Introduction to Algebraic Number Theory

Prof. Dr. Özlem Imamoglu

Jakob Glas, Kevin Yeh

ETH Zürich, Autumn 2019

Contents

Organiser: Dr. Danylo Radchenko
Tutor: Alessandro Lägeler

0 A Note on Notation

1 Introduction and Motivation

The main goal of this course is to cover the basic concepts of algebraic number theory. In particular, we will study the ring of integers of number fields, introduce the associated ideal class group and prove the finiteness of the class number and Dirichlet's Unit Theorem.

If we are ambitious we will also take a look at the Kronecker-Weber Theorem, which states that every finite Abelian extension of the rationals is contained in a cyclotomic extension. Under a more conceptual point of view, this can be understood in the following way: We can consider the exponential function $x \mapsto \exp(2\pi i)$ and look at the torsion points of its image inside the circle. Then these are exactly the roots of unity that generate the Abelian extensions of $\mathbb{Q}$.

Recall:

Definition 1.1. An *Abelian extension* is a Galois field extension where the Galois group is Abelian.

Kronecker tried to generalize this behaviour to the next "simple" cases of number fields, namely the quadratic extensions of $\mathbb{Q}$. In his famous "Jugendtraum" he conjectured that there are functions similar to the exponential that generate all Abelian extensions of quadratic extensions of $\mathbb{Q}$. In other words, he conjectured the existence of a function, call it j such that

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{D}, j(\times))/\mathbb{Q}(\sqrt{D}))$$

is Abelian. However, only if we restrict our attention to *imaginary* quadratic fields, i. e. $D < 0$, a solution is known. For real quadratic fields we still do not know such a function.

Let us now consider some typical problems from number theory to motivate further studies.

1.1 Primes represented by Quadratic Forms

Fermat proved the following:

Theorem 1.2. *Let $p \neq 2$ be a prime. Then $p = a^2 + b^2$ with $a, b \in \mathbb{Z}$ if and only if $p \equiv 1 \mod 4$.*

In the exercise sheet we will prove a slightly different version:

Exercise 1.3. $p = a^2 - ab + b^2$ if and only if $p \equiv 1 \bmod 3$.

Proof of the theorem. ($\Rightarrow$) Any square is 0 or $1 \mod 4$. So if $p = a^2 + b^2$, then $p \equiv 1 \mod 4$.
($\Leftarrow$) We use the arithmetic in the Gaussian integers $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$. Let us first recall some facts about this ring:

1. $\mathbb{Z}[i]$ is Euclidean
2. $(\mathbb{Z}[i])^\times = \{\pm 1, \pm i\}$.

Claim: If $p \equiv 1 \mod 4$, then p does not stay prime in $\mathbb{Z}[i]$.

If the claim is true, then there exist $\alpha, \beta \in \mathbb{Z}[i]$ that are not units such that $p = \alpha\beta$, which implies that $\mathrm{N}(p) = p^2 = \mathrm{N}(\alpha)\mathrm{N}(\beta)$. However, p is a prime so $\mathrm{N}(\alpha) = p = \mathrm{N}(\beta)$. So if $\alpha = a + bi$, then $p = a^2 + b^2$.

Now let us prove the claim:
If $p \equiv 1 \mod 4$, then -1 is a square $\bmod p$. Now recall that $\mathbb{F}_p^\times$ is cyclic of order $p - 1$. Then $u^{\frac{p-1}{2}} \equiv -1 \bmod p$ for a generator u of $\mathbb{F}_p^\times$. So if $p \equiv 1 \mod 4$, then $x^2 = -1$ has a solution $\bmod p$. Let n be such that $n^2 \equiv -1 \mod p$, so that $n^2 + 1 \equiv 0 \mod p$. But then $(n + i)(n - i) \equiv 0 \mod p$. If p was irreducible, p should divide either $n - i$ or $n + i$ in $\mathbb{Z}[i]$. However, the coefficient of i in $n \pm i$ is ± 1, hence this cannot happen. □

1.2 Diophantine Equations

Fermat once wrote: *"I can prove by a rigorous method that 25 is the only integer square that is less than a cube by 2."* He is claiming the equation $y^2 = x^3 - 2$ has no solution in integers other than $x = 3$ and $y = \pm 5$. Euler gave the first (rigorous) proof using arithmetic in $\mathbb{Z}[\sqrt{-2}]$. In this ring the equation becomes:

$$y^2 + 2 = x^3 = (y + \sqrt{-2})(y - \sqrt{-2}).$$

We will use

1. $\mathbb{Z}[\sqrt{-2}]$ is a UFD.
2. $\mathbb{Z}[\sqrt{-2}]^\times = \{\pm 1\}$.
3. $\gcd(y + \sqrt{-2}, y - \sqrt{-2}) = 1$.

Remark. Note that any solution $(x, y) \in \mathbb{Z}^2$ must have x odd. But if x is odd, y must also be odd.

Now

$$x^3 = (y + \sqrt{-2})(y - \sqrt{-2}).$$

Since the left hand side of this equation is a cube, the factors are relatively prime and because $\mathbb{Z}[\sqrt{-2}]$ is a UFD, each factor is a cube up to units. The only units are ± 1 and they are cubes themselves, so

$$\begin{aligned} y + \sqrt{-2} &= (a + b\sqrt{-2})^3 \\ &= (a^3 - 6ab^2) + (3a^2b - 2b^2)\sqrt{-2} \end{aligned}$$

for some $a, b \in \mathbb{Z}$. This in turn implies that

$$3a^2b - 2b^3 = b(3a^2 - 2b^2) = 1.$$

So we get $b = \pm 1$. If $b = 1$, then $a = \pm 1$ gives is a solution. If $b = -1$, there is no solution.

Check that $(a, b) = (\pm 1, 1)$ leads to Fermat's solution.
So the moral we draw from this story is:

Moral #1: *Sometimes to answer a question in $\mathbb{Z}$, it helps to look at a larger ring.*

Let us now look at another example:

Example 1.4. Find all integer solutions of $y^2 = x^3 - 26$.

We see that

$$(y + \sqrt{-26})(y - \sqrt{-26}) = x^3 \quad \text{and} \quad \mathbb{Z}[\sqrt{-26}]^\cdot = \{\pm 1\}.$$

So we get

$$\begin{aligned} y + \sqrt{-26} &= (a + b\sqrt{-26})^3 \\ &= (a^3 - 26 \times 3ab^2) + (3a^2b - 26b^3)\sqrt{-26}. \end{aligned}$$

Thus $(3a^2 - 26b^2)b = 1$, hence $b = 1, a = \pm 3$ and so $y = \pm 207, x = 35$. But this misses the trivial solution $x = 3, y = \pm 1$!

Thus, we observe:

Moral #2: *To apply Moral #1 and use a larger ring, we should understand the structure of the larger ring.*

Example 1.5. Now we look at

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

We get

$$\begin{aligned} x^3 &= y^2 + 3 \\ &= (y + \sqrt{-3})(y - \sqrt{-3}). \end{aligned}$$

But $\mathbb{Z}[\sqrt{-3}]$ is not a UFD! However, keeping Kronecker-Weber in mind, $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\rho)$, where ρ is the primitive 3rd root of unity $\frac{-1+\sqrt{-3}}{2}$. So $\mathbb{Z}[\sqrt{-3}] \subset \mathbb{Z}[\rho]$ and the latter is a UFD! However,

$$\mathbb{Z}[\rho]^\times = \{\pm 1, \pm\rho, \pm\rho^2\}.$$

As an exercise: $\gcd(y + \sqrt{-3}, y - \sqrt{-3}) = 1$, so $y \pm \sqrt{-3}$ are both cubes up to units. Hence,

$$y + \sqrt{-3} = y + 1 + 2\rho = \rho^k(a + b\rho)^3$$

for some $a, b \in \mathbb{Z}$ and $k \in \{0, 1, 2\}$. Now if $k = 0$:

$$\begin{aligned} y + 1 + 2\rho &= (a + b\rho)^3 \\ &= a^3 + 3a^2b\rho + 3ab\rho^2 + b^3 \\ &= (a^3 + b^3 - 3ab^2) + (3a^2b - 3ab^2)\rho. \end{aligned}$$

The coefficient of ρ is $3ab(a - b)$. But then $3ab(a - b) = 2$, so there is no solution.

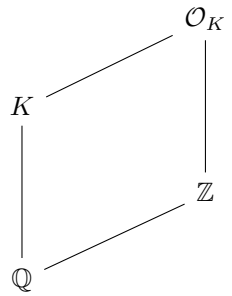
If $k = 1$, then $(y + 1 + 2\rho) = \rho(a + b\rho)^3 = \cdots \Rightarrow a^3 + b^3 - 3a^2b = 2$. If we look at this $\mod 4$ we see there is no solution by checking all possible values.

So the next moral is:

Moral #3: *The "most obvious" extension ring might not be the right ring! We need to understand and work with the "right" ring.*

In the last example, non-trivial units complicated it a bit.

Later we will systematically study the ring of integers $\mathcal{O}_K$ (and its units) of a number field K, which is an extension of $\mathbb{Z}$:



Example 1.6. Let us now look at the equation

$$y^2 = x^3 + 2.$$

We get:

$$y^2 - 2 = x^3 = (y + \sqrt{2})(y - \sqrt{2}).$$

Now the ring $\mathbb{Z}[\sqrt{2}]$ is a UFD, but the unit group is infinite: $\mathbb{Z}[\sqrt{2}]^\times = \{\pm 1\} \times (1+\sqrt{2})^n$. Set $\varepsilon = 1+\sqrt{2}$. Then we get:

$$y + \sqrt{2} = \pm \varepsilon^j (a + b\sqrt{2})^3$$

for some $a, b \in \mathbb{Z}$ and $j = 0, 1, 2$. The case $j = 0$ is as easy as before. If $j = 1$, we get

$$a^3 + 6ab^2 + 3a^2 b + 2b^3 = \pm 1.$$

The obvious solutions for this equation are $a = \pm 1, b = 0$. But are there others? This actually is a tough question.

So, **Moral # 4** *is units can cause complications. So we should understand them!*

1.3 Algebraic Numbers

Definition 1.7. Let K be a field extension of $\mathbb{Q}$. If K is a finite extension (hence algebraic) of $\mathbb{Q}$, then we call K an *algebraic number field*. The elements in K are called *algebraic numbers*. Any such x satisfies a monic polynomial equation

$$x^n + a_{n-1} + \cdots + a_0 = 0 \quad \text{with } a_i \in \mathbb{Q}.$$

If the coefficients of this polynomial are all in $\mathbb{Z}$, then x is called an *algebraic integer*.

It is not obvious that if α, β are algebraic numbers (integers), then $\alpha + \beta$, $\alpha\beta$ are also algebraic numbers (integers).

Example 1.8.

$$\begin{aligned} x &= \sqrt{2} + \sqrt{5} \\ x^2 &= 2 + 5 + 2\sqrt{10} \\ x^2 - 7 &= 2\sqrt{10} \\ (x^2 - 7)^2 &= 40 \end{aligned}$$

On the other hand, take $x = 2^{1/205} + 5^{1/417}$. To see if x satisfies a polynomial with integer coefficients with the previous method is not optimal. We need a better method. We first look at the case of algebraic numbers.

Warning! If α, β are algebraic integers, it is not always the case that α/β is an algebraic integer.

Example 1.9. The number $\frac{1}{\sqrt{2}}$ is not an algebraic integer. If it was, then there would exist $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z}$ such that

$$\left(\frac{1}{\sqrt{2}}\right)^n + a_{n-1}\left(\frac{1}{\sqrt{2}}\right)^{n-1} + \cdots + a_0 = 0.$$

This implies $1 + a_{n-1}\sqrt{2} + \cdots + a_0\sqrt{2}^n = 0$ and further $(1 + 2a_{n-2} + 4a_{n-4} + \ldots) + \sqrt{2}(a_{n-1} + 2a_{n-3} + \ldots) = 0$. If $a_{n-1} + 2a_{n-3} + \cdots \neq 0$, then

$$\sqrt{2} = -\frac{(1 + 2a_{n-2} + \ldots)}{(a_{n-1} + \ldots)} \in \mathbb{Q}$$

the right-hand side is a rational number as it is the quotient of integers, but this is a contradiction since $\sqrt{2}$ is not rational.

On the other hand, if $a_{n-1} + \cdots = 0$, then $1 + 2a_{n-2} + \cdots = 0$, but the left hand side is odd, which is also a contradiction.

Proposition 1.10. *Let L/K be a field extension. If $\alpha, \beta \in L$ are algebraic over K, then so are $\alpha + \beta$ and $\alpha\beta$.*

Proof. If α, β are algebraic over K, they satisfy polynomials of degree d, d', with $\deg \min_K(\alpha) = d$ and $\deg \min_K(\beta) = d'$, where $\min_K$ denotes the minimal polynomial of the respective element. Now we get that

$$K[\alpha, \beta] = \left\{ \sum c_{ij} \alpha^i \beta^j \mid c_{ij} \in K \right\}$$

is finite dimensional over K. So if $x \in K[\alpha, \beta]$, then $1, x, \ldots, x^{n+1}$ are linearly dependent and hence we get a polynomial equation for them. This holds in particular for $\alpha + \beta, \alpha\beta \in K[\alpha, \beta]$. □

The idea we use for integrality is due to Dedekind. He looks at the integral case by "linearizing" the problem, which led to the definition of a module.

2 Integrality

From now on all rings are commutative with 1.

Definition 2.1 (Elements integral over a ring)**.** Let R be a ring and A a subring of R. An element $x \in R$ is called *integral over* A if x is a root of a monic polynomial with coefficients in A, i.e. there exist $a_0, \dots, a_{n-1} \in A$ such that

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0.$$

Example 2.2. 1. A number $x \in \mathbb{C}$ is integral over $\mathbb{Q}$ if and only if x is an algebraic number.

2. An element $x \in \mathbb{C}$ is integral over $\mathbb{Z}$ if and only if x is an algebraic integer.

3. If $A = K$ and $R = L$, where both are fields, then $x \in L$ is integral over K if and only if x is algebraic over K.

The next theorem is about the linearization we are looking for.

Theorem 2.3. *Let $A \subset B$ be an extension of rings. Then the following are equivalent:*

1. *An element $x \in B$ is integral over A.*
2. *The ring $A[x]$ is finitely generated as an A-module.*
3. *There exists a subring R of B which contains A and x which is a finitely generated A-module.*

Proof. We will show $1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 1$. The implication $2 \Rightarrow 3$ is trivial, since we can just take $R = A[x]$, which is finitely generated by assumption. So let us show $1 \Rightarrow 2$:

Let $x \in B$ be integral over A. Then $A[x]$ is generated by x^k, $k \geq 0$. Since x is integral over A, there exist $a_0, \dots, a_{n-1}$ such that

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0.$$

Let M be the A-submodule generated by $1, x, \dots, x^{n-1}$. Clearly $x^n = -a_{n-1}x^{n-1} - \cdots - a_0 \in M$. By induction one can show that x^j for any $j \geq n$ can be written in terms of $1, x, \dots, x^{n-1}$ and hence $x^j \in M$. This implies $A[x] = M$ and hence $A[x]$ is finitely generated.

Next, we look at $3 \Rightarrow 1$:

Let R be a finitely generated A-module which contains A and x. Let $\omega_1, \dots, \omega_n$ be generators of R, i.e.

$$R = A\omega_1 + \cdots + A\omega_n, \text{ with } \omega_i \in R.$$

By assumption $x \in R$, so for any $i = 1, \dots, n$, $x\omega_i$ is also in R. Therefore we can write each $x\omega_i$ in terms of the generators:

$$x\omega_i = \sum_{j=1}^{n} a_{ij}\omega_j \text{ with } a_{ij} \in A.$$

Then we get

$$\sum_{j=1}^{n} (\delta_{ij}x - a_{ij})\omega_j = 0$$

and so

$$\begin{pmatrix} x - a_{11} & & \dots & -a_{1n} \\ \vdots & x - a_{22} & \dots & \vdots \\ \vdots & & \ddots & \vdots \\ -a_{n1} & \dots & \dots & x - a_{nn} \end{pmatrix} \begin{pmatrix} \omega_1 \\ \vdots \\ \vdots \\ \omega_n \end{pmatrix} = 0. \tag{1}$$

Let $M = (\delta_{ij}x - a_{ij})$ and $M^{adj} = (m_{ij})$ be its adjunct matrix, where $m_{ij} = (-1)^{i+j} \det M^{ij}$ and M^{ij} is the ij-th minor of M. Then Cramer's rule gives

$$M^{adj}M = \begin{pmatrix} \det M & & & \\ & \ddots & & 0 \\ & & \ddots & \\ 0 & & & \det M \end{pmatrix}.$$

If we multiply (1) by M^{adj}, then

$$\begin{pmatrix} \det M & & \\ & \ddots & \\ & & \det M \end{pmatrix} \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix} = 0,$$

which implies $(\det M)\omega_i = 0$ for all i. Hence $(\det M)r = 0$ for all $r \in R$, in particular for $r = 1$. So $\det M = 0$.

But note

$$\det M = \prod_{i=1}^{n}(x - a_{ii}) + g(x),$$

where g is a polynomial not necessarily monic, but $\deg g < n$. Hence $\det M$ is a monic polynomial with coefficients in A that has x as a root. So x is integral over A. □

Note that the end of the proof could be also be done slightly differently: Suppose $\tilde{M} = (a_{ij})$, then $P \coloneqq \det\left(\tilde{M} - \lambda \operatorname{Id}\right)$ is the characteristic polynomial of $\tilde{M}$ and has coefficients in R. Now clearly x is an eigenvalue of M and hence $P(x) = 0$.

Remark. The proof of 3. ⇒ 1. gives a method called "determinant method" to find a polynomial with integer coefficients an integral number satisfies.

1.10.2019

Proposition 2.4. *Finitely many $b_1, \ldots, b_n \in B$ are all integral over A if and only if $A[b_1, \ldots, b_n]$ is finitely generated as an A-module.*

Proof. By induction, exercise. □

Note: This says that any b in $A[b_1, \ldots, b_n]$ is also integral over A.

Corollary 2.5. *If $b_1, b_2 \in B$ are both integral over A, so are their sum and product.*

Corollary 2.6. *Let $A \subset B \subset C$ be two ring extensions of A. If C is integral over B and B is integral over A, then C is integral over A.*

Proof. Exercise. (Neukirch Prop. 2.4.). □

Definition 2.7. Let $A \subset B$ be rings.

1. We say B is *integral over* A if every $b \in B$ is integral over A.
2. Let $\overline{A} = A^B \coloneqq \{b \in B \mid b \text{ integral over } A\}$. Then A^B is called the *integral closure* of A in B.
3. The ring A is called *integrally closed in* B if $A^B = A$. (Be careful, integral closure must be with respect to an ambient ring)

Lemma 2.8. *Let $A \subset B$ be rings and A^B the integral closure of A in B. Then A^B is a subring of B and it is integrally closed in B.*

Proof. Exercise. □

Since our main interest lies in number fields and their ring of integers, we restrict ourselves to the case of integral domains and fields.

Proposition 2.9. *Let B be an integral domain and A a subring of B such that B is integral over A. Then B is a field if and only if A is a field.*

Proof. ($\Leftarrow$) Suppose A is a field and let $b \in B, b \neq 0$. Then b is integral over A, which implies $A[b]$ is a finitely generated A-module. Now consider the map $A[b] \to A[b]$, $y \mapsto by$. It is a linear transformation of $A[b]$ and it is injective because A is a domain and $b \neq 0$. Then it is also surjective, since $A[b]$ is finite dimensional over A. This implies that there exists $b' \in A[b] \subset B$ such that $bb' = 1$ and hence B is a field.

($\Rightarrow$). Suppose B is a field and $a \in A \setminus \{0\}$. Then there exists an inverse $a^{-1} \in B$. Since B is integral over A, there exist $c_0, \ldots, c_{n-1} \in A$ such that

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

Hence

$$a^{-1} + c_{n-1} + c_{n-2}a + \cdots + c_0 a^{n-1} = 0$$

and so $a^{-1} = -(c_{n-1} + c_{n-2}a + \cdots + c_0 a^{n-1}) \in A$. □

For algebraic number theory the case where A is an integral domain, K is its field of fractions and L is an algebraic extension of K is important. In particular $A = \mathbb{Z}$, $K = \mathbb{Q} = \mathrm{Quot}(\mathbb{Z})$ and L a finite extension of $\mathbb{Q}$.

Definition 2.10. Let A be an integral domain, and let $K = \mathrm{Quot}(A)$ the field of fractions of A. Then the integral closure A^K of A in K is called the *normalization of A*. The ring A is simply called integrally closed or normal if $A^K = A$, i.e. if $x \in K$ is integral over A, then $x \in A$.

Example 2.11. The ring of integers $\mathbb{Z}$ is integrally closed.

Proposition 2.12. *Any UFD is integrally closed.*

Proof. Let A be a UFD and K its field of fractions. Let $x \in K \setminus \{0\}$ and write $x = \frac{a}{b}$ with $a, b \in A$ and $b \neq 0$. We may assume $(a, b) = 1$. If x is integral over A, then there exist $c_0, \ldots, c_{n-1} \in A$ such that

$$x^n + c_{n-1}x^{n-1} + \cdots + c_0 = 0,$$

i.e.

$$\left(\frac{a}{b}\right)^n + c_{n-1}\left(\frac{a}{b}\right)^{n-1} + \cdots + c_0 = 0.$$

But this implies that $a^n + c_{n-1}a^{n-1}b + \cdots + c_0 b^n = 0$, which we can rewrite as

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

so

$$a^n + bc = 0, \quad \text{for some } c \in A$$

Now this means that any prime element that divides b also divides a, because we are in a UFD. By assumption $(a, b) = 1$ and so b is a unit and hence $x \in A$. □

Corollary 2.13. *Every PID is integrally closed.*

Example 2.14. We have that $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{Q}(i)$ and $\mathbb{Z}^{\mathbb{Q}} = \mathbb{Z}$ and $\mathbb{Z}^{\mathbb{Q}(i)} = \mathbb{Z}[i]$.

Proposition 2.15. *Let A be an integrally closed domain and $K = Quot(A)$. Let L be a finite extension of K and $B = A^L$. Then every element $x \in L$ is of the form $x = \frac{b}{a}$ with $b \in B$ and $a \in A \setminus \{0\}$.*

Proof. Let $x \in L \setminus \{0\}$. Then x is algebraic over K (due to the assumption that the extension is finite), i.e. there exist $\frac{c_i}{d_i} \in K$, $i = 1, \ldots, n$ with $c_i, d_i \in A$ and $d_i \neq 0$ such that

$$x^n + \frac{c_1}{d_1}x^{n-1} + \cdots + \frac{c_n}{d_n} = 0.$$

Let $a \coloneqq d_1 d_2 \ldots d_n \in A$. Then

$$a^n x^n + a^{n-1} d_1' c_1 x^{n-1} + \cdots + a^{n-1} d_n' c_n = 0,$$

where $d_i' = \frac{d_1 d_2 \ldots d_n}{d_i}$. Hence

$$(ax)^n + (ax)^{n-1} d_1' c_1 + \cdots + a^{n-1} d_n' c_n = 0,$$

which is a polynomial equation with coefficients in A. This implies ax is integral over A and so $ax = b$ for some $b \in B$. □

Proposition 2.16. *Let A be an integral domain which is integrally closed in its field of fractions K and L/K a finite extension. If $x \in L$ is integral over A, then its minimal polynomial over K has coefficients in A, i.e. all conjugates of x over K are also integral over A.*

Proof. Let $f \in K[x]$ be the minimal polynomial of x over K. Since x is integral over A, there exists a monic polynomial $g(x) \in A[x]$ such that $g(x) = 0$. Hence $f | g$ in $K[x]$. Let M be the splitting field of f over K, i. e. the field generated by the roots of f, and A^M be the integral closure of A in M. Then $K \cap A^M$ is integral over A, but since A is integrally closed in K, we get that $K \cap A^M = A$. The conjugates of x are also roots of g, hence they are integral over A and so belong to A^M. The coefficients of f are up to sign symmetric polynomial in the conjugates of x. Hence the coefficients of f are in $A^M \cap K = A$. □

Remark.

1. An element $x \in L$ is integral over A if and only if its minimal polynomial has coefficients in A.
2. Let $\Omega = \{z \in \mathbb{C} \mid z \text{ is integral over } \mathbb{Z}\}$ be the set of all algebraic integers. Then $\mathbb{Q} \cap \Omega = \mathbb{Z}$, since $\mathbb{Q} \cap \Omega \subset \mathbb{Z}^{\mathbb{Q}} = \mathbb{Z}$.
3. Every algebraic number z is of the form a/b, where b is an algebraic integer and a and ordinary integer, which follows from 2.15 applied to $A = \mathbb{Z}$, $K = \mathbb{Q}$ and $L = \mathbb{Q}(z)$, and thus $B = \mathbb{Z}^{\mathbb{Q}} = \mathbb{Z}$. Note that we needed the extension of $\mathbb{Q}$ to be a finite extension, that is why z must be algebraic.

Our next goal is to determine the structure of the integral closure $\mathbb{Z}^L$ of $\mathbb{Z}$ in a finite extension $L/\mathbb{Q}$. We denote $\mathbb{Z}^L$ by $\mathcal{O}_L$ and call it the *ring of integers of L*.

2.1 Quadratic fields

Definition 2.17. An extension L of degree 2 over $\mathbb{Q}$ is called a *quadratic field*. Similarly, if $[L : \mathbb{Q}] = 3, 4, 5, \ldots$ L is called a cubic, quartic, quintic,... field.

Lemma 2.18. *Every quadratic field is of the form $\mathbb{Q}(\sqrt{d})$ for a unique square-free integer d.*

Proof. We first show that every quadratic field is generated by the square root of a rational number. Suppose K is a quadratic field. Let $\alpha \in K \setminus \mathbb{Q}$. Then $1, \alpha$ are $\mathbb{Q}$-linearly independent but $1, \alpha, \alpha^2$ are $\mathbb{Q}$-linearly dependent. Therefore we have the relation

$$\alpha^2 + b\alpha + c = 0, \quad b, c \in \mathbb{Q}, c \neq 0$$

Now let $\beta \coloneqq \alpha + \frac{b}{2}$. Then solving the above quadratic equation using the quadratic formula, we can re-write β as

$$\beta = \frac{\sqrt{b^2 - 4c}}{2}$$

Then notice that

$$K = \mathbb{Q}(\alpha) = \mathbb{Q}(\beta) = \mathbb{Q}(\sqrt{b^2 - 4c}).$$

Therefore K is obtained from $\mathbb{Q}$ by adjoining the square root of a rational number. Let us write this rational number $b^2 - 4c$ as $\frac{p}{q}$ for coprime integers p and q. Then

$$\sqrt{b^2 - 4c} = \sqrt{\frac{p}{q}} = \frac{\sqrt{pq}}{q}.$$

So we can further deduce that

$$K = \mathbb{Q}(\sqrt{pq}).$$

We can also assume that the integer pq is square-free since suppose we have a non-square-free integer $d = e^2 f$, then $\sqrt{d} = e\sqrt{f}$, thus $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{f})$. Therefore by letting $d = pq$ we have that

$$K = \mathbb{Q}(\sqrt{d}).$$

Conversely, suppose d is a square-free integer. Then $\sqrt{d}$ is irrational (by a similar argument for showing $\sqrt{2}$ is irrational), therefore $\mathbb{Q}(\sqrt{d}) \neq \mathbb{Q}$. The degree of $\mathbb{Q}(\sqrt{d})$ is degree 2 since $1, \sqrt{d}$ form a $\mathbb{Q}$-basis. For uniqueness, suppose by way of contradiction that $d \neq d'$ square-free integers, but $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{d'})$. Then we can write

$$\sqrt{d'} = x + y\sqrt{d}$$

for some $x, y \in \mathbb{Q}$. Squaring both sides, we get

$$d' = x^2 + dy^2 + 2xy\sqrt{d}$$

Suppose $xy \neq 0$, this would imply that $\sqrt{d} \in \mathbb{Q}$. If $y = 0$, then $\sqrt{d'} = x \in \mathbb{Q}$. So $x = 0$ and $d' = dy^2$. Since d' is square-free by assumption it follows that $y = 1$ and hence $d = d'$. □

Recall from field theory:

Theorem 2.19. *Let F be a finite field or a field of characteristic 0. If K/F is a finite extension, then there exists a primitive element $\alpha \in K$, i.e. $K = F(\alpha)$.*

We should think of F as being $\mathbb{Q}$.

Theorem 2.20. *Let K be a quadratic field. That is, $K = \mathbb{Q}(\sqrt{d})$, where d is square-free. Now Let $\mathcal{O}_K = \{x \in K \mid x \text{ integral over } \mathbb{Z}\}$ be the ring of integral elements over $\mathbb{Z}$. Then*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z} + \mathbb{Z}\sqrt{d} = \mathbb{Z}[\sqrt{d}], & d \not\equiv 1 \mod 4 \\ \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{d}}{2} = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right], & d \equiv 1 \mod 4. \end{cases}$$

The proof will show us that that we can write them as

$$\mathcal{O}_K = \begin{cases} \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}, & d \not\equiv 1 \mod 4 \\ \{\frac{1}{2}(u + v\sqrt{d}) \mid u, v \in \mathbb{Z}, u \equiv v \mod 2\}, & d \equiv 1 \mod 4. \end{cases}$$

Proof. Let $x \in \mathcal{O}_K$, thus x is a root of some monic polynomial with integer coefficients. The minimal polynomial of x in $K/\mathbb{Q}$ is of degree 2 with integer coefficients. Let $\sigma(x)$ be the other root of the minimal polynomial. Then $\sigma(x) \in \mathcal{O}_K$. We also have $x + \sigma(x), x\sigma(x) \in \mathcal{O}_K$.

Let us write $x = a + b\sqrt{d}$ with $a, b \in \mathbb{Q}$. Then we have $\sigma(x) = a - b\sqrt{d}$. Then $x + \sigma(x) = 2a \in \mathbb{Q} \cap \mathcal{O}_K = \mathbb{Z}$ and $x\sigma(x) = a^2 - b^2 d \in \mathbb{Q} \cap \mathcal{O}_K = \mathbb{Z}$ (using Proposition 2.12).

So $x = a + b\sqrt{d} \in \mathcal{O}_K$ implies $2a \in \mathbb{Z}$ and $a^2 - b^2 d \in \mathbb{Z}$. From $a^2 - b^2 d \in \mathbb{Z}$ we get $(2a)^2 - (2b)^2 d \in \mathbb{Z}$. Since $2a \in \mathbb{Z}$ and d is squarefree, it follows that $2b$ has denominator 1. Hence $2b \in \mathbb{Z}$. Let $2a = u$ and $2b = v$. Then we get $u^2 - v^2 d \in 4\mathbb{Z}$ and $u, v \in \mathbb{Z}$. Suppose $d \equiv 2 \mod 4$. This yields:

u	even	even	odd	odd
v	even	odd	even	odd
$u^2 - v^2 d$	0	2	1	3

where the last row are the values $\mod 4$. Similarly, if $d \equiv 3 \mod 4$, then u and v are both even. In these cases, $a, b \in \mathbb{Z}$ and $x \in \mathbb{Z} + \sqrt{d}\mathbb{Z}$.

Now if $d \equiv 1 \mod 4$, we get:

u	even	even	odd	odd
v	even	odd	even	odd
$u^2 - v^2 d$	0	3	1	0

where again the last row is $\mod 4$. So if $d \equiv 1 \mod 4$, both u and v have the same parity. Hence

$$\mathcal{O}_K = \left\{ \frac{1}{2}(u + vd) \mid u, v \in \mathbb{Z} \text{ of same parity} \right\}.$$

Now we want to show that if $d \equiv 1 \mod 4$, then $\{1, (1+\sqrt{d})/2\}$ is a $\mathbb{Z}$-basis for $\mathcal{O}_K$.

If u, v are both even, then

$$\frac{u + v\sqrt{d}}{2} = a + b\sqrt{d} = (a-b) \cdot 1 + 2b\left(\frac{1+\sqrt{d}}{2}\right) \in \mathbb{Z} + \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right].$$

If they are both odd, then $u - v \in 2\mathbb{Z}$ and

$$\frac{u + v\sqrt{d}}{2} = \frac{u-v}{2} + v\left(\frac{1+\sqrt{d}}{2}\right) \in \mathbb{Z} + \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right].$$

□

In the proof we used that $x\sigma(x), x + \sigma(x) \in \mathbb{Z}$ to find the structure of $\mathcal{O}_K$ for $K = \mathbb{Q}(\sqrt{d})$.

