has positive solutions (see Part II Number Theory).

(2) Can be proved using Minkowski's theorem. We will sketch this proof.

We prove that there exists a smallest u among those > 1. Suppose not. Then $\exists u_1, u_2, \ldots, \in \mathcal{O}_K^\times$ such that $u_1, u_2 > u_3 > \cdots > 1$. Then $\frac{u_n}{u_{n+1}} \to 1$, with each term lying in $\mathcal{O}_K^\times$ and greater than 1. Then $\frac{u_n}{u_{n+1}} \geq \frac{1+\sqrt{m}}{2} > 1$, which is a contradiction. Let $v \in \mathcal{O}_K^\times$. We show that $v = \pm u^{\pm n}$ for some $n \in \mathbb{Z}$. Clearly this is true for v if and only if true for $\pm v^{\pm 1}$. So we can assume $v \geq 1$. $v = 1$ is obvious, so assume $v > 1$. We cannot have

$$v \in (u^n, u^{n+1})$$

for any $n \geq 0$ because then $v \cdot u^{-n} \in \mathcal{O}_K^\times$ and $1 < v \cdot u^{-n} < u$, contradicting the choice of u. So $v = u^n$ for some $n \geq \mathbb{Z}_{\geq 1}$. □

This u in the theorem is called the *fundamental unit*.

We can find the fundamental unit by searching through the solutions of $(*)$ or $(**)$. For this the following observation helps:

Let (a_1, b_1) and (a_2, b_2) be solutions of $(*)$ with $a_1, a_2, b_1, b_2 \geq 0$. Then $1 \leq b_1 < b_2$ implies:

$$a_1^2 = mb_1^2 \pm 1 < mb_2^2 \pm 1 = a_2^2$$

So $a_1^2 < a_2^2$, so in fact $a_1 + b_1\sqrt{m} < a_2 + b_2\sqrt{m}$. So when looking for the fundamental solution, it suffices to find the solution with b minimal.

Theorem (Dirichlet's unit theorem)**.** Let K be a number field with r real embeddings and s pairs of complex embeddings. Let W denote the roots of unity contained in $\mathcal{O}_K$, that is $\alpha \in \mathcal{O}_K$ such that $\alpha^m = 1$ for some $m \in \mathbb{Z}$. Then there are $r+s-1$ units $u_1, u_2, \dots, u_{r+s-1} \in \mathcal{O}_K^\times$ such that all units can be written uniquely as

$$\omega u_1^{n_1} \cdots u_{r+s-1}^{n_{r+s-1}}$$

for some $n_1, \dots, n_{r+s-1} \in \mathbb{Z}$ and $\omega \in W$. In addition, $|W| < \infty$.

Start of lecture 14

The logarithmic embedding is

$$\log : K \to \mathbb{R}^{r+s}; \alpha \mapsto (\log|\sigma_1(\alpha)|, \dots, \log|\sigma_r(\alpha), 2\log|\tau_1(\alpha)|, \dots, 2\log|\tau_s(\alpha)|)^\top,$$

which is a homomorphism from $(K, \cdot)$ to $(\mathbb{R}^{r+s}, +)$. Observe that

$$\log|N(\alpha)| = \sum_{i=1}^{r+s} (\log(\alpha))_j.$$

We write $V \subset \mathbb{R}^{r+s}$ for $\{x : x+1 \cdots + x_{r+s} = 0\}$. If $\alpha \in \mathcal{O}_K^\times$, then $N(\alpha) = \pm 1$, and hence $\log \alpha \in V$.

Proposition 1. $\ker(\log) = W$ and $|W| < \infty$.

Proposition 2. $\log(\mathcal{O}_K^\times)$ is a lattice in V.

Proof of Dirichlet's unit theorem (non-examinable). Let $x_1, \dots, x_{r+s-1}$ be a basis for $\log(\mathcal{O}_K^\times)$. We can choose u_j such that $\log(u_j) = x_j$. Easy to check that the theorem holds with this choice. □

Proof of Proposition 1. If $\log \alpha = 0$, then $|\sigma_j(\alpha)| = 1$, $|\tau_j(\alpha)| = 1$ for all j. This means that

$$\|\Sigma(\alpha)\| \le \sqrt{d},$$

and $\Sigma(\mathcal{O}_K)$ is a lattice, so it has a finite intersection with $B(0, \sqrt{d}) = \{v \in \mathbb{R}^d \mid \|v\| < \sqrt{d}\}$. Then $|\ker(\log)| < \infty$. $\ker(\log)$ is a group under $\cdot$. So $\alpha \in \ker \log$ has finite, i.e. $\alpha^m = 1$ for some $n \in \mathbb{Z}_{>0}$. Thus $\alpha \in W$. □

Lemma. Let $\Lambda \subset V$ be an additive subgroup. Then Λ is a lattice if and only if there is $R \in \mathbb{R}_{>0}$ such that $\Lambda \cap B(x, R)$ is finite and non-empty for all $x \in V$.