2.2 The Structure of the Ring of Integers

Our next goal is to determine, for A an integrally closed integral domain, and K a finite extension of $\mathrm{Quot}(A)$, the structure of $\mathcal{O}_K = A^K$. This will allow us to generalize the previous result on quadratic fields to arbitrary number fields $K/\mathbb{Q}$. We will show that $\mathcal{O}_K$ is a $\mathbb{Z}$-module of rank $n = [K : \mathbb{Q}]$. For this we will use the following:

Suppose A, B, C are $\mathbb{Z}$-modules. If A, C are free of rank n and B is such that $A \subset B \subset C$, then B is also free of rank n, which comes from the theory of finitely generated modules over a PID.

We fix F an arbitrary field and K/F a finite extension of fields with $[K : F] = n$. In linear algebra we defined the trace, determinant and the characteristic polynomial of an endomorphism (linear transformation as K-vector spaces) $m \colon L \to L$. If we choose a basis $\{c_i\}_{i=1}^n$ of K/F, let $(a_{ij})_{1 \le i,j \le n}$ be the matrix m with respect to this basis. Then, $\operatorname{Tr} m = \sum a_{ii}$, $\det m = \det(a_{ij})$ and the characteristic polynomial of m is $\det(t \cdot \delta_{ij} - a_{ij})$.

Definition 2.21. The trace and norm of and element $\alpha \in K$ are defined as the trace and determinant of the multiplication map

$$\begin{aligned} m_\alpha \colon K &\to K \\ y &\mapsto y\alpha \end{aligned}$$

that is

$$\mathrm{Tr}_{K/F}(\alpha) \coloneqq \mathrm{Tr}(m_\alpha) \quad \text{and} \quad \mathrm{N}_{K/F}(\alpha) \coloneqq \det(m_\alpha).$$

If the characteristic polynomial f_α of m_α is $\det(t \cdot \mathrm{Id} - m_\alpha) = t^n - a_1 t^{n-1} + \cdots + (-1)^n a_n \in F[t]$, then $a_1 = \mathrm{Tr}_{K/F}(\alpha)$ and $a_n = \mathrm{N}_{K/F}(\alpha)$.

We get homomorphisms $\mathrm{Tr}_{K/F} \colon K \to F$ and $\mathrm{N}_{K/F} \colon K \to F$.

Recall from field theory: Let K/F be a finite separable extension of degree d and let φ be an embedding of F into a fixed algebraic closure $\overline{F}$. Then φ extends to exactly d embeddings of K into $\overline{F}$ that fix F, i.e. there are exactly d embeddings $\sigma \colon K \to \overline{F}$ such that $\sigma|_F = \varphi$. In particular, if $\varphi = \mathrm{Id}$, then there are exactly d F-embeddings of K into $\overline{F}$.

Theorem 2.22. *Let K be a field of characteristic 0 or a finite field (thus any algebraic extension is separable) and L an algebraic extension of K of degree n. Let $\sigma \colon L \to \overline{K}$ vary over the different K-embeddings of L into an algebraic closure. Then for all $\alpha \in L$:*

1. $f_\alpha(t) = \prod_{\sigma \in \mathrm{Hom}(L, \overline{K})} (t - \sigma(\alpha))$, *where f_α is the characteristic polynomial of m_α*
2. $\mathrm{Tr}_{L/K}(\alpha) = \sum_{\sigma \in \mathrm{Hom}(L, \overline{K})} \sigma(\alpha)$
3. $\mathrm{N}_{L/K}(\alpha) = \prod_{\sigma \in \mathrm{Hom}(L, \overline{K})} \sigma(\alpha)$

Proof. We first look at the case $L = K(\alpha)$. Then $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a basis of L/K. Let $p_\alpha(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_0$ be the minimal polynomial of α over K. Consider the multiplication map

$$\begin{aligned} m_\alpha \colon L &\to L \\ y &\mapsto y\alpha. \end{aligned}$$

If we write y in terms of the basis elements

$$y = k_0 + k_1\alpha + \cdots + k_{n-1}\alpha^{n-1}$$

and using that α is a root of its minimal polynomial to write

$$\alpha^n = -a_0 - a_1\alpha - \cdots - a_{n-1}\alpha^{n-1}.$$

Then we can obtain the matrix of $m_\alpha \colon L \to L$ written with respect to this basis as:

$$M = \begin{pmatrix} 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & \ldots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & -a_{n-1} \end{pmatrix}.$$

This can be checked by checking the basis elements get sent to where they are supposed to.

So, $\mathrm{Tr}_{L/K}(\alpha) = -a_{n-1}$ and $\mathrm{N}_{L/K} = \det M = (-1)^n a_0 \in K$. Note that, by definition of the conjugates/minimal polynomial,

$$\det(t \cdot \mathrm{Id} - m_\alpha) = p_\alpha(t) = \prod_{\varphi \in \mathrm{Hom}(K(\alpha), \overline{K})} (t - \varphi(\alpha)).$$

In the general case L/K let $\alpha \in L$ and consider the tower $K \subset K(\alpha) \subset L$. We will see that the characteristic polynomial $f_\alpha(t)$ of m_α is the dth power of $p_\alpha(t)$ $(= \min_K(\alpha))$, where $d = [L : K(\alpha)]$.

Indeed, if $1, \alpha, \ldots, \alpha^{m-1}$ is a basis of $K(\alpha)/K$ and if $\beta_1, \ldots, \beta_d$ is a basis of $L/K(\alpha)$, then $\{\beta_i \alpha^j \mid i = 1, \ldots, d, j = 0, \ldots, m-1\}$ is a basis of L/K. In this basis the matrix of m_α is as follows:

$$\begin{pmatrix} M & & & \\ & M & & \\ & & \ddots & \\ & & & M \end{pmatrix}.$$

Hence $f_\alpha(t) = p_\alpha(t)^d$.

Since each $\varphi \in \mathrm{Hom}(K(\alpha), \overline{K})$ extends to a homomorphism $\sigma\colon L \to \overline{K}$ in exactly $d = [L : K(\alpha)]$ ways, we get that

$$\prod_{\varphi \in \mathrm{Hom}_K(K(\alpha), \overline{K})} (t - \varphi(\alpha))^d = \prod_{\sigma \in \mathrm{Hom}_K(L, \overline{K})} (t - \sigma(\alpha)).$$

□

Remark. In field theory, if $K = \mathbb{Q}$ and $L/\mathbb{Q}$ is finite extension of degree n, there are exactly n distinct embeddings $\sigma\colon L \to \mathbb{C}$ that fix $\mathbb{Q}$. We know that $L = K(\alpha)$ for some primitive element α. Also if $p_\alpha(t) = (t-\alpha_1)\ldots(t-\alpha_n)$, where the α_i are the distinct conjugates of α, then each $\mathbb{Q}$-embedding $\sigma\colon L \to \mathbb{C}$ is uniquely determined by sending α to some α_i. That is, if $\beta \in L$, then β can be written as $\beta = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$ with $a_i \in \mathbb{Q}$. Then

$$\sigma_k\colon L \to \mathbb{C}, \quad \beta \mapsto a_0 + a_1\alpha_k + \cdots + a_{n-1}\alpha_k^{n-1}$$

are distinct for all $k = 1, \ldots, n$.

Definition 2.23. Let L be an algebraic number field with $[L : \mathbb{Q}] = n$ and $L = \mathbb{Q}(\alpha)$. Then $\mathbb{Q}(\alpha_1), \ldots, \mathbb{Q}(\alpha_n)$ are called the *conjugate fields of* L. Let $\beta_1 = \beta \in L$, then $\beta_k \coloneqq a_0 + a_1\alpha_k + \cdots + a_{n-1}\alpha_k^{n-1}$ are called the *conjugates of* β *relative to* L.

Example 2.24. Let $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Put $\alpha = \sqrt{2} + \sqrt{3}$, then $\min_\alpha(x) = x^4 - 10x^2 + 1 = (x + \sqrt{2} + \sqrt{3})(x - \sqrt{2} + \sqrt{3})(x - \sqrt{2} - \sqrt{3})(x + \sqrt{2} - \sqrt{3})$. Now let $\beta = 2\sqrt{3} \in L$. Check that $\beta = 11\alpha - \alpha^3$. Then the conjugates of β are:

$$\begin{aligned} \beta &= 11\alpha - \alpha^3 = 2\sqrt{3} \\ \beta_2 &= 11\alpha_2 - \alpha_2^3 = -2\sqrt{3} \\ \beta_3 &= 2\sqrt{3} \\ \beta_4 &= -2\sqrt{3} \\ &\cdot \end{aligned}$$

The characteristic polynomial of $\beta \in L$ is $(x - 2\sqrt{3})^2(x + 2\sqrt{3})^2 = \prod_\sigma (x - \sigma(\beta)) = (x^2 - 12)^2 = (\min_K(\beta))^2$.

Theorem 2.25. *Let $K \subset L \subset M$ be a tower of field extensions. Then for all $\alpha \in M$ we have $\mathrm{Tr}_{L/K}(\mathrm{Tr}_{M/L}(\alpha)) = \mathrm{Tr}_{M/K}(\alpha)$ and $\mathrm{N}_{L/K}(\mathrm{N}_{M/L}(\alpha)) = \mathrm{N}_{M/K}(\alpha)$.*

Proof. Exercise. □

3.10.2019

Last time: L/K finite algebraic extension. For $\alpha \in L$ we defined

$$\mathrm{Tr}_{L/K}(\alpha) \coloneqq \mathrm{Tr}(m_\alpha)$$

for

$$\begin{aligned} m_\alpha\colon L &\to L \\ y &\mapsto \alpha y \end{aligned}$$

and homomorphisms

$$\mathrm{Tr}_{L/K} : L \to K$$
$$\mathrm{N}_{L/K} : L^\times \to K^\times.$$

Now fix A an integrally closed integral domain, $K = \mathrm{Quot}(A)$, and L is a finite extension of K.

Proposition 2.26. *For all $x \in B = A^L$, we have*

1. $\mathrm{N}_{L/K}(x) \in A$
2. $\mathrm{Tr}_{L/K}(x) \in A$
3. $\mathrm{N}_{L/K}(x) \in A^\times$ *if and only if* $x \in B^\times$.

Proof. For 1. If $x \in A^L$, then $\sigma(x)$ (ranging over all K-embeddings $\sigma\colon L \to \overline{K}$) are all integral, hence

$$\mathrm{Tr}_{L/K}(x) = \sum \sigma(x)$$

is also integral, but is also in K, which means it is in $A^K = A$ (since A is integrally closed in its field of fractions). The same argument gives

$$\mathrm{N}_{L/K}(x) = \prod \sigma(x) \in A.$$

This establishes 1., and 2..

For 3., ($\Leftarrow$) The norm is multiplicative, as is evident from Theorem 2.22. Thus if $x \in B^\times$, i.e. there exists $y \in B^\times$ such that $xy = 1$, then $\mathrm{N}(xy) = N(x)\,\mathrm{N}(y) = N(1) = 1$ implies $\mathrm{N}(x) \in A^\times$.

($\Rightarrow$) Suppose $\mathrm{N}_{L/K}(x) \in A^\times$. Write $\mathrm{N}(x) = x \cdot \prod_{\sigma \neq Id} \sigma(x)$, thus $1 = x(\mathrm{N}(x))^{-1} \prod_{\sigma \neq Id} \sigma(x)$. Hence if $y \coloneqq \mathrm{N}(x)^{-1} \prod_{\sigma \neq Id} \sigma(x)$, then y is the inverse of x in L. Now $A^\times \ni (\mathrm{N}(x))^{-1}$ and $\prod_{\sigma \neq Id} \sigma(x)$ is integral and hence $y = x^{-1}$ is integral over A. So $x^{-1} \in A^L = B$. □

Example 2.27. Let $L/\mathbb{Q}$, $A = \mathbb{Z}$ and $B = \mathbb{Z}^L = \mathcal{O}_L$. If $x \in \mathcal{O}_L$ then $\mathrm{N}(x), \mathrm{Tr}(x) \in \mathbb{Z}$ for $x \in \mathcal{O}_L$.

Next we define the *discriminant* for L/K a separable extension of degree n. Let $\sigma_1, \ldots, \sigma_n : L \to \overline{K}$, and let $(\alpha_1, \ldots, \alpha_n)$ be any n-tuple in L. Then

Definition 2.28. The *discriminant* of $\alpha_1, \ldots, \alpha_n$ is defined to be

$$\mathrm{disc}(\alpha_1, \ldots, \alpha_n) = d(\alpha_1, \ldots, \alpha_n) \coloneqq (\det(\sigma_i(\alpha_j))_{0 \le i,j \le n})^2$$

where the σ_i varies over the n K-embeddings $L \to \overline{K}$.

Remark. The square is to make sure it does not depend on the order of the σ_i's and α_j's.

Example 2.29. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and $\alpha_1 = 1$, $\alpha_2 = \sqrt{2}$. $\alpha_3 = \sqrt{3}$, $\alpha_4 = \sqrt{2} + \sqrt{3}$. Then

$$\mathrm{disc}(\alpha_1, \ldots, \alpha_4) = \left(\det \begin{pmatrix} 1 & \sqrt{2} & \sqrt{3} & \sqrt{2}+\sqrt{3} \\ 1 & -\sqrt{2} & \sqrt{3} & -\sqrt{2}+\sqrt{3} \\ 1 & \sqrt{2} & -\sqrt{3} & \sqrt{2}-\sqrt{3} \\ 1 & -\sqrt{2} & -\sqrt{3} & -\sqrt{2}-\sqrt{3} \end{pmatrix} \right)^2.$$

Remark. Since we have the relation

$$\mathrm{Tr}_{L/K}(\alpha_i \alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i \alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j)$$

we have the matrix

$$(\mathrm{Tr}_{L/K}(\alpha_i \alpha_j))_{i,j} = (\sigma_k(\alpha_i))^t (\sigma_k(\alpha_j)) =: T^t T$$

and hence

$$\mathrm{disc}(\alpha_1, \ldots, \alpha_n) = \det\big((\mathrm{Tr}_{L/K}(\alpha_i \alpha_j))_{0 \le i,j \le n}\big).$$

(Recall that transposing a matrix does not change its determinant.)

Example 2.30. Let $L = K(\theta), [L : K] = n$, so $1, \theta, \ldots, \theta^{n-1}$ is a basis for L/K. Let us denote $\sigma_i\theta$ by θ_i (be careful to not confuse the θ's with superscripts with those with subscripts). Then

$$\operatorname{disc}(1, \theta, \ldots, \theta^{n-1}) = \left(\det \begin{pmatrix} 1 & \theta_1 & \theta_1^2 & \ldots & \theta_1^{n-1} \\ 1 & \theta_2 & \theta_2^2 & \ldots & \theta_2^{n-1} \\ \vdots & & & & \\ 1 & \theta_n & \theta_n^2 & \ldots & \theta_n^{n-1} \end{pmatrix} \right)^2$$

the inside of which is a Vandermonde matrix so we have that

$$\operatorname{disc}(1, \theta, \ldots, \theta^{n-1}) = \prod_{i<j} (\theta_i - \theta_j)^2 \neq 0.$$

Remark. The identity $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = \det\big((\operatorname{Tr}_{L/K}(\alpha_i\alpha_j))_{i,j}\big)$ implies $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) \in K$ and if $\alpha_1, \ldots, \alpha_n \in B$ then $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) \in A$, this is a consequence of Proposition 2.26.

Proposition 2.31. *Let L/K be a separable extension and $[L : K] = n$. The map*

$$\begin{aligned} L \times L &\to K \\ (x, y) &\mapsto \operatorname{Tr}_{L/K}(xy) \end{aligned}$$

is K-bilinear symmetric non-degenerate. Furthermore, if $\alpha_1, \ldots, \alpha_n$ is a basis then $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) \neq 0$.

Proof. The second statement follows immediately from the first. Indeed, if we show $\langle x, y\rangle := \operatorname{Tr}(xy)$ is non-degenerate, then since

$$\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = \det(\operatorname{Tr}(\alpha_i\alpha_j))$$

is simply the determinant of the matrix of this bilinear form with respect to the basis $\alpha_1, \ldots, \alpha_n$ we get that $\operatorname{disc}(\alpha_1, \ldots, \alpha) \neq 0$.

Here we need the fact that a bilinear form is non-degenerate if and only if its matrix w.r.t. a basis is invertible. It is enough to find a basis for which this is the case. Since L/K is finite separable let $L = K(\theta)$ (*Classical Primitive Element Theorem*). Take basis $1, \theta, \ldots, \theta^{n-1}$. The matrix of the bilinear form with respect to this basis is the Vandermonde matrix from above, and thus has non-zero determinant. The bilinearity is a direct consequence of the trace function being a linear operator.

Another argument: By way of contradiction, let $x \in L$ such that $\langle x, y\rangle = 0$ for all $y \in L$, i.e. $\operatorname{Tr}(xy) = 0$ for all $y \in L$, so the trace is zero on $xL = L$, i.e. $\operatorname{Tr}(\ell) = 0$ for all $\ell \in L$ which is clearly not the case since $\operatorname{Tr}(1) = n$. □

The next lemma will allow us to find an A-module of rank n contained in B.

Lemma 2.32. *Let $\{e_1, \ldots, e_n\}$ be a basis of L over K. Then there exists a K-basis $b_1, \ldots, b_n$ of L with $b_i \in B$.*

Proof. Recall that we have seen in Proposition (2.15) that any $\ell \in L$ can be written as

$$\ell = \frac{b}{a}, \qquad \text{with } b \in B \text{ and } a \in A.$$

So we can write $e_i = \frac{b_i}{a_i}$. Let $M = a_1 \cdots a_n \neq 0$, and $b_i' = Me_i \in B$. We can take $b_1', \ldots, b_n' \in B$ as a K-basis of L. □

Corollary 2.33. *There exists an A-module contained in B of rank n.*

Proof. Let $b_1, \ldots, b_n \in B$ be a basis of L/K as in the Lemma. Then $Ab_1 + \cdots + Ab_n \subset B$ is the A-module of rank n we are looking for. □

Remark. This corollary gives us an A-module sitting in B. If we find an A-module containing B of rank n, then we can use the squeeze theorem to conclude that B is an A-module of rank n when A is a PID.

Proposition 2.34. *Let $b_1, \dots, b_n \in B$ be a basis of L over K. Then the discriminant $d = \operatorname{disc}(b_1, \dots, b_n) \in A \setminus \{0\}$ and*

$$B \subset \frac{1}{d}(Ab_1 + \cdots + Ab_n).$$

Proof. Let $0 \neq y \in B$. Then $yb_i \in B$ for $i = 1, \dots, n$. Then

$$\operatorname{Tr}_{L/K}(yb_i) \in A.$$

Write

$$y = k_1 b_1 + \cdots + k_n b_n, \quad k_i \in K \quad \text{(using the } K\text{-basis)}$$
$$yb_i = k_1 b_1 b_i + \cdots + k_n b_n b_i \quad \text{(multiply } b_i \text{ on both sides)}$$
$$A \ni \operatorname{Tr}(yb_i) = \sum_{j=1}^{n} \operatorname{Tr}(b_j b_i) k_j$$

Call $x_i = \operatorname{Tr}(yb_i)$ then we have

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = (\operatorname{Tr}(b_j b_i))_{1 \leq i,j \leq n} \begin{pmatrix} k_1 \\ \vdots \\ k_n \end{pmatrix}$$

If we call the matrix $(\operatorname{Tr}(b_j b_i))_{i,j} = M$, recall that Cramer's rule gives us

$$M^{adj} M = (\det M) I.$$

Since $b_i \in B$, we get that $\operatorname{Tr}(b_i b_j) \in A$ (Proposition 2.26). Therefore the entries of M^{adj} are also in A. After multiplying the linear equation above by M^{adj} we get

$$M^{adj} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = (\det M) \begin{pmatrix} k_1 \\ \vdots \\ k_n \end{pmatrix}$$

but we know $\det M = \operatorname{disc}(b_1, \dots, b_n)$. That means

$$\begin{pmatrix} k_1 \\ \vdots \\ k_n \end{pmatrix} = \frac{1}{d} M^{adj} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

and thus each $k_i = \frac{a_i}{d}$ for some $a_i \in A$. Hence

$$B \subset \frac{1}{d}(Ab_1 + \cdots + A_n b_n).$$

□

We get the following corollary, which we state as a theorem:

Theorem 2.35. *Let A be a PID. Let $K = \operatorname{Quot}(A)$, L/K a finite separable extension, and $B = A^L$. Then B is a free A-module of rank $[L : K]$.*

Proof. Let $n = [L\colon K]$. Let $b_1, \dots, b_n \in B$ be a K-basis of L, then

$$Ab_1 + \cdots + Ab_n \subset B \subset \frac{1}{d}(Ab_1 + \cdots + Ab_n).$$

Since we know $Ab_1 + \cdots + A_n$ and $\frac{1}{d}(Ab_1 + \cdots + Ab_n)$ are free A-modules of rank n, B is also one. □

Corollary 2.36. *If $A = \mathbb{Z}$, then $\mathcal{O}_L$ is a free $\mathbb{Z}$-module of rank n, i.e. a free Abelian group of rank n.*

Remark. In a general situation a system of elements $\omega_1, \dots, \omega_r \in B$ such that each $b \in B$ can be written uniquely as a linear combination of $\omega_1, \dots, \omega_r$ with coefficients in A is called an *integral basis of B over A*. Note such a basis is automatically a basis of L/K and hence $r = n$, the details are left as an exercise.

The existence of such a basis of B says that B is a free A-module of rank n. BUT, recall that in general if M is an A-module, it is not always the case that M has a basis (if it does it is called free). Even if M is finitely generated, it does not have to have a basis. For example, take $\mathbb{Z}/n\mathbb{Z}$. This is obviously a finitely generated $\mathbb{Z}$-module since it is a finite ring. But it is not free since we cannot find a linearly independent basis. Another example: take $A = \mathbb{Z}[\sqrt{-5}]$ and let I be the ideal generated by the two elements 2 and $1 + \sqrt{-5}$. So as an A-module (the ideal) has a finite set of generators. Now $\{2, 1 + \sqrt{-5}\}$ spans I as an A-module, but this subset is linearly dependent: $2a + (1 + \sqrt{-5})b = 0$ has for example the solution $a = 1 + \sqrt{-5}, b = -2$. In fact any two x, y are linearly dependent by choosing $b = -y, a = x, ay + bx = 0$. If $x = y = 0$ then choose $a = 1 = b$. That means if I has a basis then it should have just one basis element x, i.e. $I = Ax$ is principal. But one can check that I is not principal. Hence I is finitely generated but has no basis, i.e. is not free. Also this shows that a submodule of a module might require more generators than the ambient module.

In general similar arguments show that for any commutative ring A and an ideal I which is not principal we get a module which does not have a basis. **But over a PID we do not have this issue**, we have the following theorem from algebra:

Theorem 2.37. *Let A be a PID, $K = \mathrm{Quot}(A)$. Let M be an A-module generated by $r \geq 1$ elements. Then*

1. *Every submodule M' of M is generated by r elements (possibly less).*
2. *If M is non-zero and free, say $M = A^{\oplus n}$, then such an n is unique and called the* rank *of M. If M is free, then every non-zero submodule $M' \subset M$ is also free of rank $q \leq n$. Moreover if $M' \neq 0$, then there exists a basis $\{e_1, \dots, e_n\}$ of M and non-zero elements $a_1, \dots, a_q \in A$ such that $\{a_1 e_1, \dots, a_q e_q\}$ is a basis of M' and $a_i | a_{i+1}$.*

In the case that M is contained in a K-vector space V and M spans V over K, then $n = \dim_K V$.

8.10.2019

Recall that last time we proved that for A a PID, B is a free A-module of rank $n = [L : K]$. In particular, for $A = \mathbb{Z}$ and L a number field, the ring of integers $\mathcal{O}_L = \mathbb{Z}^L$ is a finitely generated Abelian group of rank n, i. e. $\mathcal{O}_L = \mathbb{Z}\omega_1 + \dots + \mathbb{Z}\omega_n$. The elements $\omega_1, \dots, \omega_n$ are called an integral basis of $L/\mathbb{Q}$.

Now we know that $\mathcal{O}_L$ is a finitely generated Abelian group of rank n. But finding an integral basis for $\mathcal{O}_L$ is not at all trivial. We can get some help from the discriminant.

Proposition 2.38. *Let $\{b_1, \dots, b_n\}$ be an A-basis of $B = A^L$. Then $\mathrm{disc}(b_1, \dots, b_n) \in A \setminus \{0\}$ is independent of $\{b_1, \dots, b_n\}$ modulo $(A^\times)^2$ (meaning that the discriminant of two different bases are identical up to multiplication by the square of some element in $A^\times$).*

Proof. Let $\{b'_1, \dots, b'_n\}$ be another basis of B. Then we can write $b'_i = \sum_{j=1}^n c_{ij} b_j$, and so $C := (c_{ij})_{0 \leq i,j \leq n} \in GL_n(A)$ is the base change matrix. Now let

$$M' = (\mathrm{Tr}_{L/K}(b'_i b'_j)) = \mathrm{Tr}\left(\left(\sum_k c_{ik} b_k\right)\left(\sum_l c_{jl} b_l\right)\right) = \sum_k \sum_l c_{ik} \mathrm{Tr}(b_k b_l) c_{jl} = CMC^t$$

where $M = (\mathrm{Tr}(b_k b_l))$. This implies $\det M' = \mathrm{disc}(b'_1, \dots, b'_n) = (\det C)^2 \det M = (\det C)^2 \mathrm{disc}(b_1, \dots, b_n)$. □

Corollary 2.39. *Let $A = \mathbb{Z}$, $K = \mathbb{Q}$, $L/\mathbb{Q}$ a finite extension and $B = \mathcal{O}_L$. Let $\{b_1, \dots, b_n\}$ be a $\mathbb{Z}$-basis of $\mathcal{O}_L$. If $\{b'_1, \dots, b'_n\} \subset \mathcal{O}_L$, then $\{b'_1, \dots, b'_n\}$ is a $\mathbb{Z}$-basis of $\mathcal{O}_L$ if and only if $\mathrm{disc}(b_1, \dots, b_n) = \mathrm{disc}(b'_1, \dots, b'_n)$ (since $\mathbb{Z}^\times = \{-1, 1\}$).*

Thus we can make the following definition:

Definition 2.40. For $A = \mathbb{Z}$ the discriminant $\mathrm{disc}(b_1, \dots, b_n) \in \mathbb{Z} \setminus \{0\}$ for any $\mathbb{Z}$-basis of $\mathcal{O}_L$ is called the *discriminant of $\mathcal{O}_L$ or L* and denoted by $\mathrm{disc}(\mathcal{O}_L)$ or $\mathrm{disc}(L)$, or Δ_L, δ_L,...

More generally, for Λ a finitely generated $\mathbb{Z}$-module, we can define $\mathrm{disc}(\Lambda)$ in the same way.

Theorem 2.41. *If we have two $\mathbb{Z}$-submodules $\Lambda = \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_n$ and $\Lambda' = \mathbb{Z}e_1' + \cdots + \mathbb{Z}e_n'$ with $\Lambda \subset \Lambda'$, then* $\operatorname{disc}\Lambda = \operatorname{disc}(e_1, \ldots, e_n) = [\Lambda' : \Lambda]^2 \operatorname{disc}\Lambda' = [\Lambda' : \Lambda]^2 \operatorname{disc}(e_1', \ldots, e_n')$.

Proof. Exercise. I think use Proposistion 2.38 □

Corollary 2.42. *Let $L = \mathbb{Q}(\alpha)$. Then* $\operatorname{disc}(\alpha) = \operatorname{disc}(1, \alpha, \ldots, \alpha^{n-1})$ *divides* $\operatorname{disc}(L)$ *and* $\operatorname{disc}(L)/\operatorname{disc}(\alpha)$ *is a square of an integer.*

Example 2.43. Let $L = \mathbb{Q}(\sqrt{-3})$. Then $\Lambda := \mathbb{Z}[\sqrt{-3}] \neq \mathcal{O}_L =: \Lambda'$.

Corollary 2.44. *Suppose L is a number field and $\omega_1, \ldots, \omega_n \in \mathcal{O}_L$ such that* $\operatorname{disc}(\omega_1, \ldots, \omega_n)$ *is square-free. Then $\{\omega_1, \ldots, \omega_n\}$ is a basis of $\mathcal{O}_L$.*

Proof. If $\{b_1, \ldots, b_n\}$ is a basis, then $\operatorname{disc}(\omega_1, \ldots, \omega_n) = (\det(a_{ij}))^2 \operatorname{disc}(b_1, \ldots, b_n)$, where $\omega_i = \sum a_{ij} b_j$. Then since by assumption $\operatorname{disc}(\omega_1, \ldots, \omega_n)$ is square-free, we must have $\det(a_{ij}) = 1$. Then by Corollary 2.39, $b_1, \ldots, b_n$ must be a basis of $\mathcal{O}_L$. □

Remark. This last corollary says that if we start with a basis $b_1, \ldots, b_n$ of L/K which is integral (not necessarily a basis of $\mathcal{O}_L$: e.g. $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Z}[\sqrt{-3}] \subset \mathcal{O}_L$). Then if $\operatorname{disc}(b_1, \ldots, b_n)$ is squarefree, we are done and $\mathcal{O}_L = \mathbb{Z}b_1 + \cdots + \mathbb{Z}b_n$. The bad news is: This will not happen all the time. There is a general theorem:

Theorem 2.45. *Let $L/\mathbb{Q}$ be a number field. Then* $\operatorname{disc}(L) \equiv 0$ *or* $1 \mod 4$.

Proof. Exercise. □

Example 2.46 (Quadratic fields)**.** Let $L = \mathbb{Q}(\sqrt{d})$. Then the discriminant is square-free and

$$\operatorname{disc}(L) = \begin{cases} 4d & d \equiv 2, 3 \mod 4 \\ d & d \equiv 1 \mod 4. \end{cases}$$

Proof. Recall if $d \equiv 2, 3 \mod 4$, then $\{1, \sqrt{d}\}$ is a basis of $\mathcal{O}_L$, else $\{1, \frac{1+\sqrt{d}}{2}\}$ is a basis. The rest is left as an exercise. □

Example 2.47. Let α be a root of $x^3 - x - 1$ and $L = \mathbb{Q}(\alpha)$. Then

$$\operatorname{disc}(1, \alpha, \alpha^2) = \det \begin{pmatrix} \operatorname{Tr} 1 & \operatorname{Tr}\alpha & \operatorname{Tr}\alpha^2 \\ \operatorname{Tr}\alpha & \operatorname{Tr}\alpha^2 & \operatorname{Tr}\alpha^2 \\ \operatorname{Tr}\alpha^2 & \operatorname{Tr}\alpha^3 & \operatorname{Tr}\alpha^4 \end{pmatrix}.$$

Now $\operatorname{Tr} 1 = [L : \mathbb{Q}] = 3$, $\operatorname{Tr}\alpha = 0 =$ coefficient of x^2 in the minimal polynomial of α. To calculate $\operatorname{Tr}\alpha^2$, one can compute the matrix of multiplication by α^2, m_{α^2} in the basis $\{1, \alpha, \alpha^2\}$. This turns out to be

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}.$$

Hence $\operatorname{tr} m_{\alpha^2} = 2$. Or: $\operatorname{Tr}\alpha^2 = \sum_{i=1}^3 \alpha_i^2 = (\sum \alpha_i)^2 - 2\sum_{i<j} \alpha_i\alpha_j = 2$, because the second sum is the coefficient of x in m_α and the first one is 0. The α_i are the 3 roots of m_α. So

$$\operatorname{disc}(1, \alpha, \alpha^2) = \det \begin{pmatrix} 3 & 0 & 2 \\ 0 & 2 & 3 \\ 2 & 3 & 2 \end{pmatrix} = -23,$$

which is squarefree. (Caution m can either mean matrix of multiplication or minimal polynomial)

Example 2.48. Let $L = \mathbb{Q}(\alpha)$, where $\alpha^3 - \alpha - 4 = 0$ (check that $\pm 1, \pm 2, \pm 4$ are no roots, hence it is irreducible). One gets that $\operatorname{disc}(1, \alpha, \alpha^2) = -4 \cdot 107$. This says $\mathbb{Z}[\alpha] = \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\alpha^2$ is either $\mathcal{O}_L$ or has index 2 in $\mathcal{O}_L$.

$$\langle \mathcal{O}_L : \mathbb{Z}[\alpha] \rangle^2 \operatorname{disc} L = \operatorname{disc}(\mathbb{Z}[\alpha])$$

So either $\mathbb{Z}[\alpha] = \mathcal{O}_L$ or $\mathbb{Z}[\alpha] \subset \mathcal{O}_L$ with index 2, i.e.

$$\mathbb{Z}[\alpha] \subset \mathcal{O}_L \subset \frac{1}{2}\mathbb{Z}[\alpha].$$

To determine $\mathcal{O}_L$ we need to check non-zero representatives of $1/2\mathbb{Z}[\alpha]/\mathbb{Z}[\alpha]$.

10.10.2019

Lemma 2.49. *Let Λ be a subgroup of $\mathcal{O}_L$ of rank n, i.e. $\Lambda = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$. If $\Lambda \neq \mathcal{O}_L$ then there exists an algebraic integer of the form*

$$\frac{1}{p}(\lambda_1\alpha_1 + \cdots + \lambda_n\alpha_n),$$

where $0 \leq \lambda_i \leq p-1, \lambda_i \in \mathbb{Z}$ and p is a prime such that $p^2 | \operatorname{disc}(\alpha_1, \ldots, \alpha_n)$.

Remark. This lemma can be used as the basis of trial and error search: If $\operatorname{disc}(\alpha_1, \ldots, \alpha_n)$ is square-free, then we are done, since no such p exists and $\mathcal{O}_L = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$.

1. Start the search with an initial guess $\Lambda = \mathbb{Z}\alpha_1 + \ldots \mathbb{Z}\alpha_n$
2. calculate $\operatorname{disc}(\alpha_1, \ldots, \alpha_n)$. If square-free, then we are done;
3. else, for each prime p that divides the discriminant test all the numbers of the form

$$\frac{1}{p}(\lambda_1\alpha_1 + \cdots + \lambda_n\alpha_n), 0 \leq \lambda_i \leq p-1, \lambda_i \in \mathbb{Z}$$

   to check if they are algebraic integers (their minimal polynomial will then have integer coefficients).
4. if any new integer β arise, enlarge Λ to $\Lambda' = \mathbb{Z}\alpha_1, \ldots, \mathbb{Z}\alpha_n + \mathbb{Z}\beta$, and repeat.

We apply this lemma to our example

$$\beta = \frac{\lambda_0}{2} + \frac{\lambda_1}{2}\alpha + \frac{\lambda_2}{2}\alpha^2, \quad \lambda_i \in \{0, 1\}.$$

Let $\beta = \frac{\alpha}{2} + \frac{\alpha^2}{2}$. We want to check whether β is integral. Let m_β be the multiplication by β map, so we have under m_β:

$$1 \mapsto \frac{\alpha}{2} + \frac{\alpha^2}{2},$$
$$\alpha \mapsto \alpha\beta = 2 + \frac{1}{2}\alpha + \frac{1}{2}\alpha^2,$$
$$\alpha^2 \mapsto \alpha^2\beta = 2 + \frac{5}{2}\alpha + \frac{1}{2}\alpha^2$$

and

$$m_\beta = \begin{pmatrix} 2 & 2 & 2 \\ 1/2 & 1/2 & 5/2 \\ 1/2 & 1/2 & 1/2 \end{pmatrix}.$$

The characteristic polynomial of m_β is $x^3 - x^2 - 3x - 2 \in \mathbb{Z}[x]$ and thus β is integral. So

$$\mathcal{O}_L = \mathbb{Z}[\alpha, \beta] \quad \text{and} \quad \operatorname{disc}(\mathcal{O}_L) = -107.$$

We can also see that

$$\operatorname{disc}(1, \beta, \beta^2) = -107.$$

This means α was not a good generator but β is:

$$\mathcal{O}_L = \mathbb{Z}[\beta].$$

Exercise 2.50 (from homework)**.** Let $K_1 = \mathbb{Q}(\gamma_1)$ and $K_2 = \mathbb{Q}(\gamma_2)$ be algebraic extensions of degree n_1 and n_2 respectively such that $L = \mathbb{Q}(\gamma_1, \gamma_2)$ has degree $n_1 n_2$. Let $\{\alpha_1, \ldots, \alpha_n\}$ and $\{\beta_1, \ldots, \beta_{n_2}\}$ be integral bases for K_1 and K_2 respectively with discriminants D_1 and D_2. If D_1 and D_2 are relatively prime, then $\{\alpha_i, \beta_j\}$ is a basis of $\mathcal{O}_L$.

Example 2.51. Let $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. A first guess would be $\mathbb{Z}[\sqrt{2}, \sqrt{3}]$. But it is not the ring of integers of L because

$$\frac{\sqrt{2}+\sqrt{6}}{2} = \frac{1+\sqrt{3}}{\sqrt{2}} \in \mathcal{O}_L$$

but it is not in $\mathbb{Z}[\sqrt{2}, \sqrt{3}]$. If $\alpha \in \mathcal{O}_L$, then since $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ is a basis of $L/\mathbb{Q}$,

$$\alpha = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}.$$

with $a, b, c, d \in \mathbb{Q}$. If $\alpha \in \mathcal{O}_L$, then its conjugates are also integral (in a splitting field) and they are given by:

$$\begin{aligned}
\alpha_2 &= 1 - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}, \\
\alpha_3 &= 1 + b\sqrt{2} - c\sqrt{3} - d\sqrt{6} \\
\alpha_3 &= 1 - b\sqrt{2} - c\sqrt{3} + d\sqrt{6}.
\end{aligned}$$

We have:

$$\begin{aligned}
\alpha + \alpha_2 &= 2a + 2c\sqrt{3} \\
\alpha + \alpha_3 &= 2a + 2b\sqrt{2} \\
\alpha + \alpha_4 &= 2a + 2d\sqrt{6}.
\end{aligned}$$

Thus $\alpha + \alpha_i \in \mathbb{Q}(\sqrt{d_i})$ where $d_2 = 3, d_3 = 2, d_4 = 6$ and they are algebraic integers so they are in $\mathcal{O}_{\mathbb{Q}(\sqrt{d_i})}$ for $d_i = 2, 3 \mod 4$. Hence they are in $\mathbb{Z}[\sqrt{d_i}]$, thus $2a, 2b, 2c, 2d \in \mathbb{Z}$. Hence

$$\alpha = \frac{A + B\sqrt{2} + C\sqrt{3} + D\sqrt{6}}{2} \quad \text{with } A, B, C, D \in \mathbb{Z}.$$

Similarly

$$\alpha\alpha_2 = (a + c\sqrt{3})^2 - (b\sqrt{2} + d\sqrt{6})^2 = \frac{A^2 + 3C^2 - 2B^2 - 6D^2}{4} + \frac{AC - 2BD}{2}\sqrt{3}$$

(where we let $A = 2a, B = 2b, C = 2c, D = 2d$) and both coefficients are in $\mathbb{Z}$. This implies that $2|AC$ and thus at least one of A and C is even. If only one is even then $A^2 + 3C^2 - 2B^2 - 6D^2$ would be odd and hence both are even.

The condition of the coefficients being in $\mathbb{Z}$ becomes $2|B^2 - 3D^2$. Thus B and D are both even or both odd. Therefore α is of the form

$$\alpha = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6},$$

with $a, c \in \mathbb{Z}$ and b, d being both integral or both half an odd integer.

Next, we will see that all numbers of this form are algebraic integers, i.e. in $\mathcal{O}_L$. Such elements are all linear combinations of $1, \sqrt{2}, \sqrt{3}$ and $\gamma = \frac{\sqrt{2}+\sqrt{6}}{2}$, but they are in $\mathcal{O}_L$. Hence

$$\mathcal{O}_L = \mathbb{Z} + \mathbb{Z}\sqrt{2} + \mathbb{Z}\sqrt{3} + \mathbb{Z}\gamma.$$

In fact, $\mathcal{O}_L = \mathbb{Z}[\gamma]$, because $\sqrt{2} = \gamma^3 - 3\gamma$ and $\sqrt{3} = \gamma^2 - 2$.

Warning! It is not true that all ring of integers $\mathcal{O}_L$ are of the form $\mathbb{Z}[\alpha]$ for some α. Number fields whose ring of integers is generated by a single element over $\mathbb{Z}$ are called monogenic. For a non-example see Exercise 3.3.

Remark (final remark on discriminant). The discriminant also has a geometrical interpretation, which can already be seen in the quadratic case. Let $L = \mathbb{Q}(\sqrt{d})$. Assume for simplicity $d = 2$ or $3 \mod 4$ so that $\mathcal{O}_L = \mathbb{Z}[\sqrt{d}]$. Let $\alpha \in L$ be such that $\alpha^2 = d$. There are two embeddings

$$\begin{aligned} \sigma_+, \sigma_- \colon L &\to \mathbb{R} \\ \alpha &\mapsto \pm\sqrt{d} \end{aligned}$$

and we define

$$\begin{aligned} \sigma \colon L &\to \mathbb{R} \times \mathbb{R} \\ x &\mapsto (\sigma_+(x), \sigma_-(x)). \end{aligned}$$

Under this map

$$\sigma(\mathcal{O}_L) = \mathbb{Z}\sigma(1) + \mathbb{Z}\sigma(\alpha)$$

where $\sigma(1) = (1, 1)$ and $\sigma(\alpha) = (\sqrt{d}, -\sqrt{d})$.

There is a fundamental parallelogram

$$\{t\sigma(1) + u\sigma(\alpha) \mid 0 \leq t < 1, 0 \leq u < 1\},$$

whose $\sigma(\mathcal{O}_L)$ translates cover all of $\mathbb{R}^2$. Its area is given by

$$\det \left| \begin{pmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{pmatrix} \right| = 2\sqrt{d} = \sqrt{\text{disc.}}$$

3 Ideals

The goal of this section is the following theorem: Any ideal I of $\mathcal{O}_L$ can be written as a product of prime ideals uniquely up to the order of factors.

Toy example: Suppose one lives in a world where the only possible integers are of the form $3n+1$. In this world we call a number prime if it cannot be factored any further. For example, $4, 7, 10, \ldots$ are all primes, whereas $16 = 4 \times 4$ is not. We can also see that $100 = 10 \times 10 = 4 \times 25$ has two different prime factorizations. If we enlarge our world to include integers of the form $3n + 2$, then $4 = 2 \times 2, 25 = 5 \times 5, 10 = 2 \times 5$ and $100 = 2 \times 5 \times 2 \times 5 = 2 \times 2 \times 5 \times 5$. So we recover unique factorization.

Example 3.1. Let $L = \mathbb{Q}(\sqrt{10}),$, then $\mathcal{O}_L = \mathbb{Z}[\sqrt{10}]$. Here we have $6 = 2 \times 3 = (4 + \sqrt{10})(4 - \sqrt{10})$.

Kummer tried to repair the lack of unique factorization similarly as in the toy example. He invented "symbols" p_1, p_2, p_3, p_4 such that $2 = p_1 \times p_2$, $3 = p_3 \times p_4$, $4 + \sqrt{10} = p_1 \times p_3$ and $4 - \sqrt{10} = p_2 \times p_4$. Thus we can write

$$6 = 2 \times 3 = (4 + \sqrt{10})(4 - \sqrt{10}) = p_1 p_2 p_3 p_4 = p_1 p_3 p_2 p_4$$

If 2 were a multiple of p_1, so would be any multiple of 2. Similarly the same holds for $4 + \sqrt{10}$ and p_1. Combining these, any $\mathbb{Z}[\sqrt{10}]$-combination should also be a multiple of p_1. This suggests that in whichever way an ideal number p is defined, it has to be linked to the numbers $a \in \mathcal{O}_L$ by a divisibility relation: $p|a$ should satisfy the rules that if $a, b, \lambda \in \mathcal{O}_L$ and $p|a, p|b$ then $p|a \pm b$, and if $p|a$ then $p|\lambda a$.

Historically a lot of mathematical mistakes arose from the misconception concerning the definition of primes in $\mathbb{Z}$ in two different ways:

1. If $p = ab$, then one of a or b must be a unit.
2. If $p|ab$, then $p|a$ or $p|b$.

Over $\mathbb{Z}$ these are equivalent, but in general 2. is more powerful than 1. The elements that satisfy 1. are called *irreducibles*.

Remark. 1. If it can be proved that there is a factorization into primes, then uniqueness is not hard.

2. Even when there is a factorization into irreducibles, it might not be unique.

Suppose D is a domain. We can attempt to write $x = ab$ where a, b are non-units. If we find such a factorization, then we can try to factor a and b and continue. If this procedure terminates, then that gives us the factorization into irreducibles. But it might not. For example consider

$$D = \mathbb{Z}^{\mathbb{C}} = \{z \in \mathbb{C} \mid z \text{ satisfies a monic polynomial in } \mathbb{Z}[X]\}.$$

Let $z \in D$. Then there exists $a_0, \ldots, a_n \in \mathbb{Z}$ such that $a_0 + a_1 z + \cdots + a_n z^n = 0$. However, we also have

$$a_0 + a_1(\sqrt{z})^2 + \cdots + a_n(\sqrt{z})^{2n} = 0$$

for any $n \in \mathbb{N}_{>0}$.

3.1 Ideals of a Dedekind Domain

Definition 3.2. A domain D is called *Noetherian* if every ideal is finitely generated.

Theorem 3.3. *The following are quivalent:*

1. *D is Noetherian.*
2. *Given an ascending chain of ideals $I_0 \subset I_2 \subset I_2 \subset \ldots$ there exists some $N \in \mathbb{N}$ such that $I_n = I_N$ for all $n \geq N$ ("ascending chain condition/ACC").*
3. *Every non-empty set of ideals in D has a maximal element.*

15.10.2019

Theorem 3.4. *The ring of integers $\mathcal{O}_L$ of a number field L is Noetherian.*

Proof. First, note that any ideal I of $\mathcal{O}_L$ is a finitely generated $\mathbb{Z}$-module of rank n. Indeed, we have already seen that $\mathcal{O}_L = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n$; let $a \in I$, then $a\omega_1, \ldots, a\omega_n \in I$. Thus

$$\mathbb{Z}a\omega_1 + \ldots \mathbb{Z}a\omega_n \subset I \subset \mathbb{Z}\omega_1 + \ldots \mathbb{Z}\omega_n$$

and so I is also free of rank n.

If $x_1, \ldots, x_n$ are generators of I as a $\mathbb{Z}$-module, then $\mathcal{O}_L x_i \in I$. Thus

$$I = \mathbb{Z}x_1 + \ldots \mathbb{Z}x_n \subset \mathcal{O}_L x_1 + \cdots + \mathcal{O}_L x_n \subset I$$

therefore we have equality

$$I = \mathcal{O}_L x_1 + \cdots + \mathcal{O}_L x_n.$$

Or in short: $\mathcal{O}_L$ is a finitely generated $\mathbb{Z}$-module. Every ideal $I \subset \mathcal{O}_L$ is a $\mathbb{Z}$-submodule of $\mathcal{O}_L$ and hence finitely generated over $\mathbb{Z}$ as well. Since $\mathbb{Z} \subset \mathcal{O}_L$, it is also finitely generated as an $\mathcal{O}_L$-module and thus as an ideal.

□

We have some easy properties:

Lemma 3.5. *Let $[L : \mathbb{Q}] = n$ and $\mathcal{O}_L$ the ring of integers. Then*

1. *For any $\alpha \in L$, there exists $m \in \mathbb{Z}$ such that $m\alpha \in \mathcal{O}_L$.*
2. $\mathrm{Quot}(\mathcal{O}_L) = L$.
3. *$\mathcal{O}_L$ is integrally closed.*

Proof. 1. and 2. follow from Proposition 2.15. The third point is trivially true by the definition of $\mathcal{O}_L$. More specifically, let $\overline{\mathcal{O}_L}$ be the integral closure of $\mathcal{O}_L$. Then

$$\mathbb{Z} \subset \mathcal{O}_L \subset \overline{\mathcal{O}_L}$$

and by transitivity of integrality, we see that $\overline{\mathcal{O}_L}$ is integral over $\mathbb{Z}$. But then that implies $\overline{\mathcal{O}_L} \subset \mathcal{O}_L$. □

Now we will show that every prime ideal of $\mathcal{O}_L$ is maximal.

Definition 3.6. Let I be an ideal of a domain D, then I is called *prime* if

1. $I \neq D$ and
2. if $xy \in I$ then $x \in I$ or $y \in I$.

Remark. Some facts to recall:

1. I is maximal if and only if D/I is a field.
2. Let $p \in D$. If $\langle p \rangle$ is maximal, then p is irreducible.
3. If D is a PID, then for an element p to be irreducible is equivalent to p being prime. That is, one can view maximal ideals as a generalization of irreducible elements to ideals.
4. If D is an integral domain, and $p \in D$. Then $\langle p \rangle$ is a prime ideal if and only if p is a prime element.
5. If an ideal is maximal, then it is prime. The reverse is in general not true.
6. I is a prime ideal if and ony if D/I is an integral domain.
7. If D is finite inegral domain, then D is a field.
8. In a UFD, irreducibility implies primality.

Proposition 3.7. *Every non-zero prime ideal $\mathfrak{p} \subset \mathcal{O}_L$ is a maximal ideal.*

Proof. Note this will follow if we can show $\mathcal{O}_L/\mathfrak{p}$ is a finite, since being a finite integral domain, it will be a field, hence $\mathfrak{p}$ will be maximal.

Claim: $\mathcal{O}_L/\mathfrak{p}$ is finite.
Proof of claim: Since $\mathfrak{p} \neq 0$, there exists a nonzero $\alpha \in \mathfrak{p} \subset \mathcal{O}_L$. Thus

$$\mathrm{N}_{L/\mathbb{Q}}(\alpha) = \prod \sigma(\alpha) \in \mathbb{Z} \quad \text{(Proposition 2.26)},$$

and set

$$N \coloneqq \alpha \prod_{\sigma \neq \mathrm{Id}} \sigma(\alpha) \in \mathbb{Z}$$

Now $\prod_{\sigma \neq \mathrm{Id}} \sigma(\alpha)$ is integral, but not necessarily in $\mathcal{O}_L$. On the other hand

$$\frac{N}{\alpha} \in L \text{ is integral,}$$

but $\mathcal{O}_L$ is integrally closed, hence $\frac{N}{\alpha} \in \mathcal{O}_L$. Therefore $N \in \alpha\mathcal{O}_L$, so $N \in \mathfrak{p}$. Now if $\mathcal{O}_L$ has an integral basis

$$\mathcal{O}_L = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n,$$

then since $N \in \mathfrak{p}$, $N\omega_1, \ldots, N\omega_n \in \mathfrak{p}$. Hence any

$$a_1\omega_1 + \cdots + a_n\omega_n \in \mathcal{O}_L, \quad a_i \in \mathbb{Z}$$

is congruent (mod $\mathfrak{p}$) to an element $b_1\omega_1 + \cdots + b_n\omega_n$ with $0 \leq b_i < N$. Since there are only finitely many choices this gives

$$\left|\mathcal{O}_L \,/_{\mathfrak{p}}\right| < \infty.$$

Or alternatively, after knowing that $\mathfrak{p} \cap \mathbb{Z} \neq 0$, we get $\mathfrak{p} \cap \mathbb{Z} = (p)$ for some prime number p. Then the fact that $\mathcal{O}_L$ is a finitely generated $\mathbb{Z}$-module implies that $\mathcal{O}_L/\mathfrak{p}$ is a finitely generated $\mathbb{Z}/p\mathbb{Z}$-module and hence finite.

□

Remark. In fact $\mathcal{O}_L/I$ is finite for any ideal I. To see this one can use the following lemma:
Any injective homomorphism $\phi : \mathbb{Z}^n \to \mathbb{Z}^n$ has finite cokernel.

We have already seen that I is a free $\mathbb{Z}$-module of rank n, i.e. $I \cong \mathbb{Z}^n$, and $\mathcal{O}_L \cong \mathbb{Z}^n$. Now take $\phi : I \to \mathcal{O}_L$ the obvious injection. Then it follows from the lemma that $\mathrm{coker}(\phi) = \mathcal{O}_L/I$ is finite.
We now have the following facts about $\mathcal{O}_L$:

1. $\mathcal{O}_L$ is integrally closed.
2. $\mathcal{O}_L$ is Noetherian.
3. Every prime ideal is maximal.

Definition 3.8. An integral domain A is called a *Dedekind domain* if

1. it is integrally closed,
2. it is Noetherian
3. and every prime ideal is maximal.

Thus

Theorem 3.9. *For L an algebraic number field, $\mathcal{O}_L$ is a Dedekind domain.*

Proof. Immediate. □

Example 3.10. The ring $D = \mathbb{Z}[\sqrt{-3}]$ is not a Dedekind domain, since D is not integrally closed.

3.2 Prime Factorization of Ideals

Our next goal is to show that every ideal in a Dedekind domain can be written uniquely as a product of prime ideals. Recall that in any ring R, if I, J are ideals, then

$$IJ \coloneqq \left\{ \sum_{i=1}^{n} x_i y_i \mid x_i \in I, y_i \in J \right\}.$$

If $I = (a_1, \ldots, a_n)$ and $J = (b_1, \ldots, b_m)$. Then IJ is given by $(a_i b_j)$. We can also look at the intersection of ideals. In general the intersection $\bigcap_\alpha I_\alpha$ of ideals is again an ideal. The sum of ideals is defined as

$$I + J \coloneqq \{x + y \mid x \in I, y \in J\},$$

which is also an ideal.

We start with a simple lemma for a general commutative ring R.

Lemma 3.11. *Suppose $I_1, \ldots, I_n$ are ideals in a ring R, and $\mathfrak{p}$ is a prime ideal. If the product $I_1 \ldots I_n \subset \mathfrak{p}$, then $I_i \subset \mathfrak{p}$ for some i.*

Proof. Suppose not. Then for all i, there exists $\alpha_i \in I_i$ with $\alpha_i \notin \mathfrak{p}$. Then $\alpha_i \ldots \alpha_n \in I_1 I_2 \ldots I_n \subset \mathfrak{p}$. But $\mathfrak{p}$ is a prime ideal, hence $\alpha_i \in \mathfrak{p}$ for some i. This is a contradiction. □

The next two propositions are crucial for our goal.

Proposition 3.12. *If I is an ideal in a Noetherian ring O, then there exist non-zero prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ of O such that $\mathfrak{p}_1 \ldots \mathfrak{p}_r \subset I$.*

Proof. Let M be the set of ideals of O for which the conclusion of the proposition fails. We aim to show $M = \emptyset$. Suppose $M \neq \emptyset$, then since O is Noetherian, M has a maximal element J. Clearly, by definition of M, J is not prime. Thus there exist $a, b \in O$ such that the product $ab \in J$ but $a \notin J$ and $b \notin J$. Let $\mathfrak{a} \coloneqq (J, a) = (a) + J$ and $\mathfrak{b} \coloneqq (J, b) = (b) + J$. Now $J \subsetneq \mathfrak{a}$ and $J \subsetneq \mathfrak{b}$. Since J is maximal in M, $\mathfrak{a}, \mathfrak{b} \notin M$, thus there exist prime ideals $\mathfrak{p}_1 \ldots \mathfrak{p}_r \subset \mathfrak{a}$, and prime ideals $\mathfrak{q}_1 \ldots \mathfrak{q}_s \subset \mathfrak{b}$. Hence

$$\mathfrak{p}_1 \ldots \mathfrak{p}_r \mathfrak{q}_1 \ldots \mathfrak{q}_s \subset \mathfrak{a}\mathfrak{b} \subset J,$$

which is a contradiction to the fact that $J \in M$ and the definition of M. □

17.10.2019

Definition 3.13. For an integral domain A with field of fractions $\mathrm{Quot}(A) = K$, and $0 \neq I \subset A$ a non-zero ideal, we define

$$I^{-1} \coloneqq \{x \in K \mid xI \subset A\}.$$

Remark. It is clear that we have the following facts:

1. $A \subset I^{-1}$
2. I^{-1} is an A-submodule of K
3. If $I = (a)$ is a principal ideal, then $I^{-1} = a^{-1}A$

Recall that one can multiply two A-submodules M, N; their product MN is the A-submodule of K generated by products of the form xy, with $x \in M$ and $y \in N$. If M, N are ideals, this is the usual product of ideals. If M, M', N are all A-submodules of K, such that $M \subset M'$ then $MN \subset M'N$.

Proposition 3.14. *Let O be a Dedekind domain, $0 \neq I$ an ideal of O and $\mathfrak{p}$ a non-zero prime ideal of O. Then*

$$\mathfrak{p}^{-1} I \coloneqq \left\{ \sum a_i x_i \mid a_i \in \mathfrak{p}^{-1}, x_i \in I \right\} \neq I.$$

Proof. We first consider the special case of $I = O$. In this case we are trying to show $\mathfrak{p}^{-1} \neq O$. Clearly $O \subset \mathfrak{p}^{-1}$ from the previous remark. By definition, if $x \in \mathfrak{p}^{-1}$, then $x\mathfrak{p} \subset O$. If $\mathfrak{p}$ were principal, say $\mathfrak{p} = (\alpha) = \alpha O$ where $\alpha \neq 0$ and $\alpha \notin O^\times$, then $\mathfrak{p}^{-1} = \alpha^{-1}O$ and $x := \frac{1}{\alpha} \in \mathfrak{p}^{-1} \setminus O$.

In general, if we can find an x of the form $x = a^{-1}b$ for well chosen elements a, b of O in the sense that

$$b\mathfrak{p} \subset (a)$$

but $b \notin (a)$, then $a^{-1}b \in \mathfrak{p}^{-1}$ and $a^{-1}b \notin O$.

Let $a \in \mathfrak{p}$ be any non-zero element of $\mathfrak{p}$. We will find an appropriate b so that $a^{-1}b \in \mathfrak{p}^{-1}$, $a^{-1}b \notin O$. By Proposition 3.12, we know there exist non-zero prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ such that $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset (a)$. We may assume $r \geq 1$ is chosen to be as small as possible. Since $(a) \subset \mathfrak{p}$, we have

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset (a) \subset \mathfrak{p}.$$

By Lemma 3.11 one of the prime ideals $\mathfrak{p}_i$ is contained in $\mathfrak{p}$. Since O is a Dedekind domain, prime ideals are maximal and so in fact $\mathfrak{p} = \mathfrak{p}_i$ for some i. Without loss of generality take $i = 1$.

If $r = 1$, then $\mathfrak{p} = (a)$. But in this case we can take $x = \frac{1}{a} \in \mathfrak{p}^{-1} \setminus O$.

Now assume $r \geq 2$. By minimality of r we must have

$$\mathfrak{p}_2 \cdots \mathfrak{p}_r \not\subset (a).$$

Hence there exists $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r$ such that $b \notin (a)$. On the other hand, by our construction

$$b\mathfrak{p} \subset \mathfrak{p}\mathfrak{p}_2 \cdots \mathfrak{p}_r \subset (a).$$

Hence we have found a b such that $b\mathfrak{p} \subset (a)$ while $b \notin (a)$. Therefore

$$x = a^{-1}b \in \mathfrak{p}^{-1} \setminus O.$$

Now we know that $I = O$, we get that $\mathfrak{p}^{-1} \neq O$.

Let us now consider the general case, where I is not necessarily O. Since O is Noetherian, I is finitely generated, say

$$I = \alpha_1 O + \cdots + \alpha_n O.$$

Suppose on the contrary that $\mathfrak{p}^{-1}I = I$. Then for all $x \in \mathfrak{p}^{-1}$ we can write

$$x\alpha_i = \sum_{j=i}^{n} a_{ij}\alpha_j, \quad a_{ij} \in O.$$

Consider the matrices $A = (a_{ij})$ and $T = xI - A$. Then

$$T \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = 0$$

This gives

$$(\det T)\alpha_i = 0, \quad \text{for all } i$$

and so $\det T = 0$. This determinant of T is a monic polynomial with coefficients in O, therefore x is integral over O. Since O is integrally closed, x lies in fact in O. Thus $\mathfrak{p}^{-1} = O$, but we have already shown this cannot happen. □

Corollary 3.15. *Let O be a Dedekind domain and $\mathfrak{p}$ be a non-zero prime ideal of O, then*

$$\mathfrak{p}^{-1}\mathfrak{p} = O.$$

Proof. By definition $x\mathfrak{p} \subset O$ for any $x \in \mathfrak{p}^{-1}$. Hence $\mathfrak{p}^{-1}\mathfrak{p} \subset O$. We also have $O \subset \mathfrak{p}^{-1}$. So

$$\mathfrak{p} = \mathfrak{p}O \subset \mathfrak{p}^{-1}\mathfrak{p} \subset O,$$

thus $\mathfrak{p}^{-1}\mathfrak{p}$ is an ideal of O. But by Proposition 3.14 $\mathfrak{p}^{-1}\mathfrak{p} \neq \mathfrak{p}$. However, O is a Dedekind domain and so $\mathfrak{p}$ is maximal. Hence $\mathfrak{p}\mathfrak{p}^{-1} = O$. □

Theorem 3.16. *Every proper ideal $0 \neq I \neq (1)$ of a Dedekind domain O admits a factorization*

$$I = \mathfrak{p}_1 \cdots \mathfrak{p}_r$$

into non-zero prime ideals $\mathfrak{p}_i$ of O which is unique up to reordering.

Proof. We need to show existence and uniqueness. First we assume existence and we will show uniqueness. Suppose

$$I = \mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s$$

for prime ideals $\mathfrak{p}_i$'s and $\mathfrak{q}_j$'s. Thus

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s \subset \mathfrak{p}_1.$$

By Lemma 3.11, since $\mathfrak{p}_1$ is prime, there exists some $\mathfrak{q}_i \subset \mathfrak{p}_1$ for some i. Since $\mathfrak{p}_1$ and $\mathfrak{q}_i$ are maximal, we have $\mathfrak{q}_i = \mathfrak{p}_1$. Without loss of generality assume $\mathfrak{q}_1 = \mathfrak{p}_1$. Multiply both sides of $\mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s$ by $\mathfrak{p}_1^{-1}$, and using the previous corollary that $\mathfrak{p}^{-1}\mathfrak{p} = (1)$ for a prime ideal $\mathfrak{p}$, we get

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

Continuing in this manner gives uniqueness.

To prove existence, we will use the Noetherian property. Let M be the set of all proper ideals of O which cannot be written as a product of prime ideals. Assume by contradiction that $M \neq \emptyset$. Then by the Noetherian property, M has a maximal element, say J. The ideal J is contained in a maximal ideal $\mathfrak{p} \subset O$. Note that $J \subsetneq \mathfrak{p}$ (since $J \in M$, so J cannot be prime). Since $O \subset \mathfrak{p}^{-1}$,

$$J = JO \subset J\mathfrak{p}^{-1} \subset \mathfrak{p}\mathfrak{p}^{-1} = O.$$

Now by Proposition 3.14, $J \neq J\mathfrak{p}^{-1}$; and since $J \neq \mathfrak{p}$, $J\mathfrak{p}^{-1} \neq \mathcal{O}$. So we actually have strict inlcusions

$$J = JO \subsetneq J\mathfrak{p}^{-1} \subsetneq \mathfrak{p}\mathfrak{p}^{-1} = O.$$

By maximality of J in M, and $J \subsetneq J\mathfrak{p}^{-1} \subsetneq O$, we have that

$$J\mathfrak{p}^{-1} \notin M.$$

Here we use that since $\mathfrak{p}^{-1}$ is a sub O-module of K, then $J\mathfrak{p}^{-1}$ is also a $\mathcal{O}$-submodule but further it is an ideal in O since it is contained in O. Now this means there is a factorization

$$J\mathfrak{p}^{-1} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$$

for some $\mathfrak{p}_1 \cdots \mathfrak{p}_r$. But then

$$J = J\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}\mathfrak{p}_1 \cdots \mathfrak{p}_r$$

is a product of prime ideals. □

In our proof of Theorem 3.16, we used the construction

$$I^{-1} \coloneqq \{x \in K \mid xI \subset O\}.$$

This construction will also allow us to define a group structure on finitely generated O-submodules of K which are called *fractional ideals*. Before that we collect some simple properties of I^{-1}.