Proof. Omitted. □

Proof of Proposition 2. To prove Proposition 2, we need the following: Given $x \in \mathbb{R}^{r+s}$ with $\sum_j x_j = 0$, we need to show that the set of units $u \in \mathcal{O}_K^\times$ that satisfy

$$\| \log(u) - x \| < R$$

is finite and non-empty. For simplicity assume $s = 0$. The above inequality is equivalent to

$$e^{x_j} e^{-\tilde{R}} \leq |\sigma_j(u)| \leq e^{x_j} \cdot e^{\tilde{R}}$$

for all i. Finiteness follows from $\Sigma(\mathcal{O}_K)$ being a lattice.

Non-empty is more difficult. Observe: enough to show $\exists u \in \mathcal{O}_K^\times$ with

$$|\sigma_j(u)| \leq C_0 e^{x_j}. \tag{$*$}$$

This is because: $|N(u)| = 1$, so

$$\prod |\sigma_j(u)| = 1 \implies |\sigma_j(u)| \geq \left(\prod_{k \neq j} |\sigma_k(u)| \right)^{-1} \geq C_0^{d-1} e^{\sum_{k \neq j} x_k} = C_0^{d-1} e^{-x_j}$$

By Minkowski's theorem applied to the lattice $\Sigma(\mathcal{O}_K)$ and the convex set

$$\{v : |v_j| < C_0 e^{x_j}\}$$

gives $\alpha \in \mathcal{O}_K$ that satisfies (**??**) provided C_0 is large enough. Now the problem is that α may not be a unit. However:

$$|N(\alpha)| \leq C_0^d \prod_i e^{x_i} = C_0^d$$

where C_0^d is some constant which depends only on K. There are only finitely many principal ideals in $\mathcal{O}_K$ with norm $\leq C_0^d$. Fix a generator in each of them, say α_I for the generator of I. Let $\alpha \in \mathcal{O}_K$ that the argument gives, so it satifies $(*)$ and $|N(\alpha)| < C_0^d$. Then $\langle \alpha \rangle = \langle \alpha_{\langle \alpha \rangle} \rangle$. Therefore $\alpha \cdot \alpha_{\langle \alpha \rangle}^{-1} \in \mathcal{O}_K^\times$. □

Cyclotomic Fields

Notation. $k \in \mathbb{Z}_{>0}$, then $\theta_k = 2^{2\pi i/k}$. This is a primitive k-th root of unity.

Lemma. Fix $p \in \mathbb{Z}$ a prime. Let $K = \mathbb{Q}(\theta_p)$. Let W be the roots of unity in $\mathcal{O}_K$. Then
$$W = \{\pm\theta_p^k : k = 0, \dots, p-1\} = \{\theta_{2p}^k : k = 0, \dots, 2p-1\}.$$

Proof. Let $t \in \mathbb{R}_{>0}$ minimal with the property that $e^{2\pi i t} \in W$. Recall that W is finite. Recall that W is finite, so this minimum exists. Claim: if $e^{2\pi i s} \in W$, then $s/t \in \mathbb{Z}$. If not then $e^{2\pi i(s-(s/t)t} \in W$. This contradicts minimality. I know $e^{2\pi i/2p} \in W$. So $t = \frac{1}{k2p}$ for some $k \in \mathbb{Z}_{>0}$. □

Start of lecture 15

TODO

Start of lecture 16

$p \in \mathbb{Z}_{\geq 3}$ a prime, $\theta_p = e^{2\pi i/p}$, $K = \mathbb{Q}(\theta_p)$. $\forall i, j \in \mathbb{Z}$ with $I \not\equiv j \pmod p$, there exists $u_{i,j} \in \mathbb{Z}[\theta_p]^\times$ such that $p = u_{i,j}(1-\theta_p)^{p-1}$.

Proof of $\mathcal{O}_K = \mathbb{Z}[\theta_p]$. We made an indirect assumption, and we want to get a contradiction. We found $\beta \in \mathcal{O}_K \setminus z\mathbb{Z}[\theta_p]$ and $\gamma \in \mathbb{Z}[\theta_p]$ and $\alpha \in \mathbb{Z}$ such that
$$(1-\theta_p)\beta = a + (1-\theta_p)\gamma.$$

We have $p \nmid a$, for otherwise
$$\beta = \frac{a}{1-\theta_p} + \gamma,$$
and if $a = pa'$, then
$$\frac{a}{1-\theta_p} = \frac{a'u(1-\theta_p)^{p-1}}{1-\theta_p} \in \mathbb{Z}[\theta_p].$$
So $\beta \in \mathbb{Z}[\theta_p]$, which is not the case. This proves $p \nmid a$. On the other hand,
$$\frac{a}{1-\theta_p} = \beta - \gamma \in \mathcal{O}_K.$$

Then
$$\underbrace{\frac{1}{a}\left(\frac{a}{1-\theta_p}\right)^{p-1}}_{\in \mathcal{O}_K} = \underbrace{\frac{a^{p-1}}{p}}_{\in \mathbb{Q}}$$

hence

$$\frac{a^{p-1}}{p} \in \mathbb{Z},$$

a contradiction to $p \nmid a$.

Proof of the claim that: $\langle p \rangle = P^{p-1}$ for a prime $P \subset \mathcal{O}_K$, and

$$P = \langle \theta_p^i - \theta_p^j \rangle$$

for any $i, j \in \mathbb{Z}$ such that $i \not\equiv j \pmod p$.

Let $P_{ij} = \langle \theta_p^i - \theta_p^j \rangle$, then $\langle p \rangle = P_{ij}^{p-1}$. $N(\langle p \rangle) = p^{p-1}$, hence $N(P_{ij}) = p$. So P_{ij} must be a prime ideal. By uniqueness of factorisation, P_{ij} does not depend on i and j.

Definition (Regular prime)**.** A prime $p \in \mathbb{Z}$ is regular if $p \nmid h(\mathbb{Q}(\theta_p))$.

Theorem (Regular Fermat's Last Theorem)**.** Let $p \geq 5$ ba a *regular prime*. Then there are no solutions of

$$x^p + y^p = z^p$$

with $x, y, z \in \mathbb{Z}$. such that $p \nmid xyz$ (the case $p \nmid xyz$ is known as "Case I").

Proposition. Assume that x, y, z is a solution of $x^p + y^p = z^p$ and assume $\gcd(x, y, z) = 1$ and $p \nmid xyz$. Then

$$x + \theta_p y = u\alpha^p$$

where $u \in \mathcal{O}_K^\times$, and $\alpha \in \mathcal{O}_K$.

Proof. Recall:

$$(x + y)(x + \theta_p y) \cdots (x + \theta_p^{p-1} y) = z^p.$$

Claim: there is no prime $Q \subset \mathcal{O}_K$ such that $Q \mid \langle x + \theta_p^i y \rangle, \langle x + \theta_p^j y \rangle$ for $i \not\equiv j \pmod p$.

Suppose the contrary. Then

$$Q \mid \underbrace{\langle \theta_p^i y - \theta_p^j y \rangle}_{P\langle y \rangle}, \underbrace{\langle \theta_p^{-i} x - \theta_p^{-j} x \rangle}_{P\langle x \rangle}.$$

If $Q = P$, then $P \mid \langle z \rangle^p$, so $P \mid \langle z \rangle$, so $z \in P \cap \mathbb{Z} = p\mathbb{Z}$, hence $p \mid z$, cotnradicting our assumption of being in Case I. So $Q \neq P$. Then $Q \mid \langle x \rangle, \langle y \rangle$, so $x, y \in Q$. We must have $\gcd(x, y) = 1$, for any common prime factor would also divide z by $z^p = x^p + y^p$, and we assume $\gcd(x, y, z) = 1$. So we can find $a, b \in \mathbb{Z}$ such that $1 = ax + by$. Then $1 \in Q$, which is not possible. So we have proved the claim (that there is no prime Q dividing more than one of the ideals $\langle x + \theta_p^i y \rangle$).

Then $\langle x + \theta_p y \rangle = I^p$ for some ideal $I \subset \mathcal{O}_K$ (not necessarily prime). We assumed that $p \nmid h(K)$. Hence the only class in the class group whose p-th power is the unit element, that is the class of principal ideals, is the unit element itself (the class of principal ideals). We know that I^p is principal because $I^p = \langle x + \theta_p y \rangle$, so I must be principal too, and the proposition follows. □

Proposition. Assume that x, y, z is a solution of $x^p + y^p = z^p$ and assume $\gcd(x, y, z)$. Then we must have $x \equiv y \pmod p$.

Proof. Suppose that there is a solution x, y, z. We may assume $\gcd(x, y, z) = 1$ (by dividing by any common factor). By a previous proposition, we get $x \equiv y \pmod p$. Applying it to $x^p - z^p = y^p$, we get $x \equiv -z \pmod p$. Then

$$x^p + y^p - z^p \equiv 3x^p \pmod p$$

But the LHS is equal to 0, so $p \mid 3x^p$, but $p \nmid 3$, because $p \geq 5$, and $p \nmid x$ because of Case I. □

Start of lecture 17

TODO

Index