Lemma 3.17. *For any ideal I of a Dedekind domain O we have*

1. *I^{-1} is an O-submodule of K.*
2. *If $I \neq 0$, then for any $0 \neq c \in I, cI^{-1} \subset O$.*
3. *$O \subset I^{-1}$, hence $I = IO \subset II^{-1}$*
4. *$II^{-1} = I^{-1}I \subset O$.*
5. *For ideals $I, J \subset O$, $I \subset J$ implies that $O \subset J^{-1} \subset I^{-1}$.*

Proof. Exercise, pretty trivial. □

Lemma 3.18. *Let I be a non-zero ideal of O with factorization $I = \mathfrak{p}_1 \cdots \mathfrak{p}_r$, then*

$$I^{-1} \coloneqq \{x \in K \mid xI \subset O\} = \mathfrak{p}_1^{-1}\mathfrak{p}_2^{-1} \cdots \mathfrak{p}_r^{-1},$$

and hence

$$II^{-1} = O.$$

Proof. Let $\tilde{I} \coloneqq \mathfrak{p}_1^{-1} \cdots \mathfrak{p}_r^{-1}$. Then clearly $I\tilde{I} = O$ using $\mathfrak{p}\mathfrak{p}^{-1} = O$. Then we have $\tilde{I} \subset I^{-1} = \{x \in K \mid xI \subset O\}$.

Conversely, if $x \in I^{-1}$ so that $xI \subset O$, this implies

$$xO = xI\tilde{I} \subset \tilde{I}.$$

Then since $x \cdot 1 \in xO \subset \tilde{I}$, we have $x \in \tilde{I}$. Hence

$$\tilde{I} = I^{-1} = \mathfrak{p}_1^{-1} \cdots \mathfrak{p}_r^{-1}$$

□

Recall: For two ideals $\mathfrak{a}, \mathfrak{b} \subset A$ we say $\mathfrak{a}|\mathfrak{b}$ if there exists an ideal $\mathfrak{c} \subset A$ such that $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$.

Lemma 3.19. *In a Dedekind domain O for two ideals $\mathfrak{a}, \mathfrak{b}$ we have that $\mathfrak{a}|\mathfrak{b}$ if and only if $\mathfrak{b} \subset \mathfrak{a}$. That is , "to contain" is equivalent to "to divide".*

Proof. If $\mathfrak{b} \subset \mathfrak{a}$, then let

$$\mathfrak{c} \coloneqq \mathfrak{b}\mathfrak{a}^{-1} \subset \mathfrak{a}\mathfrak{a}^{-1} = O.$$

Hence $\mathfrak{c}$ is an ideal of O and $\mathfrak{b} = \mathfrak{c}\mathfrak{a}$.

Conversely if $\mathfrak{b} = \mathfrak{c}\mathfrak{a}$ for $\mathfrak{a}$ an ideal, then $\mathfrak{b} = \mathfrak{c}\mathfrak{a} \subset \mathfrak{a}$. □

In the prime ideal factorization of an ideal, collecting the same prime ideals together we can write

$$I = \mathfrak{p}_1^{v_1}\mathfrak{p}_2^{v_2} \cdots \mathfrak{p}_r^{v_r}, \quad v_i > 0$$

where the $\mathfrak{p}_i$'s are pairwise distinct. Recall for any non-zero ideals I, J we have a greatest common divisor $g = (I, J)$ and the least common multiple ℓ with the following properties:

$$g|I, g|J$$

and if any $\tilde{g}$ has the same properties, then $\tilde{g}|g$;

$$I|\ell, J|\ell$$

and if any $\tilde{\ell}$ has the same properties then $\ell|\tilde{\ell}$.

If $I = \prod \mathfrak{p}_i^{e_i}$, $J = \prod \mathfrak{p}_i^{f_i}$, then

$$g = \prod \mathfrak{p}_i^{\min\{e_i, f_i\}}$$
$$\ell = \prod \mathfrak{p}_i^{\max\{e_i, f_i\}}$$

and moreover

$$g = I + J, \ell = I \cap J.$$

For a product $I = I_1 \cdots I_n$ of relatively prime ideals we have the Chinese Remainder Theorem:

Theorem 3.20 (Chinese Remainder Theorem)**.** *If $I_1, \dots, I_n$ are ideals in O such that $I_i + I_j = O$ for $i \neq j$, then if $I = \bigcap_{i=1}^n I_i$ one has*

$$O/I \cong \bigoplus_{i=1}^n O/I_i$$

Theorem 3.21. *The canonical homomorphism*

$$\begin{aligned} \phi \colon O &\to \bigoplus_{i=1}^n O/I_i \\ a &\mapsto \bigoplus_{i=1}^n a \mod I_i \end{aligned}$$

has kernel $\ker \phi = \bigcap_{i=1}^n I_i$, thus it suffices to show that ϕ is surjective (then just use First Isomorphism Theorem). So let

$$(x_i \mod I_i)_{i=1}^n \in \bigoplus_{i=1}^n O/I_i$$

Suppose that $i = 2$. Then since $O = I_1 + I_2$, we can write $1 = a_1 + a_2$ for $a_i \in I_i$. Then define

$$x \coloneqq a_1 x_2 + a_2 x_1 \in O$$

Then

$$x \mod I_i \equiv x_i \mod I_i$$

thus $\phi(x) = (x_i \mod I_i)_{i=1}^2$.

Now suppose $n > 2$....

Theorem 3.22. *If O is a Dedekind domain, then O is a UFD if and only if O is a PID.*

22.20.2019

Example from last time:

Example 3.23. Let $R = \mathbb{Z}[\sqrt{5}], K = \mathbb{Q}(\sqrt{5}), \mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$. Let $\mathfrak{p} = (2, 1+\sqrt{5})$, then

1. $\mathfrak{p}$ is a maximal ideal.
2. $\mathfrak{p}^2 = 2\mathfrak{p}, \mathfrak{p}^{-1} = (\frac{1}{2}\mathfrak{p})$. Hence
$$\mathfrak{p}\mathfrak{p}^{-1} = \left(\frac{1}{2}\right) 2\mathfrak{p} = \mathfrak{p}.$$
3. $2R \subset \mathfrak{p}$ but $\mathfrak{p} \nmid 2R$.

3.3 Fractional Ideals and the Ideal Class Group

Given ideals I, J of a Dedekind domain O, we can clearly multiply them, but we do not have inverses. To obtain a group structure, we extend our net. Recall an ideal I of O can be described as an O-submodule. If we extend our net by considering O-submodules of $K = \mathrm{Quot}(O)$, it turns out we can also get inverses. The particular submodules of K which will provide us with inverses are given in the next definition.

Definition 3.24. Let O be a Dedekind domain, and $K = \mathrm{Quot}(O)$. An O-submodule $\mathfrak{a}$ of K is called a *fractional ideal of O (or of K)* if there exists a non-zero $c \in O$ such that $c\mathfrak{a} \subset O$.

We can see immediately that the set $c\mathfrak{a} \subset O$ is an "actual" ideal of O, since an O-module $c\mathfrak{a}$ contained inside O is literally an ideal of O.

We can also see that the fractional ideals of O are subsets of K of the form

$$c^{-1}\mathfrak{b} \subset K$$

with $\mathfrak{b}$ an actual ideal of O and $0 \neq c \in O$. Indeed if $\mathfrak{a}$ is a fractional ideal according to our first definition, then clearly if we set $\mathfrak{b} = c\mathfrak{a}$, then

$$\mathfrak{a} = c^{-1}c\mathfrak{a} = c^{-1}\mathfrak{b}$$

Conversely, let $c^{-1}\mathfrak{b} \subset K$, then first of all it is clear that $c^{-1}\mathfrak{b}$ is an O-submodule of K because we have an ideal $\mathfrak{b}$ sitting on top. Then further,

$$cc^{-1}\mathfrak{b} = \mathfrak{b} \subset O$$

thus $c^{-1}\mathfrak{b}$ is a fractional ideal.

The element c should be thought of as something like a "common denominator".

Definition 3.25. A fractional ideal is called *principal* if it is of the form αO, for $\alpha \in K$.

Example 3.26. Take $O = \mathbb{Z}$, then $K = \mathbb{Q}$. Then $\frac{1}{2}\mathbb{Z}$ is a fractional ideal of $\mathbb{Z}$ (or $\mathbb{Q}$).

In general an ideal of O is clearly a fractional ideal. A fractional ideal $\mathfrak{a}$ is an ideal if and only if $\mathfrak{a} \subset O$. Ideals (in the usual sense) $\mathfrak{a} \subset O$ are called *integral ideals*.

The product of two fractional ideals is again a fractional ideal: Suppose we have $\mathfrak{a}_1 = c_1^{-1}\mathfrak{b}_1, \mathfrak{a}_2 = c_2^{-1}\mathfrak{b}_2$ where $\mathfrak{b}_1, \mathfrak{b}_2 \subset O$ are ideals and $c_1, c_2 \in O$. Then

$$\mathfrak{a}_1\mathfrak{a}_2 = (c_1c_2)^{-1}\mathfrak{b}_1\mathfrak{b}_2$$

is again a fractional ideal. This multiplication is commutative with the identity given by $(1) = O$.

Fractional ideals can be equivalently defined as finitely generated O-submodules of K. Note these definitions are indeed equivalent: Suppose $\mathfrak{a}$ is a finitely generated O-submodule of K and let

$$k_1 = \frac{a_1}{b_1}, \ldots, k_n = \frac{a_n}{b_n} \in K$$

be the generators. Define $c \coloneqq b_1b_2 \cdots b_n$, then $c\mathfrak{a} \subset O$.

Conversely, suppose $\mathfrak{a}$ is a fractional ideal, i.e. it is an O-submodule such that there exists $c \in O$ such that $c\mathfrak{a} \subset O$, then $\mathfrak{b} \coloneqq c\mathfrak{a}$ is an (integral/actual) ideal of O. Now O is Noetherian, hence every ideal is finitely generated. Let $c_1, \ldots, c_n$ be the generators of $\mathfrak{b}$ as an ideal of O. Then

$$\frac{c_1}{c}, \ldots, \frac{c_n}{c}$$

will be generators of the O-submodule $\mathfrak{a}$.

Exercise 3.27. Can you find an O-submodule of K which is not a fractional ideal?

It turns out that if we define for a fractional ideal $\mathfrak{a}$ the following

$$\mathfrak{a}^{-1} \coloneqq \{x \in K \mid x\mathfrak{a} \subset O\},$$

then we also obtain inverses. Note that $\mathfrak{a}^{-1}$ is a fractional ideal, since we can choose any $\alpha \in \mathfrak{a}$ to get $\alpha\mathfrak{a}^{-1} = \mathfrak{a}^{-1}\alpha \subset O$ (by definition of $\mathfrak{a}^{-1}$).

Theorem 3.28. *The fractional ideals of O form an Abelian group under multiplication with identity $(1) = O$. This group is denoted by J_K.*

Proof. Recall that for the case of an integral ideal $I = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ we have already seen that $I^{-1} = \mathfrak{p}_1^{-1} \cdots \mathfrak{p}_r^{-1}$. Now let $\mathfrak{a}$ be an arbitrary fractional ideal. Then there exists some $0 \neq c \in O$ such that $I = c\mathfrak{a}$ is an integral ideal. Then $I^{-1} = c^{-1}\mathfrak{a}^{-1}$, and

$$O = II^{-1} = c\mathfrak{a}c^{-1}\mathfrak{a}^{-1} = \mathfrak{a}\mathfrak{a}^{-1}.$$

□

We also have the following extended result of the factorization into prime ideals, but be casreful, in this more general version for fractional ideals, the powers of the prime ideals can be negative:

Corollary 3.29. *Every fractional ideal $\mathfrak{a}$ has a unique factorization*

$$\mathfrak{a} = \prod \mathfrak{p}_i^{\nu_i}, \quad \text{with } \nu_i \in \mathbb{Z} \text{ and } \nu_i = 0 \text{ for almost all } i.$$

where the $\mathfrak{p}_i$'s are prime (integral) ideals of O.

Proof. Let $\mathfrak{a}$ be a fractional ideal of O and $c \in K$ be such that $c\mathfrak{a} \subset O$. Define the integral ideal $\mathfrak{b} \coloneqq c\mathfrak{a}$. Then $\mathfrak{a} = \mathfrak{b}(c)^{-1}$ is the quotient of two integral ideals. So if we use the prime factorization on these integral ideals (where we take the product over all prime ideals but only finitely many with non-zero power):

$$\mathfrak{b} = \prod \mathfrak{p}_i^{\nu_i} \text{ and } (c) = \prod \mathfrak{p}_i^{e_i},$$

then

$$\mathfrak{a} = \prod \mathfrak{p}_i^{\nu_i - e_i}$$

and uniqueness follows from the unique factorization of integral ideals. □

Corollary 3.29 allows one to think of the group of fractional ideals J_K as the free Abelian group on the set of prime ideals of O.

Lemma 3.30. *The set of principal fractional ideals forms a subgroup of J_K which we denote by I_K.*

Proof. Suppose we have principal fractional ideals xO and yO, where $x, y \in K$. Then

$$xOyO = xyO$$

is again a principal fractional ideal. Also,

$$(xO)^{-1} = x^{-1}O^{-1} = x^{-1}O$$

□

Definition 3.31. The *ideal class group (or just class group) Cl_K of K* is defined as

$$J_K \big/ I_K = \{\text{all fractional ideals}\} \Big/ \{\text{all principal fractional ideals}\}.$$

We can immediately obtain an exact sequence

$$1 \to O^\times \to K^\times \to J_K \to Cl_K \to 1.$$

We will next show that every ideal of O can be generated by two elements.

Proposition 3.32. *If $\mathfrak{a}, \mathfrak{b} \subset O$ are non-zero ideals, then there exists $\alpha \in \mathfrak{a}$ such that*

$$\alpha\mathfrak{a}^{-1} + \mathfrak{b} = O.$$

This proposition says that given two ideals $\mathfrak{a}, \mathfrak{b}$, there exists an ideal $\mathfrak{c}$ such that $\mathfrak{a}\mathfrak{c}$ is principal, and $(\mathfrak{b}, \mathfrak{c}) = 1$, indeed take $\mathfrak{c} = \alpha\mathfrak{a}^{-1} \subset O$.

Proof. If $\alpha \in \mathfrak{a}$, then $\mathfrak{a}|(\alpha)$ (remember from Lemma 3.19 that "to contain" is equivalent to "to divide", among integral ideals of O). So that $\alpha\mathfrak{a}^{-1}$ is an actual ideal, and not just a fractional one. Indeed, since $\mathfrak{a}|(\alpha)$ means that $(\alpha) = \mathfrak{a}\mathfrak{c}$ for some $\mathfrak{c} \subset O$, therefore $\alpha\mathfrak{a}^{-1} = \mathfrak{c}$. Hence $\alpha\mathfrak{a}^{-1} + \mathfrak{b}$ is the g.c.d. of $\alpha\mathfrak{a}^{-1}$ and $\mathfrak{b}$. We aim to show this g.c.d. is (1). We claim that it suffices to find an $\alpha \in \mathfrak{a}$ such that

$$\alpha\mathfrak{a}^{-1} + \mathfrak{p}_i = O \quad \text{for all } i,$$

where the $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$'s are the distinct prime ideals in the factorization of $\mathfrak{b}$. This will be the case if $\mathfrak{p}_i \nmid \alpha\mathfrak{a}^{-1}$, since then

$$\mathfrak{p}_i \subsetneq \alpha\mathfrak{a}^{-1} + \mathfrak{p}_i.$$

As the $\mathfrak{p}_i$'s are all maximal, $\alpha\mathfrak{a}^{-1} + \mathfrak{p}_i = O$. So it is sufficient to choose $\alpha \in \mathfrak{a} \setminus \mathfrak{a}\mathfrak{p}_i$, for all i. If $r = 1$, by unique factorization $\mathfrak{a} \neq \mathfrak{a}\mathfrak{p}_1$. Hence there is an $\alpha \in \mathfrak{a} \setminus \mathfrak{a}\mathfrak{p}_1$. If $r > 1$, let

$$\mathfrak{a}_i \coloneqq \mathfrak{a}\mathfrak{p}_1 \cdots \mathfrak{p}_{i-1}\mathfrak{p}_{i+1} \cdots \mathfrak{p}_r.$$

Then there exist, once again by unique factorization, $\alpha_i \in \mathfrak{a}_i \setminus \mathfrak{a}_i\mathfrak{p}_i$. Then we can define

$$\alpha \coloneqq \alpha_1 + \cdots + \alpha_r.$$

Then each $\alpha_i \in \mathfrak{a}_i \subset \mathfrak{a}$, hence $\alpha \in \mathfrak{a}$. Suppose by contrary that $\alpha \in \mathfrak{a}\mathfrak{p}_i$ for some i. If $j \neq i$, then $\alpha_j \in \mathfrak{a}_j \subset \mathfrak{a}\mathfrak{p}_i$. Now

$$\alpha_i = \alpha - \alpha_1 - \cdots - \alpha_{i-1} - \alpha_{i+1} - \cdots - \alpha_r \in \mathfrak{a}\mathfrak{p}_i$$

but this contradicts

$$\alpha_i \in \mathfrak{a}_i \setminus \mathfrak{a}_i\mathfrak{p}_i.$$

□

We have the following corollary, which we state as a theorem, that every ideal of O is generated by two elements.

Theorem 3.33. *Let $\mathfrak{a} \subset O$ be an ideal and $0 \neq \beta \in \mathfrak{a}$. Then there exists $\alpha \in \mathfrak{a}$ such that*

$$\mathfrak{a} = (\alpha, \beta).$$

Hence every ideal of O is generated by two elements.

Proof. Let $\mathfrak{b} \coloneqq \beta\mathfrak{a}^{-1}$. Note that since $\beta \in \mathfrak{a}$ we have $\mathfrak{b} \subset O$. By Proposition 3.32, we can find an $\alpha \in \mathfrak{a}$ such that

$$\alpha\mathfrak{a}^{-1} + \mathfrak{b} = O,$$

that is

$$\begin{aligned} \alpha\mathfrak{a}^{-1} + \beta\mathfrak{a}^{-1} &= O \\ ((\alpha) + (\beta))\mathfrak{a}^{-1} &= O \\ (\alpha, \beta) &= \mathfrak{a}. \end{aligned}$$

□

24.10.2019

3.4 The Finiteness of the Ideal Class Group

Our goal now is to prove the finiteness of the ideal class group Cl_K, in the case of K an algebraic number field.

We give here an equivalent definition of the ideal class group: It can be defined using integral ideals and an equivalenve relation on them. Let $I, J \subset O$ be ideals of O. We say $I \sim J$ if there exist $a, b \in O$ such that $aI = bJ$. One can show that

$$\{\text{all integral ideals of } O\}\,/_{\sim} \cong Cl_K.$$

Indeed,

Remark. We know that a Dedekind domain O is a UFD if and only if O is a PID. Let π be an irreducible element that is not prime. Then (π) is not a prime ideal. It has a proper factorization into prime ideals

$$(\pi) = \mathfrak{p}_1 \cdots \mathfrak{p}_r.$$

We claim that none of the $\mathfrak{p}_i$'s are principal. For if $\mathfrak{p}_j = (a)$ for some j, then $(a)|(\pi)$ thus $a|\pi$. However, π is irreducible, so either a is a unit, in which case $(a) = O$, or a is an associate of π and thus $(\pi) = \mathfrak{p}$ which contradicts that π is irreducible but not prime.

If O has unique factorization of its elements into irreducibles, then these irreducibles are primes.

Example 3.34. Let $O = \mathbb{Z}[\sqrt{-17}]$. Then 2 and 3 are irreducibles which are not primes:

$$(2) = (2, 1 + \sqrt{-17})(2, 1 - \sqrt{-17})$$

$$(3) = (3, 1 + \sqrt{-17})(3, 1 - \sqrt{-17}).$$

One can check that all the ideals on the right are non-principal prime ideals.

The following theorem will tell us a little about why we care about the ideal class group.

Theorem 3.35. *The ring of integers $\mathcal{O}_K$ is a UFD if and only if $|Cl_K| = 1$.*

Proof. $\mathcal{O}_K$ is a UFD if and only if every ideal is principal if and only if every fractional ideal is principal. Indeed if $\mathfrak{a}$ is a fractional ideal, then there exists $c \in \mathcal{O}_K$ such that $c\mathfrak{a} \subset \mathcal{O}_K$. So $c\mathfrak{a} = \mathfrak{b}$ is an integral ideal, and thus $\mathfrak{a} = (\mathfrak{b}/c)$.

Therefore $J_K = I_K$, and so

$$Cl_K = J_K \,/ I_K$$

has one element. □

As such, we can think of the ideal class group measuring how close $\mathcal{O}$ is to being a UFD.

Now to prove the finiteness of Cl_K we need to define the *norm* of an ideal.

For the rest of this section, let $[K : \mathbb{Q}] = n$ and $\mathcal{O} \coloneqq \mathcal{O}_K$ the ring of integers.

We have already seen that for any $\mathfrak{a} \subset \mathcal{O}$, $\left|\mathcal{O} \,/ \mathfrak{a}\right|$ is finite (Proposition 3.7 together with prime factorization).

Definition 3.36. Let $\mathfrak{a} \subset \mathcal{O}$ be an (integral) ideal. The *norm of* $\mathfrak{a}$ is defined to be

$$\mathrm{N}(\mathfrak{a}) \coloneqq \left|\mathcal{O} \,/ \mathfrak{a}\right|.$$

The name is justified as we will see that if $\alpha \in \mathcal{O}$, then $\mathrm{N}((\alpha)) = \left|\mathrm{N}_{K/\mathbb{Q}}(\alpha)\right|$.

Recall that given a free $\mathbb{Z}$-module Λ' of rank n and a $\mathbb{Z}$-submodule Λ of Λ' also free of rank n, then if $\{\omega_1, \ldots, \omega_n\}$ is a $\mathbb{Z}$-basis of Λ', and $\{\alpha_1, \ldots, \alpha_n\}$ is a $\mathbb{Z}$-basis of Λ and A is a matrix with integer entries such that

$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = A \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_n \end{pmatrix},$$

then $[\Lambda' : \Lambda] = |\det A|$ and

$$\mathrm{disc}(\alpha_1, \ldots, \alpha_n) = [\Lambda' : \Lambda]^2 \,\mathrm{disc}(\omega_1, \ldots, \omega_n).$$

Proposition 3.37. *1. Let $\mathfrak{a} \subset \mathcal{O}$ be an integral ideal and $\{\alpha_1, \ldots, \alpha_n\}$ be an integral basis of $\mathfrak{a}$ (as a sub $\mathbb{Z}$-module of $\mathcal{O}$). Then*

$$\mathrm{N}(\mathfrak{a}) = \left|\frac{\mathrm{disc}(\alpha_1, \ldots, \alpha_n)}{\mathrm{disc}(K)}\right|^{1/2}.$$

2. If $\alpha \in \mathcal{O}$ then

$$\mathrm{N}((\alpha)) = \left|\mathrm{N}_{K/\mathbb{Q}}(\alpha)\right|.$$

Proof. 1. Let

$$\Lambda' \coloneqq \mathcal{O}_K = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n$$

and

$$\Lambda \coloneqq \mathfrak{a} = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n,$$

then

$$\mathrm{N}(\mathfrak{a}) = \left|\mathcal{O} \,/ \mathfrak{a}\right| = [\Lambda' : \Lambda] = \left|\frac{\mathrm{disc}(\alpha_1, \ldots \alpha_n)}{\mathrm{disc}(\omega_1 \ldots \omega_n)}\right|^{1/2}.$$

2. If $\{\omega_1 \dots \omega_n\}$ is a $\mathbb{Z}$-basis of $\mathcal{O}$ then $\{\alpha\omega_1 \dots \alpha\omega_n\}$ is a basis of (α). So if σ_i runs through the different $\mathbb{Q}$-embeddings of K, then

$$\begin{aligned}\operatorname{disc}(\alpha\omega_1, \dots, \alpha\omega_n) &= \left(\det \begin{pmatrix} \sigma_1(\alpha\omega_1) & \dots & \sigma_1(\alpha\omega_n) \\ \vdots & & \vdots \\ \sigma_n(\alpha\omega_1) & \dots & \sigma_n(\alpha\omega_n) \end{pmatrix}\right)^2 \\ &= (\sigma_1(\alpha)\cdots\sigma_n(\alpha))^2 \left(\det \begin{pmatrix} \sigma_1(\omega_1) & \dots & \sigma_n(\omega_n) \\ \vdots & & \vdots \\ \sigma_n(\omega_1) & \dots & \sigma_n(\omega_n) \end{pmatrix}\right)^2 \\ &= \mathrm{N}_{K/\mathbb{Q}}(\alpha)^2 \operatorname{disc}(K).\end{aligned}$$

Hence by part 1., $\mathrm{N}((\alpha)) = \left|\mathrm{N}_{K/\mathbb{Q}}(\alpha)\right|$.

□

Theorem 3.38. *For non-zero ideals $\mathfrak{a}, \mathfrak{b} \subset \mathcal{O}$ we have*

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

Proof. First note it is enough to show this when $\mathfrak{b} = \mathfrak{p}$ is a prime ideal. Since if $\mathfrak{b} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ then by induction we have

$$\mathrm{N}(\mathfrak{a}\mathfrak{p}_1 \cdots \mathfrak{p}_r) = \mathrm{N}(\mathfrak{a}\mathfrak{p}_1 \cdots \mathfrak{p}_{r-1})\,\mathrm{N}(\mathfrak{p}_r) = \cdots = \mathrm{N}(\mathfrak{a}\mathfrak{p}_1)\,\mathrm{N}(\mathfrak{p}_2 \cdots \mathfrak{p}_r) = \mathrm{N}(\mathfrak{a})\,\mathrm{N}(\mathfrak{b}).$$

Hence assume $\mathfrak{b} = \mathfrak{p}$. Thus we have, by unique factorization

$$\mathfrak{a}\mathfrak{b} = \mathfrak{a}\mathfrak{p} \subsetneq \mathfrak{a} \subset \mathcal{O}_K.$$

Claim:

$$\mathrm{N}(\mathfrak{a}\mathfrak{p}) = \left|\mathcal{O}/\mathfrak{a}\mathfrak{p}\right| = \left|\mathcal{O}/\mathfrak{a}\right|\left|\mathfrak{a}/\mathfrak{a}\mathfrak{p}\right|.$$

This is true because we have a homomorphism of rings

$$\begin{aligned}\phi\colon \mathcal{O}/\mathfrak{a}\mathfrak{p} &\to \mathcal{O}/\mathfrak{a} \\ x + \mathfrak{a}\mathfrak{p} &\mapsto x + \mathfrak{a}\end{aligned}$$

which is surjective with kernel $\mathfrak{a}/\mathfrak{a}\mathfrak{p}$. To prove

$$\mathrm{N}(\mathfrak{a}\mathfrak{p}) = \mathrm{N}(\mathfrak{a})\,\mathrm{N}(\mathfrak{p})$$

we need to show

$$\left|\mathfrak{a}/\mathfrak{a}\mathfrak{p}\right| = \left|\mathcal{O}/\mathfrak{p}\right|.$$

In fact we will show that

$$\mathfrak{a}/\mathfrak{a}\mathfrak{p} \cong \mathcal{O}/\mathfrak{p}.$$

To this end we will start by showing that there is no ideal I strictly between $\mathfrak{a}$ and $\mathfrak{a}\mathfrak{p}$. Indeed, if

$$\mathfrak{a}\mathfrak{p} \subset I \subset \mathfrak{a},$$

then as fractional ideals

$$\mathfrak{a}^{-1}\mathfrak{a}\mathfrak{p} \subset \mathfrak{a}^{-1}I \subset \mathfrak{a}^{-1}\mathfrak{a} = \mathcal{O}$$

and thus

$$\mathfrak{p} \subset \mathfrak{a}^{-1}I \subset \mathcal{O}.$$

Since $\mathfrak{a}^{-1}I \subset \mathcal{O}$ we see that it is actually an integral ideal containing $\mathfrak{p}$. As $\mathfrak{p}$ is maximal, either $\mathfrak{a}^{-1}I = \mathcal{O}$ and thus $I = \mathfrak{a}$; or $\mathfrak{a}^{-1}I = \mathfrak{p}$ and $I = \mathfrak{a}\mathfrak{p}$.

This means for any $a \in \mathfrak{a} \setminus \mathfrak{ap}$,

$$\mathfrak{a} = \mathfrak{ap} + (a)$$

since $\mathfrak{ap} \subsetneq I \subset \mathfrak{a}$. Fix such an a and define the map

$$\begin{aligned} \psi \colon \mathcal{O} &\to \mathfrak{a}/\mathfrak{ap} \\ x &\mapsto ax + \mathfrak{ap} \end{aligned}$$

which is surjective because $\mathfrak{ap} + (a) = \mathfrak{a}$. Its kernel is an ideal and contains the prime ideal $\mathfrak{p}$. Since $\mathfrak{p}$ is maximal, either $\mathfrak{p} = \ker \psi$ which means $\mathfrak{a}/\mathfrak{ap} \cong \mathcal{O}/\mathfrak{p}$; or $\ker \psi = \mathcal{O}$ but then $\mathfrak{a}/\mathfrak{ap}$ is trivial which it is not. □

Theorem 3.39. *Let $\mathfrak{a} \subset \mathcal{O}$ be an ideal. Then:*

1. *If $\mathrm{N}(\mathfrak{a})$ is prime, then $\mathfrak{a}$ is a prime ideal.*
2. *$\mathrm{N}(\mathfrak{a}) \in \mathfrak{a}$ or equivalently $\mathfrak{a} | \mathrm{N}(\mathfrak{a})$.*
3. *If $\mathfrak{a} = \mathfrak{p}$ is a prime ideal then it divides exactly one rational prime $p \in \mathbb{Z}$, and*

   $$\mathrm{N}(\mathfrak{p}) = p^f$$

   for some $f \leq [K : \mathbb{Q}] = n$.
4. *Let $p \in \mathbb{Z}$ be prime. Write*

   $$(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g} = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}$$

   then there exist $f_i \in \mathbb{Z}^+$ such that

   $$\mathrm{N}(\mathfrak{p}_i) = \mathfrak{p}_i^{f_i}$$

   and

   $$\sum_{i=1}^{g} e_i f_i = n.$$

Proof. 1. If $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$, then taking norms

$$p = \mathrm{N}(\mathfrak{p}) = \mathrm{N}(\mathfrak{p}_1) \cdots \mathrm{N}(\mathfrak{p}_r),$$

thus $r = 1$ and $\mathfrak{a}$ is prime.

2. Since $\mathrm{N}(\mathfrak{a}) = \left|\mathcal{O}/\mathfrak{a}\right|$, for any $x \in \mathcal{O}$, $x \,\mathrm{N}(\mathfrak{a}) \in \mathfrak{a}$. In particular $1 \cdot \mathrm{N}(\mathfrak{a}) \in \mathfrak{a}$.
3. If $\mathfrak{a} = \mathfrak{p}$ is a prime ideal, then $\mathcal{O}/\mathfrak{p}$ is a finite field with characteristic p for some prime number $p \in \mathbb{Z}$. So

   $$\left|\mathcal{O}/\mathfrak{p}\right| = p^f$$

   for some f. Since p is the characteristic, it vanishes in the finite field $\mathcal{O}/\mathfrak{p}$. Hence

   $$(p) = p\mathcal{O} \subset \mathfrak{p}.$$

   This tells us that p is unique: If there exists another prime $q \neq p$ then there exits $u, v \in \mathfrak{p}$ such that $pu + qv = 1$. This means

   $$1 \in \mathfrak{p}.$$

   meaning that $\mathfrak{p} = \mathcal{O}$ which is a contradiction.
4. Since the norm is multiplicative, we can extend it to fractional ideals using unique factorization...???

□

Definition 3.40. The unique $p \in \mathbb{Z}$ such that $\mathrm{N}(\mathfrak{p}) = p^f$ is called *the prime lying below* $\mathfrak{p}$.

Example 3.41. Let $\mathcal{O} = \mathbb{Z}[\sqrt{-17}]$ and $\mathfrak{p} = (2, 1 + \sqrt{-17})$. Then $\mathfrak{p}^2 = (2)$ and thus $\mathrm{N}(\mathfrak{p})^2 = 2 \cdot 2 = 4$. So $\mathrm{N}(\mathfrak{p}) = 2$ is prime. Thus $\mathfrak{p}$ is a prime ideal.

29.10.2019

Again, here we use the convention $[K\colon \mathbb{Q}] = n$ a finite extension (i.e. number field), and $\mathcal{O} = \mathcal{O}_K = \mathbb{Z}^K$ is the ring of integers.

Theorem 3.42. *Here we collect some finiteness properties of $\mathcal{O}$.*

1. *Every non-zero ideal $\mathfrak{a} \subset \mathcal{O}$ has a finite number of divisors.*
2. *A non-zero rational integer belongs to only a finite number of ideals of $\mathcal{O}$.*
3. *There are only finitely many integral ideals of given norm, i.e.*

$$|\{\mathfrak{a} \subset \mathcal{O} \mid \mathrm{N}(\mathfrak{a}) = \ell\}| < \infty.$$

Proof. 1. Follows from uniqueness of prime ideal factorization.

2. Suppose $m \in \mathbb{Z}$, then apply part 1. to the ideal (m), then only a finite number of ideals of $\mathcal{O}$ divide (m), i.e. only a finite number of ideals contain (m).

3. Suppose $\mathfrak{a}$ is in the set. Part 2. of Theorem 3.39 says

$$\ell = \mathrm{N}(\mathfrak{a}) \in \mathfrak{a}.$$

Now part 2. says that ℓ can only belong to a finite number of ideals.

□

Using the above theorem, to prove finiteness of the class number $h_K \coloneqq |Cl_K|$ it suffices to show that each ideal class has an integral ideal whose norm is bounded by some uniform constant M which only depends on K.

Lemma 3.43. *Let K be a number field. Then the class group is finite if and only if there exists a constant M which only depends on K such that every ideal class contains an integral ideal of norm at most M.*

Proof. Suppose such an M exists. Then each class has a representative that is an integral ideal with norm bounded by M, but there can only be finitely many such integral ideals. Hence there are only finitely many such representatives and the ideal class group is finite. Conversely, suppose that the ideal class group is finite, take an integral ideal from each class and take M to be the maximum of the norms of these integral ideals. □

The next goal is to find such an M.

Theorem 3.44. *Let K be a number field. Then there exists a constant $M > 0$ such that every integral ideal I of $\mathcal{O}_K$ contains a non-zero element $\alpha \in I$ with $|\mathrm{N}(\alpha)| \leq M\,\mathrm{N}(I)$. Moreover, if $\{\alpha_1, \ldots, \alpha_n\}$ is an integral basis of $\mathcal{O}_K$, then we can take M as*

$$M = \prod_{i=1}^{n} \sum_{j=1}^{n} |\sigma_i(\alpha_j)|.$$

Note that M depends on the choice of the integral basis.

First we note this corollary:

Corollary 3.45. *With M as above, every ideal class contains an integral ideal of norm at most M. Hence $|Cl_K| < \infty$.*

Proof. Let $\mathfrak{a}$ be an arbitrary representative of the class $[\mathfrak{a}]$ in Cl_K. Let $\gamma \in \mathcal{O}_K$ such that $\gamma\mathfrak{a}^{-1} \subset \mathcal{O}_K$ (this is possible because $\mathfrak{a}^{-1}$ is also a fractional ideal). But then $\mathfrak{b} = \gamma\mathfrak{a}^{-1}$ is an integral ideal. Then by Theorem 3.44, there exists a non-zero $\alpha \in \mathfrak{b}$ such that $|\mathrm{N}(\alpha)| \leq M\,\mathrm{N}(\mathfrak{b})$. Let $I = \alpha\mathfrak{b}^{-1}$. Since $\alpha \in \mathfrak{b}$, it follows that $I \subset \mathcal{O}_K$ is an integral ideal. So $I = \alpha\mathfrak{b}^{-1} = \alpha\gamma^{-1}\mathfrak{a} \in [\mathfrak{a}]$. Hence $\mathrm{N}(I) = |\mathrm{N}(\alpha)|\,\mathrm{N}(\mathfrak{b}^{-1}) \leq M\,\mathrm{N}(\mathfrak{b})\,\mathrm{N}(\mathfrak{b}^{-1}) = M$. □

Proof of Theorem 3.44. Let $\alpha_1, \ldots, \alpha_n$ be an integral basis of $\mathcal{O}_K$. Let I be an integral ideal. Choose $m \in \mathbb{Z}$ such that $m^n \leq \mathrm{N}(I) < (m+1)^n$. Consider the subset $S \subset \mathcal{O}_K$ defined by

$$S := \left\{ \sum_{j=1}^{n} m_j \alpha_j \mid 0 \leq m_j \leq m, m_j \in \mathbb{Z} \right\}.$$

Then $|S| = (m+1)^n > \mathrm{N}(I) = [\mathcal{O}_K : I]$ by our choice of m. Hence $S \subset \mathcal{O}_K$ contains more elements than $\mathcal{O}_K/I$. Thus by the pigeon hole principle, there exist two distinct elements $x, y \in S$ which are congruent mod I, i.e. $\alpha = x - y \in I$. Let $\alpha = \sum_{j=1}^{n} m_j \alpha_j \in I$ with $|m_j| \leq m$. Next we estimate the norm of α:

$$|\mathrm{N}(\alpha)| = \left| \prod \sigma_i(\alpha) \right| \leq \prod_{i=1}^{n} \sum_{j=1}^{n} |m_j| |\sigma_i(\alpha_j)| \leq m^n \underbrace{\prod_{i=1}^{n} \sum_{j=1}^{n} |\sigma_i(\alpha_j)|}_{=:\mathrm{M}} \leq \mathrm{N}(I) M.$$

□

Later we will see that we can use Minkowski's theory to give a bound M that does not depend on a basis. We will show that M_K can be taken as

$$M = \left(\frac{2}{\pi} \right)^{r_2} |\operatorname{disc}(K)|^{1/2},$$

and with a bit more work it can be taken as

$$M_K = \left(\frac{4}{\pi} \right)^{r_2} \frac{n!}{n^n} |\operatorname{disc}(K)|^{1/2}$$

where $[K : \mathbb{Q}] = n = r_1 + 2r_2$ and r_1 is the number of real embeddings of K and $2r_2$ is the number of complex embeddings of K.

Example 3.46. If $K = \mathbb{Q}(\sqrt{5})$, then $\operatorname{disc}(K) = 5$, $r_2 = 0$. The Minkowski bound gives $\sqrt{5}/2 = 1.118$. If we use $\{1, (1+5)/2\}$ then Dirichlet's bound $M = 4.23$. So Minkowski's bound gives us much more information, as it tells us that O_K is a PID.

31.10.2019
Last time: $|Cl_K| = h_K < \infty$. The proof of this also suggests a way to construct the class group in some small cases:

1. Given a field K, compute $M_K =$ good bound,
2. then we know every ideal is equivalent to an integral ideal of norm at most M_K. We also know the unique factorization into prime ideals,
3. determine all primes $p < M_K$,
4. determine prime factorization $(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_t^{e_t}$,
5. determine all products of prime ideals having norm $< M_K$. Every integral ideal will be equivalent to at least one ideal on this list.

We have seen that $h_K = 1$ if $K = \mathbb{Q}(\sqrt{5})$. However in general $h_K > 1$ for quadratic fields. Gauss conjectured the following:

Conjecture 3.47 (Gauss)**.** *For $d < 0$, the number of quadratic fields of a given class number is finite.*

Gauss class number problem: Find an effective algorithm for determining all negative discriminants d such that $h_d = n$.

Gauss also conjectured the class number 1 problem:

Conjecture 3.48. *The imaginary quadratic of class number* 1 *are exactly* $d = -1, -4, -7, -8, -11, -19, -43, -67, -163$. *One can check that in all these cases we indeed have* $h_d = 1$.

The solution was given in 1966 by Baker, 1967 by Stark, and 1952 by Heegner, even though his proof was not acknowledged for many years.

Class number 2 problem: 1971 Baker-Stark.

Class number 3 problem 1983 Oesterlé.

h up to 100, Watkins in 2004.

In 1918 Hecke showed that if the generalized Riemann hypothesis (GRH) is true then Gauss's conjecture is true.

Theorem 3.49 (Hecke)**.** *Let* $D < 0$ *and* $\chi : {}^{\mathbb{Z}}/_{D\mathbb{Z}} \to \mathbb{C}$ *be a character modulo* D *(real, primitive). If*

$$\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \neq 0$$

for s *real and*

$$s > 1 - \frac{c}{\log |D|}$$

then

$$h(D) > c_1 \frac{|D|^{1/2}}{\log |D|}$$

where c, c_1 *are fixed abs. constants.*

Theorem 3.50 (Deuring-Mordell-Heillbron, 1933)**.** *If GRH is false, then* $h(D) \to \infty$ *as* $D \to \infty$

Theorem 3.51 (Hecke-Deuring-Mordell-Heillbronn)**.** $h(D) \to \infty$ *as* $-D \to \infty$.

Theorem 3.52 (Siegel)**.** *For every* $\varepsilon > 0$ *there exists a constant* $c > 0$ *(which cannot be effectively computed) such that*

$$h(D) > c|D|^{1/2-\varepsilon}$$

Due to the ineffectiveness in Siegel's theorem, the Gauss class number problem remained unsolved until 1983 due to Gross-Zagier based on previous work of Goldfeld.

For $D > 0$ Gauss conjectured that there are infinitely many real quadratic fields of class number 1. This problem is open.

We will see in the future that Dirichlet's unit theorem says $\mathcal{O}_K^\times$ is a finitely generated abelian group of rank $r = r_1 + r_2 - 1$ where r_1 is number of real embeddings $\sigma \colon K \to \mathbb{R}$ and r_2 is number of complex embeddings $\sigma \colon K \to \mathbb{C}$.

If K is an imaginary quadratic field, $r_1 = 0$ and $r_2 = 1$. So $r = 0$ and $\mathcal{O}_K^\times$ only consists of torsion elements.

If K is real quadratic of discriminant $D > 0$, $r_1 = 2$ and $r_2 = 0$. Hence the infinite part of $\mathcal{O}_K^\times$ is cyclic and a generator ε_D is called a *fundamental unit*. So Siegel's Theorem gives use

$$h_D \log \varepsilon_D > c|D|^{1/2-\varepsilon}.$$

Let

$$\zeta_K(s) \coloneqq \sum_{\mathfrak{a} \text{ integral ideals of } \mathcal{O}_K} \frac{1}{N(\mathfrak{a})^s} = \prod_{\mathfrak{p} \text{ prime}} (1 - \mathrm{N}(\mathfrak{p})^s)^{-1}, \quad \text{for } \mathrm{Re}(s) > 1.$$

Then ζ_K has an analytic continuation to all of $\mathbb{C} \setminus \{1\}$ with a simple pole at $s = 1$ and the residue is given by

$$\operatorname*{Res}_{s=1} \zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2} h_K R}{\omega |d_K|^{1/2}},$$

where R is the *regulator* of K and ω is the number of roots of unity in K. We define the regulator later when we treat Dirichlet's unit theorem.

4 Lattices

Definition 4.1. Let V be an n-dimensional real vector space. A *lattice* in V is a subgroup (under addition) of the form

$$\Gamma = \mathbb{Z}v_1 = \cdots + \mathbb{Z}v_m$$

where $\{v_1, \ldots, v_m\}$ is a linearly independent set of vectors in V.

The vectors $\{v_1, \ldots v_m\}$ are called a *basis* of Γ. To Γ or rather to its generating set $\{v_1, \ldots, v_m\}$ we associate its *fundamental mesh* or the *fundamenal region*

$$\Phi_\Gamma \coloneqq \{\alpha_1 v_1 + \cdots + \alpha_m v_m \mid 0 \leq \alpha_i < 1\}.$$

Γ is called a *complete lattice* if $m = n$. Completeness is equivalent to

$$V = \bigcup_{\gamma \in \Gamma} (\Phi_\Gamma + \gamma).$$

Now recall that a subset Γ of $\mathbb{R}^n$ is *discrete* if for every $r \geq 0$,

$$|(\Gamma \cap B_r(0))| < \infty.$$

Proposition 4.2. *A subgroup Γ of V is a lattice if and only if it is discrete.*

Proof. Assume Γ is a lattice. Let $v_1, \ldots, v_m$ be a basis of Γ, and let

$$\mathbb{R}^m \cong V_0 \coloneqq \langle v_1, \ldots, v_m \rangle$$

Since $v_1, \ldots, v_m$ are linearly independent, we can extend it to a basis $v_1, \ldots, v_n$ for V where $m \leq n$. Now consider the map

$$\phi \colon V \to \mathbb{R}^m$$
$$a_1 v_1 + \cdots + a_n v_n \mapsto (a_1, \ldots, a_m).$$

is linear, and thus continuous.

Let $r \geq 0$ be any radius. Consider the closed ball $B = \overline{B_r(0)}$. Then B is compact, and under the continuous mapping $\phi(B)$ is also compact. If $v = a_1 v_1 + \ldots a_n v_n \in B$, then

$$\|\phi(v)\| = \|(a_1, \ldots a_n)\| \leq M$$

for some M. Hence each $|a_i| \leq M$. However, there are only finitely many points with this property in Γ.

Conversely, suppose $\Gamma \subset V$ is discrete. Let $V_0 \coloneqq \mathrm{Span}_{\mathbb{R}}(\Gamma)$, a subspace of V of dimension $m \leq n$. Let $\{u_1, \ldots u_m\}$ be a basis of V_0 formed from elements in Γ. Let

$$\Gamma_0 = \mathbb{Z}u_1 + \ldots \mathbb{Z}u_m \subset \Gamma$$

which is clearly a subgroup of Γ. So we can write

$$\Gamma = \bigcup_{i \in I} \Gamma_0 + \gamma_i,$$

where γ_i runs over a set of representatives of Γ/Γ_0. Now Γ_0 is complete in V_0, hence

$$V_0 = \bigcup_{\gamma \in \Gamma_0} \Phi_0 + \gamma,$$

where Φ_0 is the fundamental mesh of Γ_0. We have $\gamma_i \in V_0 = \mathrm{Span}\,\Gamma$ hence it is the translate of some element $\mu_i \in \Phi_0$ by an element of Γ_0. But then

$$\Gamma_0 + \gamma_i = \Gamma_0 + \mu_i$$

and so

$$\Gamma = \bigcup_{i \in I} \Gamma_0 + \mu_i.$$

However, $\mu_i \in \Gamma$ and $\mu_i \in \Phi_0$. As Γ is discrete, $\Gamma \cap \Phi_0$ is finite, i.e. Γ/Γ_0 is finite. Say $[\Gamma : \Gamma_0] = q$. So $q\Gamma \subset \Gamma_0$. Hence

$$\Gamma \subset \mathbb{Z}\left(\frac{1}{q}u_1\right) + \cdots + \mathbb{Z}\left(\frac{1}{q}u_m\right)$$

and so Γ is a subgroup of a free abelian group of rank m. Thus, Γ admits a $\mathbb{Z}$-basis. i.e.

$$\Gamma = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_r.$$

In fact the set $\{v_1, \dots v_r\}$ span $V_0 = \mathrm{Span}_{\mathbb{R}}(\Gamma)$ which has dimension m and thus $r = m$. □

Proposition 4.3. *A lattice Γ is complete if and only if there exists a bounded set $B_V \subset V$ such that the collection of all translates $M + \gamma, \gamma \in \Gamma$, covers the entire space V, i.e.*

$$V = \bigcup_{\gamma \in \Gamma} (B_V + \gamma).$$

Proof. If $\Gamma = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n$ is complete, then one may take M to be the fundamental mesh $\Phi = \{x_1v_1 + \cdots + x_nv_n \mid 0 \le x_i < 1\}$.

Conversely, let M be a bounded subset of V whose translates $M + \gamma$, for $\gamma \in \Gamma$, cover V. Let V_0 be the subspace spanned by Γ. We have to show that $V = V_0$. So let $v \in V$. Since $V = \bigcup_{\gamma \in \Gamma}(M + \gamma)$ we may write, for each $k \in \mathbb{N}$,

$$kv = a_k + \gamma_k, \quad a_k \in M, \gamma_k \in \Gamma \subset V_0.$$

Now since M is bounded, $\lim_{k\to\infty} \frac{1}{k}a_k$ converges to zero, and V_0 is closed, thus

$$v = \lim_{k\to\infty} \frac{a_k}{k} + \lim_{k\to\infty} \frac{\gamma_k}{k} = \lim_{k\to\infty} \frac{\gamma_k}{k} \in V_0.$$

□

In $\mathbb{R}^n$ we have a natural inner product and we can define lengths, norms, volumes. The cube spanned by the orthonormal basis $e_1, \dots, e_n$ has volume 1. More generally a prallelopiped spanned by n linearly independent vectors $\{v_1, \dots, v_n\}$

$$\Phi = \{x_1v_1 + \cdots + x_nv_n \mid 0 \le x_i < 1\}$$

has a volume

$$\mathrm{vol}(\Phi) = |\det A|,$$

where $A = (a_{ik})$ is the change of basis matrix from the basis $e_1, \dots, e_n$ to $v_1, \dots, v_n$, so that $v_i = \sum_k a_{ik}e_k$.

Using this we can define the volume of a lattice as the volume of the fundamental mesh:

Definition 4.4. Let $\Gamma = \mathbb{Z}v_1 + \dots v_m\mathbb{Z} \subset V$ be a lattice and Φ_Γ be its fundamental mesh. Then we define the *volume of* Γ as

$$\mathrm{vol}(\Gamma) \coloneqq \mathrm{vol}(\Phi_\Gamma).$$

Lemma 4.5. *Suppose $\Gamma = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_m$ is a lattice in $\mathbb{R}^n$, where $m \le n$. If $v_i = (a_{i1}, \dots, a_{in})$. Then*

$$\mathrm{vol}(\Gamma) = |\det(a_{ij})| = |\det\langle v_i, v_j\rangle|^{1/2}.$$

Proof. We have

$$(\langle v_i, v_j\rangle)_{0\le i,j\le m} = \left(\sum_{k,\ell} a_{ik}a_{j\ell}\langle e_k, e_\ell\rangle\right)_{0\le i,j\le m} = \left(\sum_k a_{ik}a_{jk}\right) = AA^T.$$

Therefore

$$\det(A)^2 = \det(\langle v_i, v_j\rangle)_{0\le i,j\le m}$$

and thus

$$\mathrm{vol}(\Gamma) = |\det(A)| = \left|\det(\langle v_i, v_j\rangle)_{0\le i,j\le m}\right|^{1/2}.$$

□

Definition 4.6. A region $X \subset V$ in the n-dimensional vector space V is called *centrally symmetric* if $x \in X$ implies $-x \in X$. A region is called *convex* if given $x, y \in X$, and $t \in [0,1]$, then $tx + (1-t)y \in X$.

Then we have the following theorem:

Theorem 4.7 (Minkowski's Lattice Point Theorem)**.** *Let* $\dim V = n$ *and* Γ *be a complete lattice in* V*. Suppose* X *is a convex centrally symmetric subset of* V *and*

$$\mathrm{vol}(X) > 2^n \,\mathrm{vol}(\Gamma).$$

Then X *contains at least one non-zero lattice ppint in* V*.*

5.11.2019

Proof. It is enough to show the following claim:
There exist distinct $\gamma_1, \gamma_2 \in \Gamma$ such that

$$\left(\frac{1}{2}X + \gamma_1\right) \cap \left(\frac{1}{2}X + \gamma_2\right) \neq \emptyset.$$

To see why the claim suffices, suppose there exist such γ_1, γ_2 as above. Then it is true that there exist $x_1, x_2 \in X$ such that $\frac{1}{2}x_1 + \gamma_1 = \frac{1}{2}x_2 + \gamma_2$. But then

$$0 \neq \gamma_1 - \gamma_2 = \frac{1}{2}x_2 - \frac{1}{2}x_1 \in X,$$

since X is symmetric and convex. Thus we have found a lattice point $\gamma_1 - \gamma_2$ in X.

Now to prove the claim, assume on the contrary that the sets $\frac{1}{2}X + \gamma$ for $\gamma \in \Gamma$ are pairwise disjoint. Then $(\frac{1}{2}X + \gamma) \cap \Phi_\Gamma$ are pairwise disjoint as well. Hence

$$\mathrm{vol}(\Phi_\Gamma) \ge \sum_{\gamma\in\Gamma} \mathrm{vol}\left(\Phi_\Gamma \cap \left(\frac{1}{2}X + \gamma\right)\right)$$

and further

$$\mathrm{vol}\left(\Phi_\Gamma \cap \left(\frac{1}{2}X + \gamma\right)\right) = \mathrm{vol}\left((\Phi_\Gamma - \gamma) \cap \frac{1}{2}X\right).$$

By assumption Γ is a complete lattice, so the sets $\Phi_\Gamma - \gamma$ cover V. So the sets $(\Phi_\Gamma - \gamma) \cap \frac{1}{2}X$ cover $\frac{1}{2}X$. Thus,

$$\mathrm{vol}(\Phi_\Gamma) \ge \sum \mathrm{vol}\left((\Phi_\Gamma - \gamma) \cap \frac{1}{2}X\right) = \mathrm{vol}\left(\frac{1}{2}X\right) = 2^{-n}\,\mathrm{vol}(X),$$

contradicting our hypothesis on $\mathrm{vol}(X)$. □

Our next goal is to attach a lattice to $\mathcal{O}_K$ and to ideals in $\mathcal{O}_K$.

Example 4.8 (Imaginary Quadratic)**.** Let $K = \mathbb{Q}(\sqrt{-3})$, then $\mathcal{O}_K = \mathbb{Z}[(1+\sqrt{-3})/2]$. A basis of $\mathcal{O}_K$ is $\{1, (1+\sqrt{-3})/2\}$.

In Figure 1 we see that the basis vectors of $\mathcal{O}_K$ naturally span a lattice in the $\mathbb{R}$-vector space $\mathbb{C}$. with a fundamental mesh given by the shaded region.

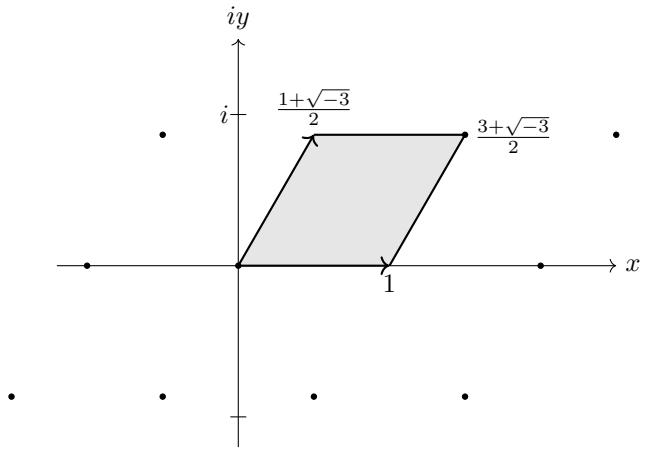


Figure 1: $\mathbb{Z}[(1+\sqrt{-3})/2]$ as a lattice in $\mathbb{C}$

Consider the map

$$\begin{aligned} i\colon \mathcal{O}_K &\to \mathbb{R}^2 \\ 1 &\mapsto (1,0) \\ \frac{1+\sqrt{-3}}{2} &\mapsto \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right) \end{aligned}$$

Then

$$\operatorname{vol}(i(\mathcal{O}_K)) = \det \begin{pmatrix} 1 & 1/2 \\ 1 & \sqrt{3}/2 \end{pmatrix} = \sqrt{3}/2 = 2^{-1}|\delta_K|^{1/2}.$$

Example 4.9 (Real Quadratic Case)**.** Let $K = \mathbb{Q}(\sqrt{2})$, then $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}] = \mathbb{Z} + \mathbb{Z}[\sqrt{2}]$.

Define $i\colon \mathcal{O}_K \to \mathbb{R}^2$, $(x + y\sqrt{2}) \mapsto (x + y\sqrt{2}, x - y\sqrt{2})$, $1 \mapsto (1, 1)$ and $\sqrt{2} \mapsto (\sqrt{2}, -\sqrt{2})$. Then

$$\mathrm{vol}(i(\mathcal{O}_K)) = \det \begin{pmatrix} 1 & \sqrt{2} \\ 1 & -\sqrt{2} \end{pmatrix} = 2\sqrt{2} = |\delta_K|^{1/2}.$$

We can see that $\mathcal{O}_K$ is mapped under i to a lattice, where the fundamental mesh is the shaded region in Figure 2.

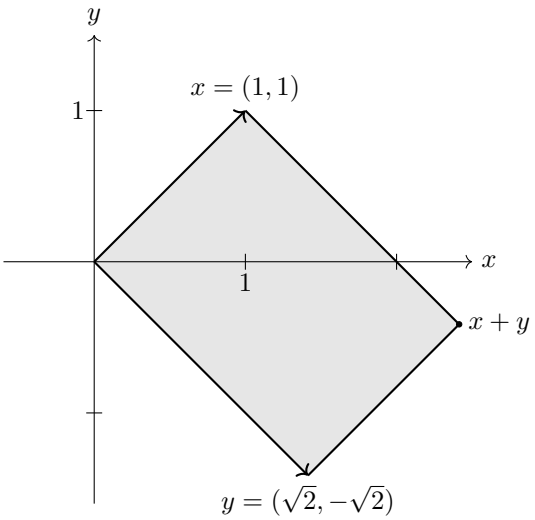


Figure 2: The image of the basis vectors of $\mathbb{Z}[\sqrt{2}]$ under i.

5 Minkowski Theory

For this section, as usual , we fix K to be a number field of degree n over $\mathbb{Q}$, and $\mathcal{O} = \mathcal{O}_K$ the ring of integers.

5.1 Embedding of $\mathcal{O}_K$ as a Lattice in $\mathbb{R}^n$

Let $\sigma_1, \dots, \sigma_n$ be the set of all K-embeddings into $\mathbb{C}$. If $\sigma_i(K) \subset \mathbb{R}$, we say σ_i is *real* and otherwise we call it *complex*. Define $\bar{\sigma}_i(\alpha) = \overline{\sigma_i(\alpha)}$. Since complex conjugation is an automorphism of $\mathbb{C}$, $\bar{\sigma}_i$ is also a K-embedding and hence $\bar{\sigma}_i = \sigma_j$ for some j and $\sigma_i = \bar{\sigma}_i$ if σ_i is real. So we have either real or pairs of complex embeddings. Therefore, let us write $n = r_1 + 2r_2$, where r_1 is the number of real embeddings and r_2 is the number of pairs of complex embeddings.

We standardize the notation of the embeddings as

$$\sigma_1, \dots, \sigma_{r_1}, \sigma_{r_1+1}, \bar{\sigma}_{r_1+1}, \dots, \sigma_{r_1+r_2}, \bar{\sigma}_{r_1+r_2},$$

where σ_i is real for $1 \le i \le r_1$ and complex otherwise.

Next, define

$$K_{\mathbb{R}} = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} = \{x = (x_1, \dots, x_{r_1}, x_{r_1+1}, \dots, x_{r_1+r_2}) \mid x_i \in \mathbb{R} \text{ for } 1 \le i \le r_1 \text{ and } x_j \in \mathbb{C} \text{ for } r_1{+}1 \le j \le r_1{+}r_2\}.$$

Then $K_{\mathbb{R}}$ is a n-dimensional vector space over $\mathbb{R}$ and also a ring under componentwise addition and multiplication. For $x \in K_{\mathbb{R}}$ we define the norm of x as

$$\mathrm{N}(x) := x_1 \cdots x_r |x_{r_1+1}|^2 \cdots |x_{r_1+r_2}|^2.$$

The norm $\mathrm{N}(x)$ is real for all $x \in K_{\mathbb{R}}$ and multiplicative.
Define a map $i \colon K \to K_{\mathbb{R}}$ by $\alpha \mapsto (\sigma_1(\alpha), \dots, \sigma_{r_1}(\alpha), \sigma_{r_1+1}(\alpha), \dots, \sigma_{r_1+r_2}(\alpha))$. Then clearly

$$i(\alpha + \beta) = i(\alpha) + i(\beta) \text{ and } i(\alpha\beta) = i(\alpha)i(\beta).$$

So i is in fact a ring morphism. Furthermore, we have

$$\mathrm{N}_{K/\mathbb{Q}}(\alpha) = \sigma_1(\alpha) \cdots \sigma_{r_1}(\alpha)\sigma_{r_1+1}(\alpha)\bar{\sigma}_{r_1+1}(\alpha) \cdots \sigma_{r_1+r_2}(\alpha)\bar{\sigma}_{r_1+r_2}(\alpha) = \mathrm{N}(i(\alpha)).$$

Theorem 5.1. *If $\alpha_1, \dots, \alpha_n$ is a basis of K over $\mathbb{Q}$ (viewing K as an n-dimensional $\mathbb{Q}$-vector space), then $i(\alpha_1), \dots, i(\alpha_n)$ are linearly independent over $\mathbb{R}$ in the vector space $K_{\mathbb{R}}$.*

Proof. First note that that the kernel of $i \colon K \to K_{\mathbb{R}} = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} = \mathbb{R}^n$ is an ideal of K. Since K is a field, i is therefore identically 0 or injective. The linear independence over $\mathbb{Q}$ is obvious. We want more though, we want linear independence over $\mathbb{R}$. To show linear independence of $i(\alpha_1), \dots, i(\alpha_n)$, it is enough to show that the $n \times n$ matrix obtained by writing the n column vectors $i(\alpha_1), \dots, i(\alpha_n)$ in terms of their coordinates in $\mathbb{R}^n$ has non-zero determinant.

Call that matrix A, i. e.

$$A = \begin{pmatrix} \sigma_1(\alpha_1) & \dots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_{r_1}(\alpha_1) & \dots & \sigma_{r_1}(\alpha_n) \\ \mathrm{Re}(\sigma_{r_1+1}(\alpha_1)) & \dots & \mathrm{Re}(\sigma_{r_1+1}(\alpha_n)) \\ \mathrm{Im}(\sigma_{r_1+1}(\alpha_1)) & & \mathrm{Im}(\sigma_{r_1+1}(\alpha_n)) \\ \vdots & \ddots & \vdots \\ \mathrm{Re}(\sigma_{r_1+r_2}(\alpha_1)) & \dots & \mathrm{Re}(\sigma_{r_1+r_2}(\alpha_n)) \\ \mathrm{Im}(\sigma_{r_1+r_2}(\alpha_1)) & \dots & \mathrm{Im}(\sigma_{r_1+r_2}(\alpha_n)) \end{pmatrix}.$$

We apply the elementary row operations of adding $i\,\mathrm{Im}(\sigma_{r_1+k}(\alpha_j))$ to $\mathrm{Re}(\sigma_{r_1+k}(\alpha_j))$ to get

$$\begin{pmatrix} \sigma_1(\alpha_1) & \dots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_{r_1}(\alpha_1) & \dots & \sigma_{r_1}(\alpha_n) \\ \sigma_{r_1+1}(\alpha_1) & \dots & \sigma_{r_1+1}(\alpha_n) \\ \mathrm{Im}(\sigma_{r_1+1}(\alpha_1)) & \dots & \mathrm{Im}(\sigma_{r_1+1}(\alpha_n)) \\ \vdots & \ddots & \vdots \\ \sigma_{r_1+r_2}(\alpha_1) & \dots & \sigma_{r_1+r_2}(\alpha_n) \\ \mathrm{Im}(\sigma_{r_1+r_2}(\alpha_1)) & \dots & \mathrm{Im}(\sigma_{r_1+r_2}(\alpha_n)) \end{pmatrix}.$$

This does not change the determinant so far. Then we multiply each imaginary row $\mathrm{Im}(\sigma_{r_1+k}(\alpha_j))$ by $-2i$ and add $\sigma_{r_1+k}(\alpha_j)$ to $-2i\,\mathrm{Im}(\sigma_{r_1+k}(\alpha_j))$ to get $\bar{\sigma}_{r_1+k}(\alpha_j)$.

So in total we get with $\tilde{A} = (\sigma_i(\alpha_j))$ that

$$\det(A) = (-2i)^{-r_2} \det\left(\tilde{A}\right) = (-2i)^{-r_2} \sqrt{\mathrm{disc}(K)} \neq 0.$$

□

07.11.2019

Corollary 5.2. *Same setup as before, let K be a degree n extension of $\mathbb{Q}$.*

1. *$\mathbb{Q}$-linearly independent elements of K map under i to $\mathbb{R}$-linearly independent elements of $K_\mathbb{R}$.*
2. *If G is a subgroup of $(K,+)$ with $\mathbb{Z}$-basis $\{\alpha_1,\dots,\alpha_n\}$, then the image of G in $K_\mathbb{R}$ is a lattice in $K_\mathbb{R}$ with generators $i(\alpha_1),\dots,i(\alpha_n)$.*

Since $K_\mathbb{R}$ is isomorphic to $\mathbb{R}^n$, we want to transfer the Euclidean metric to $K_\mathbb{R}$. This means choosing a basis of $K_\mathbb{R}$ and defining an inner product with respect to which this basis is orthonormal. The natural basis to choose is the following:

$$\begin{gathered} (1,0,\dots;0,\dots,0) \\ \vdots \\ (0,0,\dots,1;0,\dots,0) \\ (0,0,\dots;1,0,\dots,0) \\ (0,0,\dots;i,0,\dots,0) \\ \vdots \\ (0,0,\dots;0,0,\dots,0,1) \\ (0,0,\dots;0,0\dots,i) \end{gathered}$$

With this basis chosen, an element $x \in K_\mathbb{R}$

$$x = (x_1,\dots,x_{r_1};u_1+v_1i,\dots,u_{r_2}+v_{r_2}i)$$

has coordinates

$$(x_1,\dots,x_{r_1};u_1,v_1,u_2,v_2,\dots,u_{r_2},v_{r_2}).$$

Let $\tilde{x} = (\tilde{x}_1,\dots,\tilde{x}_{r_1};\tilde{u}_1,\tilde{v}_1,\tilde{u}_2,\tilde{v}_2,\dots,\tilde{u}_{r_2},\tilde{v}_{r_2})$ be another element written in terms of the basis. Thus we can define the inner product

$$\langle x,\tilde{x}\rangle \coloneqq x_1\tilde{x}_1+\dots+u_1\tilde{u}_1+v_1\tilde{v}_1+\dots u_{r_2}\tilde{u}_{r_2}+v_{r_2}\tilde{v}_{r_2}$$

so

$$\|x\| = \sqrt{\langle x,x\rangle} = \sqrt{x_1^2+\dots+x_{r_1}^2+u_1^2+v_1^2+\dots+v_{r_2}^2}.$$

Theorem 5.3. *Let $\mathcal{O} = \mathcal{O}_K$ be the ring of integers. Let $\mathfrak{a} \subset \mathcal{O}$ be an ideal. Then $i(\mathfrak{a})$ is a lattice of rank n in $K_{\mathbb{R}}$. The volume of the fundamental mesh for $i(\mathfrak{a})$ in $K_{\mathbb{R}}$ is*

$$2^{-r_2}\,\mathrm{N}(\mathfrak{a})|\mathrm{disc}(K)|^{1/2}.$$

Proof. The fact that $i(\mathfrak{a})$ is a lattice of rank n is a corollary of Theorem 5.1. More precisely, we know that $\mathfrak{a}$ has a $\mathbb{Z}$-basis $\{\alpha_1, \ldots, \alpha_n\}$, then

$$i(\mathfrak{a}) = \mathbb{Z}i(\alpha_1) + \cdots + \mathbb{Z}i(\mathfrak{a}_n) \subset K_{\mathbb{R}} = \mathbb{R}^n$$

is a lattice since the $i(\alpha_j)'s$ are linearly independent.

On the other hand, if we let

$$A = \begin{pmatrix} \sigma_1(\alpha_1) & \ldots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_{r_1}(\alpha_1) & \ldots & \sigma_{r_1}(\alpha_n) \\ \mathrm{Re}(\sigma_{r_1+1}(\alpha_1)) & \ldots & \mathrm{Re}(\sigma_{r_1+1}(\alpha_n)) \\ \mathrm{Im}(\sigma_{r_1+1}(\alpha_1)) & & \mathrm{Im}(\sigma_{r_1+1}(\alpha_n)) \\ \vdots & \ddots & \vdots \\ \mathrm{Re}(\sigma_{r_1+r_2}(\alpha_1)) & \ldots & \mathrm{Re}(\sigma_{r_1+r_2}(\alpha_n)) \\ \mathrm{Im}(\sigma_{r_1+r_2}(\alpha_1)) & \ldots & \mathrm{Im}(\sigma_{r_1+r_2}(\alpha_n)) \end{pmatrix}.$$

and

$$\tilde{A} = (\sigma_i(\alpha_j))_{0 \le i,j \le n}$$

be as in Theorem 5.1, then

$$\mathrm{vol}(i(\mathfrak{a})) = |\det A|,$$

(notice here that A is the base change matrix because of the way the map i is defined) and

$$|\det A| = 2^{-r_2}\left|\det \tilde{A}\right|.$$

Moreover,

$$\left|\det \tilde{A}\right|^2 = \mathrm{disc}(\alpha_1, \ldots, \alpha_n).$$

We have seen

$$\mathrm{N}(\mathfrak{a}) = \left|\frac{\mathrm{disc}(\alpha_1, \ldots, \alpha_n)}{\mathrm{disc}(K)}\right|^{1/2}.$$

This gives

$$\mathrm{vol}(i(\mathfrak{a})) = 2^{-r_2}\,\mathrm{N}(\mathfrak{a})|\mathrm{disc}(K)|^{1/2}.$$

□

5.2 Finding a Good Bound

Recall that to show $h_K < \infty$ we argued as follows: Suppose there exists M such that every ideal $\mathfrak{a}$ contains a non-zero $\alpha \in \mathfrak{a}$ with $|\mathrm{N}(\alpha)| \le M\,\mathrm{N}(\mathfrak{a})$; then we used that every ideal class is represented by an integral ideal of norm at most M, hence $h_K < \infty$. **So showing $h_K < \infty$ boils down to showing that non-zero ideals contain elements of small norm**.

If we have $X \subset \mathbb{R}^n$ a convex symmetric region such that

$$\mathrm{vol}\, X > 2^n\,\mathrm{vol}(i(\mathfrak{a}))$$

then Minkowski's Lattice Point Theorem provides us with a non-zero $\alpha \in \mathfrak{a}$ having $i(\alpha) \in X$. We want to choose X so that having $i(\alpha) \in X$ forces $|\mathrm{N}(\alpha)|$ to be small.

For each $M > 0$, there is a natural region $X_0(M) \subset \mathbb{R}^n$ corresponding precisely to the condition $|\mathrm{N}(\alpha)| \leq M$. Namely,

$$X_0(M) = \left\{ (x_1, \ldots, x_n) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} = K_{\mathbb{R}} \colon \prod_{i=1}^{r_1} |x_i| \prod_{j=r_1+1}^{r_1+r_2} |x_j|^2 \leq M \right\}.$$

The problem is X_0 is not convex, for example:

Example 5.4. Let K be real quadratic so that $r_1 = 2$ and $r_2 = 0$. Then

$$X_0(1) = \{(x_1, x_2) \mid |x_1 x_2| \leq 1\}$$

which is not convex. But note that it contains a region given by conditions

$$X_1(1) = \{(x_1, x_2) \mid |x_1| < 1, |x_2| < 1\}.$$

This is a guiding example together with the following proposition.

Proposition 5.5. *If Λ is a complete lattice in $K_{\mathbb{R}}$ of dimension $n = r_1 + 2r_2$ having a fundamental mesh of volume V, and if $c_1, \ldots, c_{r_1}, c_{r_1+1}, \ldots, c_{r_1+r_2}$ are positive real numbers whose product*

$$c_1 \cdots c_{r_1+r_2} > \left(\frac{4}{\pi}\right)^{r_2} \cdot V,$$

then there exists a non-zero $x = (x_1, \ldots, x_{r_1+r_2}) \in \Lambda$ such that

$$|x_1| < c_1, \ldots, |x_{r_1}| < c_{r_1}, |x_{r_1+1}|^2 < c_{r_1+1}, \ldots, |x_{r_1+r_2}|^2 < c_{r_1+r_2}. \tag{2}$$

Proof. Let

$$X = \{(x_1, \ldots, x_{r_1+r_2}) \in K_{\mathbb{R}} \mid (2) \text{ holds}\}.$$

Note that X is a Cartesian product of line segments and circular regions, hence convex; it is also symmetric and

$$\begin{aligned}
\mathrm{vol}(X) &= \int_{-c_1}^{c_2} \mathrm{d}x_1 \cdots \int_{-c_{r_1}}^{c_{r_2}} \mathrm{d}x_{r_1} \iint\limits_{u_1^2+v_1^2<c_{r_1+1}} \mathrm{d}u_1 \mathrm{d}v_1 \cdots \iint\limits_{u_{r_2}^2+v_{r_2}^2<c_{r_1+r_2}} \mathrm{d}u_{r_2} \mathrm{d}v_{r_2} \\
&= (2c_1)(2c_2)\cdots(2c_{r_1})(\pi c_{r_1+1})\cdots(\pi c_{r_1+r_2}) \\
&= 2^{r_1}\pi^{r_2} c_1 \cdots c_{r_1+r_2}.
\end{aligned}$$

Minkowski's Lattice Point Theorem gives us the result if

$$\mathrm{vol}(X) > 2^n V$$

i.e. provided that

$$c_1 \cdots c_{r_1+r_2} > \left(\frac{4}{\pi}\right)^{r_2} \cdot V$$

but this is exactly what we assumed about the c_i's □

As a corollary we get

Theorem 5.6. *If $0 \neq \mathfrak{a} \subset \mathcal{O}$ is an ideal, then there exists a non-zero element $\alpha \in \mathfrak{a}$ with*

$$\mathrm{N}(\alpha) \leq \left(\frac{2}{\pi}\right)^{r_2} \mathrm{N}(\mathfrak{a}) |\mathrm{disc}(K)|^{1/2}.$$

Proof. Let $\Lambda = i(\mathfrak{a})$ the lattice in $K_{\mathbb{R}}$, then by Theorem 5.3 its volume is

$$V = \mathrm{vol}(\Lambda) = 2^{-r_2}\,\mathrm{N}(\mathfrak{a})|\mathrm{disc}(K)|^{1/2}$$

and hence

$$\left(\frac{4}{\pi}\right)^{r_2} \cdot V = \left(\frac{2}{\pi}\right)^{r_2} \mathrm{N}(\mathfrak{a})|\mathrm{disc}(K)|^{1/2}.$$

For fixed arbitrary $\varepsilon > 0$ choose real numbers $c_1, \cdots, c_{r_1+r_2}$ such that

$$c_1 \cdots c_{r_1+r_2} = \left(\frac{2}{\pi}\right)^{r_2} \mathrm{N}(\mathfrak{a})|\mathrm{disc}(K)|^{1/2} + \varepsilon > \left(\frac{4}{\pi}\right)^{r_2} \cdot V.$$

By Proposition 5.5, there exists $0 \neq \alpha \in \mathfrak{a}$ such that

$$|\sigma_1(\alpha)| < c_1, \ldots, |\sigma_{r_1}(\alpha)| < c_{r_1}, |\sigma_{r_1+1}(\alpha)|^2 < c_{r_1+1}, \ldots, |\sigma_{r_1+r_2}(\alpha)|^2 < c_{r_1+r_2}.$$

Multyplying these inequalities together gives

$$|\mathrm{N}(\alpha)| < c_1 \cdots c_{r_1+r_2} = \left(\frac{2}{\pi}\right)^{r_2} |\mathrm{N}(\alpha)||\mathrm{disc}(K)|^{1/2} + \varepsilon$$

Since Λ is discrete, the set of such α

$$A_\varepsilon \coloneqq \{\alpha \in \mathfrak{a} \mid \mathrm{N}(\alpha) < c_1 \cdots c_{r_1+r_2}\}$$

is finite for all $\varepsilon > 0$. It is also non-empty by Minkowski's Lattice Point Theorem, and so taking the intersection over all possible ϵ's, which is an intersection of non-empty sets with finitely many possible elements in every set gives a non-empty set:

$$A \coloneqq \bigcap_{\epsilon > 0} A_\varepsilon \neq \emptyset.$$

If we pick $\alpha \in A$ then

$$\mathrm{N}(\alpha) < \left(\frac{2}{\pi}\right)^{r_2} \mathrm{N}(\mathfrak{a})|\mathrm{disc}(K)|^{1/2} + \varepsilon, \text{ for all } \varepsilon,$$

and hence

$$\mathrm{N}(\alpha) < \left(\frac{2}{\pi}\right)^{r_2} \mathrm{N}(\mathfrak{a})|\mathrm{disc}(K)|^{1/2}.$$

□

Thus for M in our proof of $h_K < \infty$ we could take

$$M = \left(\frac{2}{\pi}\right)^{r_2} |\mathrm{disc}(K)|^{1/2}.$$

But when we actually want to say more about Cl_K, better bounds help.

The convex region we used to get the above M is a hypercube. Something spherical can be better. For example in $\mathbb{R}^2$

$$\{(x_1, x_2) \mid |x_1| < 1, |x_2| < 1\}$$

has area 4 which has no non-zero lattice points, i.e. no points have integer coordinates. On the other hand, there is no circle of area more than π containing no lattice points. Even better is to use a diamond shaped area whose sides are diagonal and parallel to $\pm x = y$. Any such square whose area is bigger than 2 will have a lattice point. So we have the following sets:

$$X_0 = \{(x, y) \mid |xy| < 1\} \quad \text{has lattice points, not convex}$$
$$X_1 = \{(x, y) \mid |x| < 1, |y| < 1\} \quad \text{no lattice points, convex}$$

$$X_2 = \{(x,y) \mid x^2 + y^2 < 1\} \quad \text{no lattice points, convex}$$
$$X_3 = \{(x,y) \mid |x| + |y| < 2\} \quad \text{has lattice points, convex}$$

To see algebraically that $X_3 \subset X_0$, one can use the arithmetic geometric mean inequality

$$\sqrt{ab} \leq \frac{a+b}{2}, \quad \text{for } a, b > 0$$

to get

$$|ab| \leq \frac{(|a| + |b|)^2}{4}.$$

To make a good choice for X, we will use the general version of the arithmetic geometric mean inequality:

Lemma 5.7 (AGM)**.** *Let $b_1, \ldots, b_n$ be any non-negative real numbers. Then*

$$A := \frac{b_1 + \cdots + b_n}{n} \geq (b_1 \cdots b_n)^{1/n} =: G.$$

Now let

$$X_t := \{(x_1, \ldots, x_{r_1}; u_1 + iv_1, \ldots, u_{r_2} + iv_{r_2}) \in K_{\mathbb{R}} \mid |x_1| + \cdots + |x_{r_1}| + 2|u_1 + iv_1| + \cdots + 2|u_{r_2} + iv_{r_2}| \leq t\}.$$

Exercise 5.8. 1. X_t is convex

2. $\mathrm{vol}(X_t) = \frac{t^n}{n!} 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2}$

A motivation for the definition of X_t is the following: Consider $\alpha \in K$ so that $i(\alpha) \in X_t$ and suppose $i(\alpha) = (x_1, \ldots, x_{r_1+r_2})$ with $x_1 = \sigma_1(\alpha), \ldots, x_{r_1} = \sigma_{r_1}(\alpha)$ and $2|x_k| = |x_k| + |\bar{x}_k|$ for $r_1 + 1 \leq k \leq r_1 + r_2$. Then

$$t \geq \sum_{i=1}^{r_1} |x_i| + 2 \sum_{j=r_1+1}^{r_1+r_2} |x_j| = \sum_{i=1}^{r_1} |\sigma_i(\alpha)| + \sum_{j=r_1+1}^{r_1+r_2} \left(|\sigma_j(\alpha)| + \left|\overline{\sigma_j(\alpha)}\right|\right)$$

Now using AGM,

$$|\mathrm{N}(\alpha)|^{1/n} = \left(\prod_\sigma |\sigma(\alpha)|\right)^{1/n} \leq \frac{1}{n} \sum_\sigma |\sigma(\alpha)|.$$

Notice that the right-hand-side is $1/n$ times the right-hand-side of the previous equation. Hence, if $i(\alpha) \in X_t$, then

$$|\mathrm{N}(\alpha)|^{1/n} \leq t/n,$$

or equivalently

$$|\,\mathrm{N}(\alpha)| \leq (t/n)^n.$$

Now choose t so that $\mathrm{vol}(X_t) > 2^n \,\mathrm{vol}(i(\mathfrak{a}))$. This is possible by the following argument: Using Theorem 5.3 and Exercise 5.8, we can write this inequality as

$$2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{t^n}{n!} > 2^{r_1+2r_2} 2^{-r_2} \,\mathrm{N}(\mathfrak{a}) |\mathrm{disc}(K)|^{1/2}.$$

So we just need to choose t such that

$$t^n = n! \frac{4}{\pi}^{r_2} |\mathrm{disc}(K)|^{1/2} \,\mathrm{N}(\mathfrak{a}) + \varepsilon.$$

Then by Minkowski's Lattice Point Theorem there exists an $\alpha \in \mathfrak{a}$ with $i(\alpha) \in X_t$ and

$$\mathrm{N}(\alpha) \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^{r_2} \sqrt{|\mathrm{disc}(K)|}\,\mathrm{N}(\mathfrak{a}).$$

This implies the following:

Corollary 5.9. *Every ideal $\mathfrak{a}$ contains an element α with*

$$\mathrm{N}(\alpha) < \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2} |\mathrm{disc}(K)|^{1/2}\,\mathrm{N}(\mathfrak{a}).$$

12.11.2019
This corollayr immediately gives us that every ideal class of K contains an integral ideal I such that

$$\mathrm{N}(I) \le M = \left(\frac{4}{\pi}\right)^{r_2}\left(\frac{n!}{n^n}\right)|\mathrm{disc}(K)|^{1/2}.$$

Theorem 5.10 (Minkowski)**.** *If $K \neq \mathbb{Q}$, then*

$$|\mathrm{disc}(K)| = |\Delta_K| > 1.$$

Proof. Since every ideal class contains an ideal of norm at most M_K, and we have $M_K \ge 1$ ($\mathrm{N}(\mathcal{O}_K) = 1$), we get

$$\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}|\Delta_K|^{1/2} \ge 1$$

and so

$$|\Delta_K| \ge \left(\frac{n^n}{n!}\right)^2\left(\frac{\pi}{4}\right)^{2r_2}$$

with

$$r_1 + 2r_2 = n, r_2 \le \frac{n}{2} \text{ and } \frac{\pi}{4} < 1.$$

If we let

$$a_n \coloneqq \left(\frac{n^n}{n!}\right)^2\left(\frac{\pi}{4}\right)^n \le |\Delta_K|,$$

then

$$\begin{aligned}\frac{a_{n+1}}{a_n} &= \frac{\pi}{4}(1+\frac{1}{n})^{2n}\\ &= \frac{\pi}{4}\left(2 + \binom{2n}{1}\frac{1}{n} + \cdots\right)\\ &= \frac{\pi}{4}(1 + 2 + \text{positive terms})\\ &> \frac{3\pi}{4}.\end{aligned}$$

Now $a_2 = \pi^2/4$ and so we get

$$|\Delta_K| \ge a_n \ge \frac{\pi^2}{4}\left(\frac{3\pi}{4}\right)^{n-2} > 1.$$

□

Theorem 5.11 (Hermite)**.** *There are only finitely many number fields of a given discriminant.*

6 Units in $\mathcal{O}_K$

We first look at K a quadratic extension.

6.1 Units in Imaginary Quadratic Fields

Lemma 6.1. *Let $K = \mathbb{Q}(\sqrt{d})$ with $d < 0$ square-free. If $d = -1$, then $\mathcal{O}_K^\times = \{\pm 1, \pm i\}$. If $d = -3$, then $\mathcal{O}_K^\times = \{\pm 1, \pi\rho, \pm\rho^2\}$ where $\rho = \frac{-1+\sqrt{-3}}{2}$. In all other cases we have $\mathcal{O}_K^\times = \{\pm 1\}$.*

Proof. We have ε is a unit in $\mathcal{O}_K^\times$ if and only if $\mathrm{N}(\varepsilon) = 1$. If $d = 2, 3 \mod 4$, then $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ and norm 1 elements correspond to solutions of $a^2 + b^2|d| = 1$. When $d = -1$, the solutions of $a^2 + b^2 = 1$ in integers are $a = \pm 1, b = 0$ or $a = 0, b = \pm 1$ thus

$$\mathcal{O}_K^\times = \{\pm 1, \pm i\}. The remaining cases are left as an exercise.$$

□

6.2 Units in Real Quadratic Fields

We have that $\alpha \in \mathcal{O}_K$ is a unit if and only if $\mathrm{N}(\alpha) = \pm 1$.

Theorem 6.2. *Let K be a real quadratic field (i.e. $d > 0$). Then $\mathcal{O}_K$ contains a unit $\varepsilon_0 > 1$ such that*

$$\mathcal{O}_K^\times = \{\pm\varepsilon_0^j \mid j \in \mathbb{Z}\}.$$

Remark. Since $\varepsilon_0 > 1$, ε_0^j grows without bound and hence $\mathcal{O}_K^\times$ is an infinite group. But concerning infinite groups, it is as good as it can get in the sense that one generator is enough.

To prove the theorem, we can show that the group of positive units $(\mathcal{O}_K^\times)^+$ is infinite cyclic. We turn this multiplicative problem into an additive one via the logarithm.

The log map $\log\colon \mathbb{R}^+ \to \mathbb{R}$ is a group homomorphism and

$$(\mathcal{O}_K^\times)^+ \coloneqq (\mathcal{O}_K^\times)^+ \cong \log\big(U(\mathcal{O}_K)^+\big).$$

Lemma 6.3. $\log(U(\mathcal{O}_K)^+)$ *is a discrete subgroup of* $\mathbb{R}$.

Lemma 6.4. *Let Λ be a discrete subgroup of $\mathbb{R}$. If $\Lambda \neq \{0\}$ then Λ has a smallest element v such that $\Lambda = \mathbb{Z}v$.*

Lemma 6.5 (combining previous two lemmas)**.** *Either* $\log(U(\mathcal{O}_K)^+)$ *is trivial or there is a positive unit that generates everything*

We are seeking for $\varepsilon \in \mathcal{O}_K, \varepsilon \neq 1$ with $\mathrm{N}(\varepsilon) = \pm 1$.

To get a sense of ε assume $\varepsilon = a + b\sqrt{d}$. Then $\mathrm{N}(\varepsilon) = \pm 1$ implies $a^2 - b^2 d = \pm 1$. Thus $a^2 \sim db^2$ with the smallest possible non-zero error. We can turn this around and say $\frac{a}{b}$ is a good rational approximation to $\sqrt{d}$. To find ε, we should look for good rational approximations to $\sqrt{d}$. Let $\{x\}$ denote the fractional part of x:

$$\{x\} \coloneqq x - \lfloor x \rfloor.$$

Write $\|x\|$ for the distance of x to the nearest integer.

Theorem 6.6 (Dirichelet's Approximation Theorem)**.** *Let $x \in \mathbb{R}$, then for all positive integers Q, there exists a positive integer $q \leq Q$ with*

$$\|qx\| \leq \frac{1}{Q+1}.$$

Corollary 6.7. *There are infinitely many pairs of positive integers (p, q) with $\left|p^2 - dq^2\right| < 2\sqrt{d}$.*

We also know that for each $M > 0$, there exist only finitely many non-zero ideals of $\mathcal{O}_K$ of norm bounded by M.

Proof of Theorem 6.2. Consider the ideals of the form $\langle p+q\sqrt{d}\rangle$ where p runs over integers of satisfying the conditions of Corollary 6.7. For each of them we have

$$\mathrm{N}((p+q\sqrt{d})) = \sqrt{p^2-dq^2} \leq 2\sqrt{d}.$$

There are infinitely many p, q but finitely many such ideals. Thus there exist some p, q, p', q' such that

$$(p+1\sqrt{d}) = (p'+q'\sqrt{d}).$$

That is, $p+q\sqrt{d} \sim p'+q'\sqrt{d}$ are associates. Hence there exists $\varepsilon \neq 1$ such that

$$\varepsilon = \frac{p+q\sqrt{d}}{p'+q'\sqrt{d}}.$$

So we found a unit $\varepsilon \neq 1$. □

14.11.2019

Recall: We were studying units in a quadratic field $K = \mathbb{Q}(\sqrt{d})$. In the case $d < 0$, they are the roots of unity. For $d > 0$ we have

$$\mathcal{O}_K^\times = \{\pm\varepsilon^j \mid j \in \mathbb{Z}\}.$$

6.3 Continued Fractions

Let $X \in \mathbb{R}$, then we can expand it as a *continued fraction*:

$$X = a_0 + \frac{1}{a_1 + \frac{1}{a_2+\cdots}}$$

where $a_n \in \mathbb{Z}$ and $a_i \geq 1$ for $i \geq 1$. For this same X, let us define the rational number

$$[a_0; a_1; \ldots; a_n] \coloneqq \frac{p_n}{q_n} = a_0 + \frac{1}{a_1 + \frac{1}{\cdots \frac{1}{+a_n}}}$$

then we can write X as $\lim_{n\to\infty} \frac{p_n}{q_n}$.

Fact. Suppose $X \in \mathbb{Q}$, then there exist exactly two continuous fractions for X. But it is unique if we impose $a_n > 1$, which we will impose from now on.

It is not hard to see that for $X \in \mathbb{R} \setminus \mathbb{Q}$, there exists a unique continued fraction (an infinite one). But how to compute this thing? Notice that we always have

$$X \in [a_0, a_0+1)$$

since $a_i \geq 1$ for all $i > 0$ and $a_n > 1$. Thus $a_0 = \lfloor X \rfloor$. Then let $X_1 = \frac{1}{X-a_0}$ to get

$$X_1 = a_1 + \frac{1}{a_2 + \ldots}$$

but then we know how to calculate the first term so

$$a_1 = \lfloor X_1 \rfloor$$

then we form

$$X_2 = \frac{1}{X_1 - a_1}$$

to get $a_2 = \lfloor X_2 \rfloor$ and continue.

Remark. If we apply Euclidean algorithm to X and 1:

$$\begin{aligned} X &= a_0 \cdot 1 + r_1, \quad a_0 \in \mathbb{Z} \\ 1 &= a_1 r_1 + r_2, \quad 1 > r_1 > 0 \\ r_1 &= a_2 \cdot r_2 + r_3, \quad a_2 \in \mathbb{Z}, r_2 > r_3 > 0 \end{aligned}$$

$$\vdots$$

then

$$X = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \cdots}}.$$

How to compute $\frac{p_n}{q_n}$ given $\{a_n\}_{n \geq 0}$?

$$\begin{aligned} \frac{p_0}{q_0} &= a_0, \quad p_0 = a_0, \quad q_0 = 1 \\ \frac{p_1}{q_1} &= a_0 + \frac{1}{a_1}, \quad p_1 = a_0 a_1 + 1, \quad q_1 = a_1 \\ p_n &= a_n p_{n-1} + p_{n-2}, \quad n \geq 2 \\ q_n &= a_n q_{n-1} + q_{n-2}, \quad n \geq 2 \end{aligned}$$

or use

$$p_{-1} = 1, \quad q_{-1} = 0, \quad p_{-2} = 0, \quad q_{-2} = 1, \quad n \geq 0.$$

Example 6.8.

$$\begin{aligned} \pi &= [3; 7, 15, 1, 292, \dots] \\ \frac{e^2 + 1}{e^2 - 1} &= [1; 3, 5, 7, 9, 11, \dots] \\ \frac{1 + \sqrt{5}}{2} &= [1; 1, 1, 1, 1, 1, \dots] \\ \sqrt{2} &= [1; 2, 2, \dots] \end{aligned}$$

Theorem 6.9 (Lagrange)**.** *X is a quadratic irrational number if and only if $\{a_n\}_{n \geq 0}$ is eventually periodic, i.e. there exists N such that for all $n \geq N$, $a_{n+T} = a_n$ for some $T > 0$.*

Example 6.10.

$$\begin{aligned} \sqrt{7} &= [2; 1, 1, 1, 4, 1, 1, 1, 4, \dots] \\ \sqrt{67} &= [8; 5, 2, 1, 1, 7, 1, 1, 2, 5, 16, \dots] \end{aligned}$$

Theorem 6.11 (Galois)**.** *The sequence $\{a_n\}_{n \geq 0}$ is purely periodic if and only if $X > 1$ and $-1 < X' < 0$ where X' is the conjugate of X.*

Example 6.12. For the situation of Lagrange

$$X = \sqrt{d} + \lfloor \sqrt{d} \rfloor > 1,$$

and

$$X' = -\sqrt{d} + \lfloor \sqrt{d} \rfloor \in (0, 1).$$

Lemma 6.13. *Let $X \in \mathbb{R}$, then*

$$\left| X - \frac{p_n}{q_n} \right| < \frac{1}{q_n^2}, \quad n \geq 0.$$

Proof. Exercise. □

Theorem 6.14 (Hasse)**.** *Let*

$$\tau = \begin{cases} \sqrt{d} & \text{if } d \equiv 2, 3, \mod 4 \\ \frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \mod 4 \end{cases}$$

with $d > 0$ and consider its continued fraction

$$\tau = [a_0; a_1, \ldots, a_{T-1}, a_T, \ldots],$$

where $T > 0$ is the period, then if

$$[a_1; a_2, \ldots, a_{T-1}] = \frac{p}{q}$$

and

$$[a_1; a_2, \ldots, a_{T-2}] = \frac{p'}{q'}$$

we get

$$q\frac{1}{\{\tau\}} + q' = \varepsilon_0,$$

where ε_0 is the fundamental unit of $\mathbb{Q}(\sqrt{d})$.

The theorem is equivalent to: If

$$\sqrt{d} = [a_0; a_1, \ldots, a_{T-1}, \ldots]$$

and

$$\frac{p_{T-1}}{q_{T-1}} = [a_0; a_1, \ldots, a_{T-1}],$$

then $p_{T-1}^2 - dq_{T-1}^2 = \pm 1$ and $p_{T-1} + \sqrt{d}q_{T-1} \in \mathcal{O}_K^\times$.

7 Dirichlet's Unit Theorem

Theorem 7.1. *Let K be a number field, and r_1, r_2 the numbers of real and complex emebeddings, respectively. Then*

$$\mathcal{O}_K^\times \cong \mu_K \times \mathbb{Z}^r \text{ with } r = r_1 + r_2 - 1,$$

where μ_K is the subgroup of K whose elements are roots of unity contained in K. Moreover, μ_K is a finite cyclic group of even order.

To prove this, what we want is a suitable setting for Minkowski's theory. We use logarithms to transfer the multiplicative structure of $\mathcal{O}_K^\times$ into an additive one. Recall we have the map

$$\begin{aligned} i\colon K &\hookrightarrow K_\mathbb{R} = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \\ x &\mapsto (\sigma_1(x), \sigma_2(x), \dots, \sigma_{r_1}(x), \sigma_{r_1+1}(x), \dots, \sigma_{r_1+r_2}(x)). \end{aligned}$$

Define the map

$$\begin{aligned} \ell\colon K_\mathbb{R}^\times &\to \mathbb{R}^{r_1} \times \mathbb{R}^{r_2} \\ (x_1, \dots, x_{r_1}, z_1, \dots, z_{r_2}) &\mapsto (\log|x_1|, \dots, \log|x_{r_1}|, \log|z_1|^2, \dots, \log|z_{r_2}|^2) \end{aligned}$$

where

$$K_\mathbb{R}^\times \coloneqq \{(x_1, \dots, x_r, z_1, \dots, z_{r_2}) \mid x_i \neq 0, z_j \neq 0\}.$$

Then $K_\mathbb{R}^\times$ is a multiplicative group with coordinate-wise multiplication and ℓ is a homomorphism between the groups $(K_\mathbb{R}^\times, \cdot)$ and $(\mathbb{R}^{r_1} \times \mathbb{R}^{r_2}, +)$.

Recall the trace

$$\begin{aligned} \operatorname{tr}\colon \mathbb{R}^{r_1} \times \mathbb{R}^{r_2} &\to \mathbb{R} \\ (x_1, \dots, x_{r_1+r_2}) &\mapsto x_1 + x_2 + \cdots + x_{r_1+r_2} \end{aligned}$$

and norm

$$\begin{aligned} \mathrm{N}\colon K_\mathbb{R} &\to \mathbb{R} \\ (x_1, \dots, x_{r_1}, z_1, \dots, z_{r_2}) &\mapsto x_1 \cdots x_{r_1} |z_1|^2 \cdots |z_{r_2}|^2, \end{aligned}$$

then

$$\operatorname{tr}(\ell(x)) = \log|\mathrm{N}(x)|.$$

We can compose ℓ with $i\colon K \to K_\mathbb{R}$. Suppose $\alpha \in K$, then:

$$\ell(i(\alpha)) = (\log|\sigma_1(\alpha)|, \log|\sigma_2(\alpha)|, \dots, \log|\sigma_{r_1+1}(\alpha)|^2, \dots, \log|\sigma_{r_1+r_2}(\alpha)|^2).$$

We can obtain a commutative diagram:

$$\begin{array}{ccccc} K^\times & \xhookrightarrow{i} & K_\mathbb{R}^\times & \xrightarrow{\ell} & \mathbb{R}^{r_1} \times \mathbb{R}^{r_2} \\ \downarrow{\scriptstyle \mathrm{N}_{K/\mathbb{Q}}} & & \downarrow{\scriptstyle \mathrm{N}} & & \downarrow{\scriptstyle \operatorname{tr}} \\ \mathbb{Q}^\times & \hookrightarrow & \mathbb{R}^\times & \xrightarrow{\log|\cdot|} & \mathbb{R} \end{array}$$

Let $U = \mathcal{O}_K^\times$ be the group of units. Then define $\lambda\colon U \to \mathbb{R}^{r_1} \times \mathbb{R}^{r_2}$ by $\lambda \coloneqq \ell \circ i|_U$. Then

$$\lambda(\alpha) = (\log|\sigma_1(\alpha)|, \dots, \log|\sigma_{r_1}(\alpha)|, \log|\sigma_{r_1+1}(\alpha)|^2, \dots, \log|\sigma_{r_1+r_2}(\alpha)|^2).$$

Note that $\lambda\colon U \to \mathbb{R}^{r_1} \times \mathbb{R}^{r_2}$ is not surjective since $\operatorname{tr}(\lambda(\alpha)) = \log\left|\mathrm{N}_{K/\mathbb{Q}}(\alpha)\right| = 0$ for all $\alpha \in U$. The map λ is a homomorphism from U to $\mathbb{R}^{r_1} \times \mathbb{R}^{r_2}$.

Now, a lemma that we use to determine the kernel of λ.

Lemma 7.2 (Kronecker)**.** *Let $\alpha \in \mathbb{C}$ be an algebraic integer and α_i for $i = 1, \dots, n$ its conjugates with $|\alpha_i| \leq 1$. Then $\alpha^N = 1$ for some $\mathrm{N} \in \mathbb{N}$.*

Proof. Let $p(T) = (T - \alpha_1) \cdots (T - \alpha_m) = T^n + b_1 T^{n-1} + \cdots + b_0 \in \mathbb{Z}[T]$. Then $b_k = \mathcal{S}_k(\alpha_1, \dots, \alpha_n)(-1)^k$ where $\mathcal{S}_k$ is the kth elementary symmetric polynomial in n variables. Hence $|b_k| \leq 2^n$ since $|\alpha_i| \leq 1$.Thus there are only finitely many possibilities for $p(T)$ associated to α^j for some $j \in \mathbb{N}$, since α^j has conjugates α_i^j and $|\alpha_i^j| \leq 1$ for all $i = 1, \dots, n$. So there exist $k < l$ such that $\alpha^k = \alpha^l$ and thus $\alpha^N = 1$ for $N = l - k$. □

Proposition 7.3. *The kernel of λ is the set of roots of unity that are contained in K , i.e. $\ker(\lambda) = \mu_k$. Moreover, $\ker(\lambda)$ is a finite cyclic group of even order.*

Proof. The kernel of λ is given by $\ker(\lambda) = \{\alpha \in U \mid |\sigma_i(\alpha)| = 1 \text{ for all } 1 \leq i \leq r_1 + r_2\}$. For $\alpha \in \mathcal{O}_K$ let $p \in \mathbb{Z}[T]$ its minimal polynomial. Then p^k is the characteristic polynomial of α for some $k \in \mathbb{N}$. So $p^k(T) = Q(T) = (T - \sigma_1(\alpha)) \cdots (T - \sigma_{r_1+r_2}(\alpha))$. Thus $p(T) = (T - \alpha_1) \cdots (T - \alpha_m)$ for some α_i with $|\alpha_i| = 1$ for $1 \leq i \leq m$ and $m \in \mathbb{N}$. Then Lemma 7.2 implies that $\ker(\lambda) \subset \mu_k$. On the other hand, if $\alpha^N = 1$ for some N, then $\lambda(\alpha) = 0$ and so $\ker(\lambda) = \mu_k$. Furthermore, any finite subgroup of $K^\times$ is cyclic and since $\pm 1 \in \ker(\lambda)$, it has even order.

So the only remaining part is to show that $\ker(\lambda)$ is finite. For this observe that $\alpha \in \ker(\lambda)$ implies that $i(\alpha) \in i(\mathcal{O}_K)$, which is a lattice in $K_\mathbb{R}$. We also have $|\sigma_i(\alpha)| = 1$ and so $i(\alpha) \in B$, where B is a bounded subset. Thus, $i(\alpha) \in B \cap i(\mathcal{O}_K)$ which is finite. □

19.11.2019.
Our goal is to find out about the image $\lambda(\mathcal{O}_K^\times) =: \Gamma$.

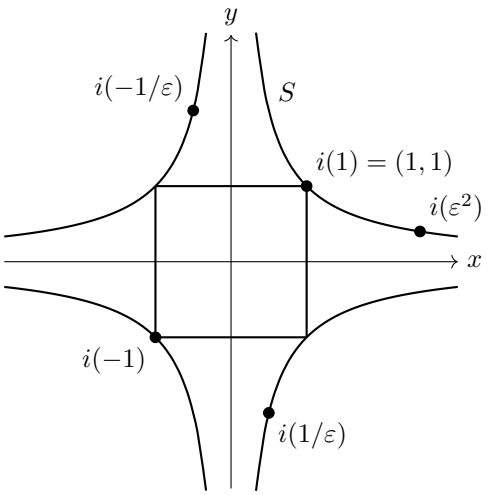
Lemma 7.4. *The image of $\mathcal{O}_K^\times$ under λ, which we denote by Γ, is a lattice of dimension $\leq r_1 + r_2 - 1$.*

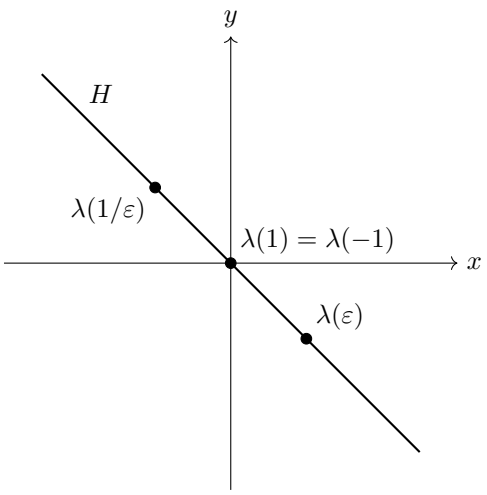
Remark. Since the norm of any unit $\varepsilon \in \mathcal{O}_k^\times$ is ± 1, for any such ε we have $\mathrm{tr}(\lambda(\varepsilon)) = \log|\mathrm{N}(\varepsilon)| = 0$. Hence all points of $\lambda(\mathcal{O}_K^\times)$ lie in the subspace $H = \{x \in \mathbb{R}^{r_1+r_2} \mid x_1 + \cdots + x_{r_1+r_2} = 0\}$. On the other hand the image of $\mathcal{O}_K^\times$ under i lies in $S = \{y \in K_\mathbb{R} \mid |\mathrm{N}(y)| = 1\}$, called the "Norm 1 surface". So we have the diagram:

$$\begin{array}{ccccc} \mathcal{O}_K^\times & \xhookrightarrow{\ i\ } & S & \xhookrightarrow{\ \ell\ } & H \\ & \searrow^{\lambda} & & \nearrow & \end{array}$$

Example 7.5. Let $K = \mathbb{Q}(\sqrt{2})$, then $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$ and $\mathcal{O}_K^\times = \pm(1 + \sqrt{2})^\mathbb{Z} = \{\pm\varepsilon^n \mid n \in \mathbb{Z}\}$, where $\varepsilon = 1 + \sqrt{2}$.

The pictures below depict the images of $\mathcal{O}_K^\times$ under i and λ respectively.





The crucial fact is that the logarithm takes points from the hyperbolas in S onto a line in H and so we get a one dimensional lattice.

Now how do the units $\tilde{U} = i(\mathcal{O}_K^\times)$ move S around? Multiplying S by some $u \in \tilde{U}$ moves the arcs between consecutive points in the hyperbola picture to other arcs between consecutive points. It then exchanges the hyperbolas $y = 1/x$, $y = -1/x$. If $\mathrm{N}(u) = -1$, multiplication by $i(-1)$ on S exchanges 2 branches of the hyperbola. (Comment: In that way we get a transitive action of the groups of units on S and we can choose a compact line segment as a representative for the quotient space.) In fact modulo $\tilde{U} = i(\mathcal{O}_K^\times)$ any $(x, y) \in S$ is equivalent to a point on the arc between $i(1) = (1, 1)$ and $i(\varepsilon^2)$. Hence the map $[1, \varepsilon^2] \to S/\tilde{U}, x \mapsto (x, 1/x)\tilde{U}$ is surjective. This means that $S = \cup_{\varepsilon \in \mathcal{O}_K^\times} i(\varepsilon)X_0$, where X_0 is the arc on S between $i(1)$ and $i(\varepsilon^2)$.

Proof of Lemma 7.4. For any $\varepsilon \in \mathcal{O}_K^\times$ the image $\lambda(\varepsilon)$ lies in H. Now H has dimension $r_1 + r_2 - 1$. We need to show that Γ is a lattice. So let us first show that Γ is discrete:

Let $\|\cdot\|$ denote the usual length in $\mathbb{R}^{r_1+r_2}$. Suppose $0 < c \in \mathbb{R}$. We want to show that $B = \{x \in \mathbb{R}^{r_1+r_2} \mid \|x\| < c\}$ contains only finitely many points of $\Gamma = \ell(i(\mathcal{O}_K^\times))$. We have

$$\ell^{-1}(\Gamma \cap B) = \ell^{-1}(\Gamma) \cap \ell^{-1}(B) = i(\mathcal{O}_K^\times) \cap \ell^{-1}(B).$$

By definition of ℓ, $\|\ell(\varepsilon)\| < c$ implies that $|\sigma_k(\varepsilon)| < e^c$ for $k = 1, \ldots, r_1$ and $|\sigma_k(\varepsilon)|^2 < e^c$ for $k = r_1 + 1, \ldots, r_1 + r_2$, so $\ell^{-1}(B)$ is bounded. We also know that $i(\mathcal{O}_K)$ is a lattice. Hence

$$i(\mathcal{O}_K^\times) \cap \ell^{-1}(B) \subset i(\mathcal{O}_K) \cap \ell^{-1}(B)$$

and since the latter is finite, we can apply ℓ again to conclude. □

Our next goal is to show that Γ is actually complete, i.e. its dimension is $r_1 + r_2 - 1$. To show Γ is complete we will use that if V is a vector space and Γ a lattice in V, then Γ is complete if and only if there exists a bounded set $B \subset V$ such that $V = \bigcup_{\gamma \in \Gamma}(B + \gamma)$.

We will construct our region by working in S and applying ℓ, i.e. we will construct a bounded set X_0 in the norm-one-surface S such that $S = \bigcup_{\varepsilon \in \mathcal{O}_K^\times} i(\varepsilon)X_0$ as we did in the example of real quadratic fields.

21.11.2019
We start with

Theorem 7.6. *There is a bounded region $X_0 \subset S$ such that $S = \bigcup_{\varepsilon \in \mathcal{O}_K^\times} i(\varepsilon)X_0$.*

Before proving this let us note the corollary:

Corollary 7.7. *Γ is a complete lattice.*

Proof. Suppose there exists $X_0 \subset S$ such that $S = \bigcup_{\varepsilon \in \mathcal{O}_K^\times} i(\varepsilon)X_0$ where X_0 is bounded. Then let $B = \ell(X_0)$. We claim B is bounded.

Note that this requires proof since log sends the bounded interval $(0, 1]$ to $(-\infty, 0]$ which is unbounded.

To see the boundedness of B,

$$X_0 \subset S = \{y \mid |\mathrm{N}(y)| = 1\}.$$

If $x \in X_0$, then its coordinates $|x_j|$ are bounded from above because X_0 is bounded. If $x \in X_0$,

$$|\mathrm{N}(x)| = \prod_{i=1}^{r_1} |x_i| \prod_{j=r_1+1}^{r_1+r_2} |x_j|^2 = 1$$

hence the $|x_j|$'s are also bounded away from zero. So $\ell(X_0) = B$ is bounded. Applying ℓ to $S = \bigcup i(\varepsilon)X_0$ we get

$$H = \bigcup_{\varepsilon \in \mathcal{O}^\times} \ell(i(\varepsilon)) + B = \bigcup_{\gamma \in \Gamma} \gamma + B.$$

□

Proof of Theorem 7.6. Let $y \in S$. We want to write $y = i(\varepsilon)x$ for some $\varepsilon \in \mathcal{O}_K^\times$ and some element x in a bounded region X_0 of S. Let Λ be the lattice corresponding to $\mathcal{O}_K$, i.e. $\Lambda = i(\mathcal{O}_K)$. Consider the lattice $y\Lambda$. Since $y \in S$, $|\mathrm{N}(y)| = 1$ and $\mathrm{vol}(y\Lambda) = \mathrm{vol}(\Lambda)$. (Recall the volume is $v = w^{-r_2}|\mathrm{disc}(K)|^{1/2}$.)

Choose numbers $c_i > 0$ with

$$q = c_1 \cdots c_{r_1+r_2} > \left(\frac{4}{\pi}\right)^{r_2} v.$$

Consider the set

$$X \coloneqq \{x \in K_{\mathbb{R}} \mid |x_k| < c_k, k = 1, \ldots, r_1, |x_{r_1+j}|^2 < c_{r_1+j}, j = 1, \ldots, r_2\}.$$

By Minkowski, there exists a non-zero $x = (x_1, \ldots, x_{r_1+r_2}) \in X \cap y\Lambda$. So we have

$$x = yi(\alpha)$$

for some $0 \neq \alpha \in \mathcal{O}_K$. So we have

$$\mathrm{N}(x) = \mathrm{N}(y)\,\mathrm{N}(\alpha) = \pm\,\mathrm{N}(\alpha)$$

thus

$$\mathrm{N}(\alpha) < c_1 \cdots c_{r_1+r_2} = q$$

Since ther are only finitely many ideals of $\mathcal{O}_K$ of norm at most q and since any element of norm q would generate a principal ideal of norm at most q, it follows that there are only finitely many non-associate numbers α of norm at most q. Choose such a set

$$\{\alpha_1, \ldots, \alpha_N\}$$

consisting of a complete set of non-associate numbers of norm at most q.

So we have for some $j \in \{1, \ldots, N\}$ and some unit ε

$$\alpha\varepsilon = \alpha_j.$$

Thus

$$y = xi(\alpha^{-1}) = xi(\alpha_j^{-1})i(\varepsilon).$$

Define

$$X_0 = S \cap \bigcup_{j=1}^{N} i(\alpha_j^{-1})X.$$

Since X is bounded, its translates $i(\alpha_j^{-1})X$ are bounded and because it is a finite union of bounded sets, X_0 is also bounded.

Now for $y \in S, i(\varepsilon) \in S$,

$$y = xi(\alpha_j^{-1})i(\varepsilon)$$

then

$$xi(\alpha_j^{-1}) \in S \cap i(\alpha_j^{-1})X \in X_0$$

thus

$$y = xi(\alpha_j^{-1})i(\varepsilon) \in i(\varepsilon)X_0$$

which is what we wanted to show. □

We present here a lemma we used:

Lemma 7.8. *Up to multiplication by units, there are only finitely many elements $\alpha \in \mathcal{O}_K$ of a given norm*

$$M = \mathrm{N}(\alpha).$$

Proof. Let $M \in \mathbb{Z}$, $M > 1$. In all $[\mathcal{O}_K : M\mathcal{O}_K]$ cosets of $\mathcal{O}_K / M\mathcal{O}_K$ there exists up to multiplication by units at most one element α such that

$$\mathrm{N}(\alpha) = M.$$

To see this, let $\beta = \alpha + M\gamma$ where $\gamma \in \mathcal{O}_K$ is another element with $\mathrm{N}(\beta) = M$. Then

$$\frac{\alpha}{\beta} = 1 + \frac{\mathrm{N}(\beta)}{\beta} \in \mathcal{O}_K$$

since

$$\frac{\mathrm{N}(\beta)}{\beta} \in \mathcal{O}_K.$$

We also have similarly $\frac{\beta}{\alpha} \in \mathcal{O}_K$. Hence they are associates. □

We thus have proved Theorem 7.1, which states that if $K/\mathbb{Q}$ is a number field, and $[K : \mathbb{Q}] = n = r_1 + 2r_2$. Then

$$\mathcal{O}_K \cong \mu_K \times \mathbb{Z}^r$$

where μ_K are toots of unity in K and $r = r_1 + r_2 - 1$, i.e. there exists $\varepsilon_1, \ldots, \varepsilon_r$ such that all $\varepsilon \in \mathcal{O}_K^\times$ can be written uniquely in the form

$$\varepsilon = \zeta \varepsilon_1^{\nu_1} \cdots \varepsilon_r^{\nu_r}, \quad \zeta \in \mu_K.$$

The ε_i's are called *fundamental units*.

A natural question is what is $\mathrm{vol}(\Gamma)$, where $\Gamma = \lambda(\mathcal{O}_K^\times)$.

Let $\varepsilon_1, \ldots, \varepsilon_r$ be a system of fundamental units. Let Φ_Γ be the fundamental mesh for Γ. We want to know $\mathrm{vol}(\Phi_\Gamma)$, i.e. the volume spanned by vectors $\lambda(\varepsilon_1), \ldots, \lambda(\varepsilon_r)$ in H.

Recall

$$\lambda(\varepsilon_1) = (\log|\sigma_1(\varepsilon_1)|, \ldots, \log|\sigma_{r_1+r_2}(\varepsilon_1)|^2)$$

First note that

$$\lambda_0 = \frac{1}{\sqrt{(r_1 + r_2)}}(1, 1, \ldots, 1) \in \mathbb{R}^{r_1+r_2}$$

has length 1 and is orthogonal to H since $\lambda_0 x = 0$ for all $x \in H$. Hence the $(r+1)$-dimensional parallelopiped spanned by $\lambda_0, \lambda(\varepsilon_1), \ldots, \lambda(\varepsilon_r)$ in $\mathbb{R}^{r_1+r_2}$ has the same volume as the $(r_1 + r_2 - 1)$-dimensional $\Phi_\Gamma \subset H$. This volume is given by

$$\frac{1}{\sqrt{r_1 + r_2}} \det \begin{pmatrix} 1 & | & \ldots & | \\ \vdots & \lambda(\epsilon_1) & \ldots & \lambda(\epsilon_r) \\ 1 & | & \ldots & | \end{pmatrix}$$

If we add all rows to a fixed row, say the ith row, then this row will have all entries 0 expect for the first one, which will be $r_1 + r_2$. If we expand using the ith row we obtain that this volume is

$$\mathrm{vol}(\lambda(\mathcal{O}_K^\times)) = \frac{r_1 + r_2}{\sqrt{r_1 + r_2}} |\det M'|$$

where M' is any $r \times t$ minor of the matrix of M (which has size $(r_1 + r_2) \times (r_1 + r_2 - 1)$):

$$\begin{pmatrix} \lambda_1(\varepsilon_1) & \ldots & \lambda_1(\varepsilon_r) \\ \vdots & & \vdots \\ \lambda_{r_1+r_2}(\varepsilon_1) & \ldots & \lambda_{r_1+r_2}(\varepsilon_r) \end{pmatrix}$$

We proved before that the volume Φ_Γ of the fundamental mesh of $\Gamma = \lambda(\mathcal{O}_K^\times)$ in H is

$$\mathrm{vol}(\lambda(\mathcal{O}_K^\times)) = \sqrt{r_1 + r_2} R$$

where R is the absolute value of the determinant of any minor of M of rank $r = r_1 + r_2 - 1$. The value R is called the *regulator of* K.

Example 7.9. Consider $\mathbb{Q}(\sqrt{d})$ with $d > 0$. If ε_d is the fundamental unit then $R_K = \log \varepsilon_d$.

Remark. In the case of real quadratic fields, each ideal class is associated to a conjugacy class of a hyperbolic element $\gamma \in SL_2(\mathbb{R})$, where hyperbolic means $\operatorname{tr} \gamma > 2$

Next we state some simple corollaries of Dirichlet's unit theorem:

Corollary 7.10. *$\mathcal{O}_K^\times$ is finite if and only if $r = r_1 + r_2 - 1 = 0$ if and only if $(r_1, r_2) = (1, 0)$ in the $\mathbb{Q}$ case or $(r_1, r_2) = (0, 1)$ in the imaginary quadratic case.*

Corollary 7.11. *$\mathcal{O}_K$ has rank 1 if and only if $r_1 + r_2 - 1 = 1$ if and only if $r_1 + r_2 = 2$. This happens exactly in the following cases:*

Real quadratic case: $(r_1, r_2) = (2, 0)$.

Cubic case: $(r_1, r_2) = (1, 1)$.

Quartic, totally imaginary case: $(r_1, r_2) = (0, 2)$.

In all these cases

$$\mathcal{O}_K^\times = \mu_K \cdot \varepsilon^{\mathbb{Z}}$$

for some fundamental unit ε.

Example 7.12. Let $K = \mathbb{Q}(\alpha)$, $\alpha^3 - \alpha - 1 = 0$. Check that $x^3 - x - 1$ is irreducible. In this case $r_1 = 1, r_2 = 1, r_1 + r_2 - 1 = 1$. Here

$$\operatorname{disc}(\alpha) = -23$$

which is square-free. Thus $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Since α satisfies $\alpha^3 - \alpha - 1 = 0$, α is a unit.

Question: is α the fundamental unit?

Is there a unit u such that $1 < u < \alpha$?

Assume $u > 1, u \in \mathcal{O}_K^\times$ and let σ be the complex embedding. Then

$$\mathrm{N}_{K/\mathbb{Q}}(u) = u\sigma(u)\bar{\sigma}(u) = u|\sigma(u)|^2 > 0$$

and $\mathrm{N}(u) = 1$.

The minimal polynomial of u is some degree 3 polynomial, say

$$m(x) = x^3 + ax^2 + bx - 1.$$

The roots of m are u, $\sigma(u), \bar{\sigma}(u)$. Hence

$$a = -(u + \sigma(u) + \bar{\sigma}(u))$$

$$b = u\sigma(u) + u\bar{\sigma}(u) + \sigma(u)\bar{\sigma}(u)$$

$$|a| \leq u + 2|\sigma(u)| \leq \alpha + 2 \approx 3.3$$

$$|b| \leq 2u|\sigma(u)| + |\sigma(u)|^2 \leq 2\alpha + 1 \approx 3.6$$

$$\mathrm{N}(u) = u|\sigma(u)|^2 = 1, u > 1$$

thus

$$|\sigma(u)| \leq 1$$

if $u < \alpha$. Thus $a, b \in \{0, \pm 1, \pm 2, \pm 3\}$ There are 49 such polyniomials. If u is a root of such a polynomial, $u > 1$, u a unit, since

$$\operatorname{disc}(\mathbb{Z}[u]) = (\mathcal{O}_K : \mathbb{Z}[u])^2 \operatorname{disc}(K)$$

such a u must have a disc a square multiple of -23. There are only four such polynomials

$$x^3 - x - 1$$

$$x^3 - 2x^2 + x - 1$$

$$x^3 - 3x^2 + 2x - 1$$

$$x^3 - 2x^2 - 3x - 1$$

All roots of these polynomials are bigger than α and hence α is a fundamental unit.

8 Factoring Primes in a Number Field

26.11.2019
Recall (most can be found in Theorem 3.39):

1. If I is an ideal of $\mathcal{O}_K$ and $\mathrm{N}(I) = p$ with p prime, then I is a prime ideal.
2. If $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$, then there exists exactly one prime $p \in \mathbb{Z}$ such that $\mathfrak{p} \mid p$. In this case, $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. We call p the *prime lying below* $\mathfrak{p}$.
3. The norm of a prime ideal $\mathfrak{p}$ is related the prime lying below it via $\mathrm{N}(\mathfrak{p}) = p^f$ for some $f \in \{1, \dots, [K : \mathbb{Q}]\}$.

   Definition 8.1. Let $p \in \mathbb{Z}$ be the prime lying below the prime ideal $\mathfrak{p}$ such that $\mathrm{N}(\mathfrak{p}) = p^f$. Then $f = f_K(\mathfrak{p})$ is called the *inertia degree* of $\mathfrak{p}$ in $\mathcal{O}_K$.
4. Let $p \in \mathbb{Z}$ and suppose $p\mathbb{Z} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$ for distinct prime ideals $\mathfrak{p}_i \subset \mathcal{O}_K$ and positive integers e_i's (by prime factorization). If $f_i = f_K(\mathfrak{p}_i)$, then
$$\sum_{i=1}^{g} e_i f_i = n = [K : \mathbb{Q}].$$
5. We have $[\mathcal{O}_K : \mathfrak{p}] = \mathrm{N}(\mathfrak{p}) = p^f$. Since $\mathcal{O}_K/\mathfrak{p}$ is a finite field, its prime field F is isomorphic to $\mathbb{Z}/p\mathbb{Z}$. In fact one can show that $F = \{a + \mathfrak{p} \mid a = 0, \dots, p-1\}$. In particular, if $f_K(\mathfrak{p}) = 1$, then $[\mathcal{O}_K/\mathfrak{p} : F] = 1$ and $\mathcal{O}_K/\mathfrak{p} = \{\mathfrak{p} + a \mid a = 0, \dots, p-1\}$. So if $\alpha \in \mathcal{O}_K$, then there exists $a \in \{0, \dots, p-1\}$ such that $\alpha + \mathfrak{p} = a + \mathfrak{p}$.

Definition 8.2. With the above facts in mind, we have some definitions:

1. The integer g from above (appearing in $p\mathbb{Z} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$) is called the *decomposition number of p in K* and denoted by $g_K(p)$.
2. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ and $p \in \mathbb{Z}$ the prime lying below $\mathfrak{p}$. Then there exists a unique integer e such that $\mathfrak{p}^e \mid p\mathcal{O}_K$ but $\mathfrak{p}^{e+1} \nmid p\mathcal{O}_K$. This e is called the *ramification index* of $\mathfrak{p}$ in K and denoted by $e_K(\mathfrak{p})$.
3. If $e_i > 1$ for some $i \in \{1, \dots, g\}$, then p is said to be *ramified in K*. Otherwise p is *unramified*.

The following theorem can be useful to detect ramification. We will not prove it though.

Theorem 8.3. *Let K be a number field. Then $p \in \mathbb{Z}$ is ramified in K if and only if $p \mid \mathrm{disc}(K)$.*

You know this seems like a pretty useful and important theorem, to be honest I don't know why we don't prove this Prof. Imamoglu.

8.1 Factoring Primes in Quadratic Fields

Let $K = \mathbb{Q}(\sqrt{d})$ with d square-free and $p \in \mathbb{Z}$ a prime number.

If $g_K(p) = 2$, then $e_1 f_1 + e_2 f_2 = 2$ and so $e_1 = f_1 = e_2 = f_2 = 1$. If $g_K(p) = 1$, then (e_1, f_1) is either $(2, 1)$ or $(1, 2)$.

So we have three possibilities:

1. $g_K(p) = 2$ and $e_i = f_i = 1$. Then $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ and so $\mathrm{N}(\mathfrak{p}_1) = \mathrm{N}(\mathfrak{p}_2) = p$. In this case we call p *split*.
2. $g_K(p) = 1$ and $e_1 = 2, f_1 = 1$. Then $p\mathcal{O}_K = \mathfrak{p}^2$ and $\mathrm{N}(\mathfrak{p}) = p$. In this case p is ramified.
3. $g = 1$ and $e_1 = 1$ and $f_1 = 2$. Then $p\mathcal{O}_K = \mathfrak{p}$ and $\mathrm{N}(\mathfrak{p}) = p^2$. In this case p is said to be *inert*, i.e. it remains prime.

Let

$$\tau = \begin{cases} \sqrt{d}, & d \equiv 2,3 \mod 4 \\ \frac{1+\sqrt{d}}{2}, & d \equiv 1 \mod 4 \end{cases}$$

and $\min_\tau(x)$ its minimal polynomial over $\mathbb{Q}$. Then

$$\min_\tau(x) = \begin{cases} x^2 - d, & d \equiv 2,3 \mod 4 \\ x^2 - x - \frac{1-d}{4}, & d \equiv 1 \mod 4. \end{cases}$$

Recall that the *Legendre-symbol* $\left(\frac{a}{p}\right)$ for a non-zero integer a and an odd prime p gives 1 if a is a quadratic residue $\mod p$; -1 if a is not a square $\mod p$ and 0 if $p \mid a$.

Theorem 8.4. *Suppose p is an odd prime, and d as before is such that $K = \mathbb{Q}(\sqrt{d})$. Then:*

1. *If $p \nmid d$ and $\left(\frac{d}{p}\right) = 1$, then $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ with $\mathrm{N}(\mathfrak{p}_i) = p$ where $\mathfrak{p}_1 = (p, a + \sqrt{d}), \mathfrak{p}_2 = (p, a - \sqrt{d})$.*
2. *If If $p \nmid d$, and $\left(\frac{d}{p}\right) = -1$ then $p\mathcal{O}_K$ remains prime, $\langle p \rangle = \mathfrak{p}$, $\mathrm{N}(\mathfrak{p}) = p^2$.*
3. *If $p \mid d$ then $p\mathcal{O}_K = \mathfrak{p}^2$ where $\mathfrak{p} = \langle p, \sqrt{d} \rangle$.*

Proof. Case 1: Suppose for simplicity $d \equiv 3, 2 \mod 4$. If $\left(\frac{d}{p}\right) = 1$, then there exists $a \in \mathbb{Z}$ such that $a^2 \equiv d \mod p$. As $p \nmid d$, also $p \nmid a$. Let $\mathfrak{p}_1 \coloneqq \langle p, a + \sqrt{d} \rangle$ and $\mathfrak{p}_2 \coloneqq \langle p, a - \sqrt{d} \rangle$. First note that $\mathfrak{p}_1 \neq \mathfrak{p}_2$: Suppose $\mathfrak{p}_1 = \mathfrak{p}_2$. then $2a = a + \sqrt{d} + a - \sqrt{d} \in \mathfrak{p}$, but $2a \in \mathbb{Z}$ and hence $2a \in \mathfrak{p}_1 \cap \mathbb{Z} = p\mathbb{Z}$, which is a contradiction. Next, we show that $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$:

$$\begin{aligned} \mathfrak{p}_1\mathfrak{p}_2 &= \langle p^2, p(a + \sqrt{d}), p(a - \sqrt{d}), a^2 - d \rangle \\ &= \langle p \rangle \langle p, a + \sqrt{d}, a - \sqrt{d}, (a^2 - d)/p \rangle \\ &= p\mathcal{O}_K, \end{aligned}$$

where we used that $p \mid a^2 - d$ and $(a, p) = 1$.

Case 2 and 3: Exercise. □

Remark. Note that the factoring of $\mathfrak{p}$ in $\mathcal{O}_K$ mimics the behaviour of $x^2 - d \mod p$. This is a general behaviour when K is monogenic, i.e. $\mathcal{O}_K = \mathbb{Z}[\theta]$ for some θ.

28.11.2019 Before giving the general case,

Theorem 8.5. *For $p = 2$, if $d \equiv 2, 3 \mod 4$ then 2 is ramified. If $d \equiv 5 \mod 8$ then 2 remains prime. If $d \equiv 1 \mod 8$ then 2 splits.*

Definition 8.6 (Kronecker symbol)**.** Let D be a non-square integer such that $D \equiv 0, 1 \mod 4$. The Kronecker symbol is defined by

$$\left(\frac{D}{2}\right) = \begin{cases} 0, & D \equiv 0 \mod 4 \\ 1, & D \equiv 1 \mod 8 \\ -1, & D \equiv 5 \mod 8. \end{cases}$$

Note that we now have the Kronecker and the Legendre symbol. We will denote them both by $\chi_D(p)$, which is the Kronecker symbol for $p = 2$ and the Legendre symbol otherwise.

Theorem 8.7. *Let K be a quadratic field with $D = \mathrm{disc}(K)$ and let $p \in \mathbb{Z}$ be prime. Then*

1. *(p) splits if and only if $\chi_D(p) = \left(\frac{D}{p}\right) = 1$*
2. *(p) ramifies if and only if $\chi_D(p) = \left(\frac{D}{p}\right) = 0$*

3. (p) *is inert if and only if* $\chi_D(p) = \left(\frac{D}{p}\right) = -1$

Recall: Given K a number field, we can determine the class number $h_K = |Cl_K|$ and generators as follows:

1. Compute the Minkowski bound $M_K = \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}(\text{disc}(K))^{1/2}$.
2. Every ideal of $\mathcal{O}_K$ is equivalent to an ideal of norm at most M_K.
3. We can determine all primes $p \leq M_K$ and their prime ideal factorization
$$(p) = \mathfrak{p}_1 \cdots \mathfrak{p}_r.$$
4. Determine all products of these prime ideals having norm $\leq M_K$.

Then every ideal will be equivalent to some ideal in this list .

Example 8.8. Let $K = \mathbb{Q}(\sqrt{-5})$. Then $\mathcal{O}_K$ has basis $(1, \sqrt{-5})$ and $M_K \approx 2.84$.

So every ideal is equivalent to one with norm either 1 or 2. The only norm 1 ideal is $\mathcal{O}_K$. If $\mathfrak{a}$ has norm 2, then it divides the ideal generated by 2:
$$(2) = (2, 1 + \sqrt{5})^2 =: \mathfrak{p}^2.$$

Note $\mathfrak{p}$ is not principal since if it were, say $\mathfrak{p} = (\alpha)$ for some $\alpha \in \mathcal{O}_K$,
$$\alpha = a + b\sqrt{-5}$$
but
$$\text{N}(\alpha) = a^2 + 5b^2 = 2$$
is not solvable in integers. Thus
$$Cl_K = \{[1], [\mathfrak{p}]\} \cong \mathbb{Z}/2\mathbb{Z}.$$

Check $\langle 3 \rangle = \mathfrak{p}_3\mathfrak{q}_3 = (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5})$ and that they are not principal.

8.2 Factoring Primes in a Monogenic Field

Let K be a number field that is a monogenic field, i.e. there exists $\theta \in \mathcal{O}_K$ such that $\mathcal{O}_K = \mathbb{Z}[\theta]$.

Theorem 8.9. *Let* $K = \mathbb{Q}(\theta)$ *with* $\mathcal{O}_K = \mathbb{Z}[\theta]$ *and* $p \in \mathbb{Z}$ *prime. Suppose* $h(x) \in \mathbb{Z}[x]$ *is the minimum polynomial of* θ *and let*
$$\bar{\cdot}\colon \mathbb{Z}[x] \to \mathbb{Z}/p\mathbb{Z}[x]$$
be the natural $\mod p$ *reduction map. Let*
$$\bar{h}(x) = \bar{h}_1(x)^{e_1} \cdots \bar{h}_g(x)^{e_g}$$
be the prime factorization of h *into distinct irreducible monic* $\bar{h}_i$*'s in* $\mathbb{Z}/p\mathbb{Z}[x]$ *with* $e_1, \ldots, e_g$ *positive integers. Choose any monic polynomials* $h_i \in \mathbb{Z}[x]$ *that reduce to* h_i.

Then the prime factorization of (p) *is given by*
$$(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$$
where $\mathfrak{p}_i = (p, h_i(\theta))$. *Moreover, the* $\mathfrak{p}_i$*'s are distinct prime ideals with* $\text{N}(\mathfrak{p}_i) = p^{\deg h_i}$.

Proof. Let θ_i be a root of $\bar{h}_i$ in an extension of $\mathbb{Z}/p\mathbb{Z}$. This extension is a finite field
$$(\mathbb{Z}/p\mathbb{Z})[x] \Big/ (\bar{h}_i) \cong \mathbb{Z}/p\mathbb{Z}[\theta_i].$$

Let

$$\psi_i \colon \mathbb{Z}[\theta] \to \mathbb{Z}/p\mathbb{Z}[\theta_i]$$
$$g(\theta) \mapsto \bar{g}(\theta_i).$$

Then

$$\mathbb{Z}[\theta] \,/_{\ker \psi_i} \cong \psi_i(\mathbb{Z}[\theta]) = \mathbb{Z}/p\mathbb{Z}[\theta_i]$$

$\mathbb{Z}(\theta) \,/_{\ker \psi_i}$ is a field, and hence $\ker \psi_i$ is a prime ideal. We want to show $\ker \psi_i = \langle p, h_i(\theta) \rangle$. Clearly $\psi_i(p) = 0, h_i(\theta) \in \ker \psi_i$. Thus

$$\langle p, h_i(\theta) \rangle \subset \ker \psi_i.$$

For the reverse inclusion, let $g(\theta) \in \ker \psi_i$. Then

$$\bar{g}(\theta_i) = \psi_i(g(\theta)) = 0$$

so $\bar{h}_i(x) \mid \bar{g}(x)$ in $\mathbb{Z}/p\mathbb{Z}[x]$. Hence

$$\bar{g}(x) = \bar{h}_i(x)\bar{f}(x)$$

for some $f \in \mathbb{Z}[x]$. hence $(g - h_i f)(x) \in \mathbb{Z}[x]$ has coefficients divisible by p:

$$g(\theta) = g(\theta) - h_i(\theta)f(\theta) + h_i(\theta)f(\theta) = (g - h_i f)(\theta) + h_i(\theta)f(\theta) \in \langle p \rangle + \langle h_i(\theta) \rangle = \langle p, h_i(\theta) \rangle$$

and so

$$\ker \psi_i = \langle p, h_i(\theta) \rangle = \mathfrak{p}_i.$$

Next we show that these are distinct. Let $i \neq j$ and

$$\mathfrak{p}_i = \langle p, h_i(\theta) \rangle, \mathfrak{p}_j = \langle p, h_j(\theta) \rangle.$$

The mod p reductions $\bar{h}_i, \bar{h}_j$ are distinct irreducibles i.e. there exist $f, g, \in \mathbb{Z}[x]$ such that

$$h_i(x)f(x) + h_j(x)g(x) \equiv 1 \mod p$$

i.e. for some $Q(x) \in \mathbb{Z}[x]$,

$$h_i(x)f(x) + h_j(x)g(x) = 1 + pQ(x).$$

Now take $x = \theta$,

$$h_i(\theta)f(\theta) + h_j(\theta)g(\theta) - pQ(\theta) = 1 \in \mathfrak{p}_i + \mathfrak{p}_j$$

hence

$$\mathfrak{p}_i + \mathfrak{p}_j = \langle 1 \rangle$$

so in particular distinct.

It remains to show that

$$\langle p \rangle = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}$$

Recall: for any A, B_1, B_2 we have

$$(A + B_1)(A + B_2) \subset A + B_1 B_2$$

Consider

$$\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g} = \langle p, h_1(\theta) \rangle^{e_1} \cdots \langle p, h_g(\theta) \rangle^{e_g} \subset \langle p, h_1(\theta)^{e_1} \cdots h_g(\theta)^{e_g} \rangle = \langle p \rangle + \langle h(\theta) \rangle = \langle p \rangle$$

so

$$\prod_{i=1}^{g} \mathfrak{p}_i^{e_i} \subset \langle p \rangle$$

so

$$\langle p\rangle \mid \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}$$

We also have

$$p \subset \langle p, h_i(\theta)\rangle = \mathfrak{p}_i.$$

Hence

$$\langle p\rangle = \mathfrak{p}_1^{k_1}\cdots\mathfrak{p}_g^{k_g} \text{ with } k_i \in \{1,\dots,e_i\}.$$

Now

$$\mathcal{O}_K \big/ \mathfrak{p}_i = \mathbb{Z}[\theta] \big/ \mathfrak{p}_i = \mathbb{Z}[\theta] \big/ \ker \psi_i \cong \mathbb{Z}/p\mathbb{Z}[\theta_i]$$

and thus

$$\mathrm{N}(\mathfrak{p}_i) = \mathrm{card}(\mathbb{Z}/p\mathbb{Z}[\theta_i]) = p^{d_i}$$

where $d_i = \deg \bar{h_i}$. This implies

$$p^n = \mathrm{N}(\langle p\rangle) = \mathrm{N}(\mathfrak{p}_1^{k_1}\cdots\mathfrak{p}_g^{k_g}) = p^{k_1d_1+\cdots+k_gd_g}.$$

Comparing the degres

$$\bar{h} = \bar{h_1}^{e_1}\cdots\bar{h_g}^{e_g}$$

$$d_1e_1 + \cdots + d_ge_g = n$$

gives $k_i = e_i$. Moreover $\mathrm{N}(\mathfrak{p}_i) = p^{d_i} = p^{\deg h_i}$. □

Remark. Using some algebra there is the following simpler proof of the theorem:

Proof. Notice that the assumption implies that

$$\mathbb{Z}[x] \Big/ h(x) \cong \mathcal{O}_K$$

via $x \mapsto \theta$ and hence

$$\mathcal{O}_K \big/ p\mathcal{O}_K \cong \mathbb{Z}[x]/(h(x)) \Big/ (p) = \mathbb{Z}/p\mathbb{Z}[x] \Big/ (\bar{h}(x)) =: R.$$

Now recall that if that $\mathfrak{a} = \mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_r^{e_r}$ is the prime factorization of an ideal $\mathfrak{a} \subset \mathcal{O}_K$ into distinct prime ideals $\mathfrak{p}_i$, then the $\mathfrak{p}_i$ are uniquely characterized by $\mathfrak{a} \subset \mathfrak{p}_i$ and the integers e_i by $\mathfrak{a} \subset \mathfrak{p}^{e_i}$ but $\mathfrak{a} \not\subset \mathfrak{p}_i^{e_i+1}$.

The prime ideals of R are exactly given by $\mathfrak{q}_i \coloneqq (\bar{h}_i(x))$ and we have

$$(\bar{h}(x)) \subset (\bar{h}_i(x))^{e_i} \text{ but } (\bar{h}(x)) \not\subset (\bar{h}_i(x))^{e_i+1}. \tag{3}$$

Under the isomorphism induced by $x \mapsto \theta$ the ideals $\mathfrak{q}_\mathfrak{i}$ correspond to $(p\mathcal{O}_K + (h_i(\theta)))/p\mathcal{O}_K$ in $\mathcal{O}_K/p\mathcal{O}_K$. Hence the prime ideals above $p\mathcal{O}_K$ in $\mathcal{O}_K$ are exactly $\mathfrak{p}_i \coloneqq p\mathcal{O}_k + (h_i(\theta)) = (p, h_i(\theta))$. The exponent of $\mathfrak{p}_i$ in the prime factorization of $p\mathcal{O}_K$ is then characterized by (3).

To get the inertia degree, note that

$$\mathcal{O}_K \big/ \mathfrak{p}_i \cong (\mathbb{Z}[x])/(h(x)) \Big/ (p, h_i(x)) \cong (\mathbb{Z}/p\mathbb{Z})[x] \Big/ (\bar{h}_i(x))$$

and that the latter is a vector space of dimension $\deg h_i$ over $\mathbb{Z}/p\mathbb{Z}$. Hence $\mathrm{N}(\mathfrak{p}_i) = p^{\deg h_i}$. □

Example 8.10. Let $K = \mathbb{Q}(\sqrt[3]{2})$, then $\mathcal{O}_K = \mathbb{Z}[\theta]$ with $\theta = \sqrt[3]{2}$, $\min_\theta(x) = x^3 - 2$ and $\mathrm{disc} = -108$. Consider $p = 5$:

$$x^3 - 2 = (x+2)(x^2 - 2x - 1) \mod 5$$

By Theorem 8.9

$$\langle 5\rangle = \mathfrak{pq}$$

where

$$\mathfrak{p} = \langle 5, \theta + 2 \rangle \text{ and } \mathfrak{q} = \langle 5, \theta^2 - 2\theta - 1 \rangle.$$

Then

$$\mathrm{N}(\mathfrak{p}) = p^{1=\deg(x+2)} \text{ and } \mathrm{N}(\mathfrak{q}) = p^{2=\deg(x^2-2x-1)}.$$

Note

$$5 = 4 + 1 = \theta^6 + 1 = (\theta^2 + 1)(\theta^4 - \theta^2 + 1) = (\theta^2 + 1)(2\theta + 1 - \theta^2).$$

Hence

$$\theta^2 - 2\theta - 1 \mid 5$$

and

$$\mathfrak{q} = \langle 1 + 2\theta - \theta^2 \rangle$$

is principal. So

$$\mathfrak{pq} = \langle 5 \rangle$$

and

$$\mathfrak{p} = \langle 5 \rangle \mathfrak{q}^{-1} = \langle 5 \rangle \langle 1 + 2\theta - \theta^2 \rangle^{-1} = \langle 1 + \theta^2 \rangle$$
$$(1 + \theta^2)(1 + 2\theta - \theta^2) = 5.$$

Hence $\mathfrak{p}$ is also principal. Is everything principal?

$$M_K \approx 2.9$$

We need to check $p = 2$.

The previous theorem is a special case of :

Theorem 8.11 (Kronecker-Dedekind Factorization)**.** *Let $K = \mathbb{Q}(\theta)$ where $\theta \in \mathcal{O}_K$. Suppose p is a prime such that*

$$p \nmid [\mathcal{O}_K : \mathbb{Z}[\theta]]$$

Let $h(x)$ be the minimum polynomial of θ. Write

$$h(x) = h_1(x)^{e_1} \cdots h_g(x)^{e_g} \mod p$$

Where $h_i(x)$ are monic irreducible. Then

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$$

where

$$\mathfrak{p}_i = (p, h_i(\theta)),$$
$$\mathrm{N}(\mathfrak{p}_i) = p^{\deg h)i}$$

and the $\mathfrak{p}_i$'s are all distinct.

We note some simple corollaries. Let $K = \mathbb{Q}(\theta)$ with for an algebraic integer θ.

Corollary 8.12. *If $p \nmid [\mathcal{O}_K : \mathbb{Z}[\theta]]$ then p ramifies in $\mathcal{O}_K$ if and only if $p \mid \Delta_K = \mathrm{disc}(K)$.*

Proof. Let $h(x) = \prod_{i=1}^n (x - \theta_i)$ be the minimal poly of θ. By the theorem,

$$\langle p \rangle = \langle p, h_1(\theta) \rangle^{e_1} \cdots \langle p, h_g(\theta) \rangle^{e_g}$$

and p ramifies if and only if $e_i > 1$ for some i. That is the case if and only if the poly $\bar{h}$ does not have distinct roots modulo p. But these are exactly the primes that divide

$$\mathrm{disc}\, h(x) = \prod_{i<j} (\theta_i - \theta_j)^2 = \Delta(\theta).$$

So $\bar{h}(x)$ has multiple roots in $\mathbb{F}_p$ if and only if $p \mid \Delta(\theta)$. Recall

$$\Delta(\theta) = \mathrm{disc}(1, \theta, \ldots, \theta^{n-1}) = (\mathrm{disc}(K))[\mathcal{O}_K : \mathbb{Z}[\theta]]^2$$

But our assumption is $p \nmid [\mathcal{O}_K : \mathbb{Z}(\theta)]$. Hence p ramifies if and only if $p \mid \mathrm{disc}(K)$. □

Corollary 8.13. *If K is any number field then there exist only finitely many primes p that ramify in K.*

Proof. There exist only finitely many p that divide $\operatorname{disc}(K)$ or $[\mathcal{O}_K : \mathbb{Z}[\theta]]$. □

05.12.2019

Here is another corollary of the Kummer-Dedekind factorization.

Corollary 8.14. *Let θ be any algebraic integer with minimal polynomial $h(x)$. Assume $h(x)$ is Eisenstein at prime p. If $K = \mathbb{Q}(\theta)$ then p is totally ramified in $\mathcal{O}_K$.*

Recall that Eisenstain at p means if

$$h(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

then

$$p \mid a_1, \ldots, p \mid a_{n-1}, p || a_0,$$

where $||$ means exactly divides.

Proof. The result follows from the following claim.

Claim: If $h(x)$ is Eisenstein at p, then

$$p \nmid [\mathcal{O}_K : \mathbb{Z}[\theta]].$$

Proof of claim: Exercise.

By the claim, we can apply the Kummer-Dedekind factorization theorem to get

$$h(x) = x^n \mod p$$

and hence $(p) = \mathfrak{p}^n$ where $\mathfrak{p} = (p, \theta)$. □

The following sufficient condition for $p \nmid [\mathcal{O}_K : \mathbb{Z}[\theta]]$ is simpler to check in practice.

Proposition 8.15. *Suppose $K = \mathbb{Q}(\theta)$. Let $f = \min_\theta(x)$ of degree n. If $p^2 \nmid \operatorname{disc}(f)$, then $p \nmid [\mathcal{O}_K : \mathbb{Z}[\theta]]$.*

Proof. Recall that

$$\operatorname{disc}(f) \coloneqq (-1)^{n(n-1)} \prod_{i \neq j} (\theta_i - \theta_j) = \prod_{i<j} (\theta_i - \theta_j)^2 = \pm \operatorname{N}_{K/\mathbb{Q}}(f'(\theta)),$$

where θ_i's are the roots in some extension. Also recall that

$$\operatorname{disc}(1, \theta, \ldots, \theta^{n-1}) = \prod_{i<j} (\theta_i - \theta_j)^2.$$

Moreover,

$$\operatorname{disc}(1, \theta, \ldots, \theta^{n-1}) = \operatorname{disc}(K)[\mathcal{O}_K : \mathbb{Z}[\theta]]^2$$

and hence if $p^2 \nmid \operatorname{disc}(f)$, then $p \nmid [\mathcal{O}_K : \mathbb{Z}[\theta]]$. □

Example 8.16. Let $K = \mathbb{Q}(\theta)$ be the cubic field where $\theta^3 - \theta + 4 = 0$.

For a general cubic equation $f(x) = x^3 + ax + b \in \mathbb{Z}[x]$ which is irreducible, we have

$$\operatorname{disc}(f) = -4a^3 - 27b^2.$$

One can prove this using

$$\operatorname{disc}(\theta) = \operatorname{disc}(f) = (-1)^{n(n-1)/2} \prod_{i=1}^{n} f'(\theta_i).$$

If $\theta_1, \ldots, \theta_n$ are the roots and if $n = 3$, then

$$\theta_1 + \theta_2 + \theta_3 = 0$$

$$\theta_1\theta_2 + \theta_2\theta_3 + \theta_2\theta_3 = a$$
$$\theta_1\theta_2\theta_3 = b$$
$$f'(x) = 3x^2 + a$$
$$\theta_1^2 + \theta_2^2 + \theta_3^2 = (\theta_1 + \theta_2 + \theta_3)^2 - 2a = -2a.$$

Now

$$\operatorname{disc}(\theta) = -4 - 27 \cdot 4^2 = -2^2 \cdot 107,$$

so $\operatorname{disc}(K)$ is either $-4 \cdot 107$ or 107.

Check that

$$\alpha = \frac{1}{2}\theta + \frac{1}{2}\theta^2$$

is an algebraic integer with

$$\alpha^3 - \alpha^2 + 3\alpha - 2 = 0.$$

Hence disc $= -107$ and $[\mathcal{O}_K \colon \mathbb{Z}[\theta]] = 2$. So for primes other than 2 we can apply the Kummer-Dedekind factorization theorem.

1. Let $p = 107$. Note that $x^3 - x + 4 = (x-6)^2(x+12) \mod 107$. Hence $(107) = \mathfrak{p}^2\mathfrak{q}$ for $\mathfrak{p} = (107, \theta - 6)$ and $\mathfrak{q} = (107, \theta - 12)$ and $\mathrm{N}(\mathfrak{p}) = \mathrm{N}(\mathfrak{q}) = 107$.
2. Let $p = 3$. Then $x^3 - x + 4 = x^3 - x + 1 \mod 3$, which is irreducible. Hence $(3) = \mathfrak{p}$ for $\mathfrak{p} = (3, \theta^3 - \theta + 1)$ and $\mathrm{N}(\mathfrak{p}) = p^3$.

Next we show K is monogenic to factor 2. Let $\alpha = \frac{\theta + \theta^2}{2}$, then $\mathcal{O}_K = \mathbb{Z}[\alpha]$:

$$\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\left(\frac{\theta + \theta^2}{2}\right)$$

and we want to write θ as a $\mathbb{Z}$-combination of α. Note that

$$\alpha^2 = \left(\frac{\theta + \theta^2}{2}\right)^2 = \cdots = -2 - \theta + \alpha,$$

hence $\theta = -\alpha^2 + \alpha - 2$ and so

$$\begin{aligned}\mathcal{O}_K &= \mathbb{Z} + \mathbb{Z}(-\alpha^2 + \alpha - 2) + \mathbb{Z}\alpha \\ &= \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\alpha^2 \quad (\alpha - 2 \in \mathbb{Z}[\alpha]) \\ &= \mathbb{Z}[\alpha].\end{aligned}$$

Now we can use this to factor 2:

$$\min_{\alpha}(x) = x^3 - x^2 + 3x - 2 = x(x^2 - x + 1) \mod 2.$$

Thus $(2) = \mathfrak{p}\mathfrak{q}$ for $\mathfrak{p} = (2, \alpha)$ and $\mathfrak{q} = (2, \alpha^2 - \alpha + 1)$ with $\mathrm{N}(\mathfrak{p}) = 2$ and $\mathrm{N}(\mathfrak{q}) = 2^2$.

If we did not have noticed that $2 \mid [\mathcal{O}_K : \mathbb{Z}[\theta]$ and applied the Kummer-Dedekind factorization, we would have got that 2 ramifies, which is wrong.

8.3 Factorization in Arbitrary Extensions

What happens if the base field is not $\mathbb{Q}$ but some field K and we have an extension $\mathbb{Q} \subset K \subset L$? In general, if A is an integrally closed integral domain, and $K = \mathrm{Quot}(A)$, L a finite separable extension of K with $[L\colon K] = n$. Let B be the integral closure of A in L.

1. We have seen that if A is a PID then every finitely generated B-submodule M of L is a free A-module of rank $[L\colon K]$.

2. In particular, for the integral closure of $\mathbb{Z}$ in K, i.e. $\mathcal{O}_K$, we have that every finitely generated $\mathcal{O}_K$-submodule $\mathfrak{a}$ of K is a free $\mathbb{Z}$-module of rank $[K\colon \mathbb{Q}]$.

3. The ring $\mathcal{O}_K$ is Noetherian, integrally closed and every prime ideal is maximal, i.e. $\mathcal{O}_K$ is a Dedekind ring.

4. If A is not a PID, then finitely generated does not mean free.

   Example 8.17. $A = \mathbb{Z}[\sqrt{-5}], M = (2, 1 + \sqrt{-5})$ is finitely generated but has no basis.

5. But in general one has

   Theorem 8.18. *Let A be a Dedekind domain with $K = \mathrm{Quot}(A)$ and L finite extension of K with B the integral closure of A in L. Then B is a Dedekind domain.*

   For proofs see Neukirch Prop. 8.1 or Samuel Theorem 1 Sec. 3.4.

   Any prime ideal $\mathfrak{p}$ of A gives rise to an ideal $\mathfrak{p}B$ in B. We can write

   $$\mathfrak{p}B = \prod_{i=1}^{g} \mathfrak{B}_i^{e_i}$$

   where the $\mathfrak{B}_i$'s are distinct prime ideals of B and the e_i's are positive integers.

   Facts: The $\mathfrak{B}_i$'s are precisely those prime ideals $\mathfrak{B}$ of B such that $\mathfrak{B} \cap A = \mathfrak{p}$. As before we say $\mathfrak{B}$ lies above $\mathfrak{p}$.

   We have equivalent conditions for divisibility: $\mathfrak{B} \mid \mathfrak{p}B$ if and only if $\mathfrak{p}B \subset \mathfrak{B}$ if and only if $\mathfrak{B} \cap A = \mathfrak{p}$. So every prime ideal $\mathfrak{B}$ of B lies over a unique prime ideal $\mathfrak{p}$ of A.

   The factor ring $A/\mathfrak{p}$ can be identified as a subring of $B/\mathfrak{B}_i$. Note both rings are fields since $\mathfrak{p}$ and $\mathfrak{B}$ are maximal. The containment of A in B induces a ring homomorphism

   $$A \to B/\mathfrak{B}_i$$

   with kernel $\mathfrak{B}_i \cap A = \mathfrak{p}$. So we obtain an embedding

   $$A/\mathfrak{p} \hookrightarrow B/\mathfrak{B}_i.$$

   These fields are called *residue fields*. They are finite fields and $B/\mathfrak{B}_i$ is an extension of $A/\mathfrak{p}$. Let f_i be its degree:

   $$f_i := [B/\mathfrak{B}_i : A/\mathfrak{p}],$$

   then the f_i's are called *inertia degree* of $\mathfrak{B}_i$ over $\mathfrak{p}$. The exponents e_i in the factorization

   $$\mathfrak{p}B = \prod_{i=1}^{g} \mathfrak{B}_i^{e_i}$$

   are called *ramification indices*.

Theorem 8.19. *With e_i and f_i as above,*

$$\sum_{i=1}^{g} e_i f_i = n = [L\colon K]$$

where e, f are multiplicative in towers, that is if we have $\mathfrak{p} \subset \mathfrak{B} \subset \mathfrak{Q}$ in the situation depicted below,

$$\begin{array}{ccccc}
\mathfrak{Q} & \hookrightarrow & C & \hookrightarrow & L \\
\downarrow & & \downarrow & & \downarrow \\
\mathfrak{B} & \hookrightarrow & B & \hookrightarrow & K \\
\downarrow & & \downarrow & & \downarrow \\
\mathfrak{p} & \hookrightarrow & A & \hookrightarrow & k
\end{array}$$

with a tower of fields $k \subset K \subset L$, then $e(\mathfrak{Q}|\mathfrak{p}) = e(\mathfrak{Q}|\mathfrak{B})e(\mathfrak{B}|\mathfrak{p})$ and $f(\mathfrak{Q}|\mathfrak{p}) = f(\mathfrak{Q}|\mathfrak{B})f(\mathfrak{B}|\mathfrak{p})$.

A generalization of the Kummer-Dedekind factorization theorem also holds. The condition $p \nmid [\mathcal{O}_K\colon \mathbb{Z}[\theta]]$ is replaced by a "relatively prime to the conductor" condition.

The conductor $\mathcal{F}$ of $\mathcal{O}_K[\theta]$ in $\mathcal{O}_L$ is an ideal of $\mathcal{O}_L$:

$$\mathcal{F} = \{\alpha \in \mathcal{O}_L \mid \alpha\mathcal{O}_L \subset \mathcal{O}_K[\theta]\}.$$

Theorem 8.20. *Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ which is relatively prime to the conductor $\mathcal{F}$ and let*

$$p(x) = p_1(x)^{e_1} \cdots p_g(x)^{e_g}$$

be the factorization of the minimal polynomial of θ with

$$\bar{p}(x) = p(x) \mod \mathfrak{p}$$

into irreducibles over the residue field $\mathcal{O}_K \big/ \mathfrak{p}$ with $p_i(x) \in \mathcal{O}_K[x]$ monic. Then

$$\mathfrak{B}_i = \mathfrak{p}\mathcal{O}_L + p_i(\theta)\mathcal{O}_L.$$

Recall: In the case of K is quadratic (which is Galois), we had either

(a) $(p) = \mathfrak{p}$ stayed prime with $\mathrm{N}(\mathfrak{p}) = p^2$, or
(b) $(p) = \mathfrak{p}\mathcal{O}_k$ splits with $\mathrm{N}(\mathfrak{p}) = \mathrm{N}(\mathfrak{q}) = p$, or
(c) $(p) = \mathfrak{p}^2$ is ramified and $\mathrm{N}(\mathfrak{p}) = p$.

When L/K is a Galois extension with $G = \mathrm{Gal}(L/K)$, let $\mathfrak{B}$ be a prime ideal of $\mathcal{O}_L$ above $\mathfrak{p} \subset \mathcal{O}_K$. Then so is $\sigma\mathfrak{B}$ for every $\sigma \in G$. To see this:

$$\sigma\mathfrak{B} \cap \mathcal{O}_K = \sigma(\mathfrak{B} \cap \mathcal{O}_K) = \sigma(\mathfrak{p}) = \mathfrak{p}.$$

And so in fact we have the

Proposition 8.21. *If L/K is Galois with Galois group G, then G acts transitively on the set of all prime ideals $\mathfrak{B}$ of $\mathcal{O}_L$ lying above $\mathfrak{p}$. Moreover they have the same residual degree f and ramification index e. Thus*

$$\mathfrak{p}\mathcal{O}_L = \left(\prod_{i=1}^{g} \mathfrak{B}_i\right)^e$$

and $n = efg$.

9 Ideal Counting and the Class Number Formula

Recall Riemann's zeta function

$$\zeta(s) \coloneqq \sum_{n=1}^{\infty} \frac{1}{n^s}$$

which is defined for $\mathrm{Re}(s) > 1$ and has a simple pole with residue 1 at $s = 1$. Let

$$\Lambda(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s).$$

Then $\Lambda(s)$ has an analytic continuation to the whole complex plane with simple poles at $s = 0, 1$ and satisfies the functional equation

$$\Lambda(s) = \Lambda(1 - s).$$

The Gamma function $\Gamma(s) = \int_0^\infty e^{-t}t^s \frac{\mathrm{d}t}{t}$ has poles at every negative integer and thus ζ has zeros at all even negative integers.

Riemann's second proof of the analytic continuation of $\Lambda(s)$ uses Jacobi's θ-function. It represents $\Gamma(s)$ as an integral transform of

$$\theta(z) = \sum_{n\in\mathbb{Z}} e^{\pi i n^2 z}$$

which converges absolutely and uniformly for $z \in \mathbb{H}$. Then

$$\Lambda(s) = \frac{1}{2}\int_0^\infty (\theta(iy) - 1)y^s \frac{\mathrm{d}y}{y} \tag{4}$$

and θ has some transformation properties:

$$\theta(z + 2) = \theta(z)$$

$$\theta\left(-\frac{1}{2}\right) = \theta(z)$$

$$\theta(iy) = \theta\left(\frac{1}{y}\right).$$

These are used after splitting up the integral in (4) from 0 to 1 and 1 to ∞ to establish the desired transformation properties of $\Lambda(s)$ and show convergence.

Now consider the elliptic curve given by $y^2 = x^3 + ax + b$ and let a_p be the number of solutions modulo p. Further, let Δ be the discriminant of the polynomial on the right hand side. Define

$$L(E, s) \coloneqq \prod_{p|\Delta}(\dots)\prod_{p\nmid\Delta}(1 - a_p p^{-s} + p^{-2s})$$

to be the L-function associated to the elliptic curve. Then L-has an analytic continuation and satisfies a functional equation relating s and $2 - s$. Now $L(E, s)$ has the same analytic properties as the L-function of a modular of weight 2. Deep conjectures of Shimura, Taniyama and Weil state that there exists a cusp form f of weight 2 such that $L(f, s) = L(E, s)$. Wiles and Taylor gave a proof of a special case of this conjecture (namely for so called semi-stable elliptic curves) and thus established Fermat's Last Theorem following work of Frey, Ribet and Serre. The full conjecture was proven in 2001 by Breuil, Conrad, Diamond and Taylor.

Now we focus on number fields again.

Definition 9.1. Let $[K\colon \mathbb{Q}] = n = r_1 + 2r_2$ and define the *Dedekind zeta function of K* to be

$$\zeta_K(s) \coloneqq \sum_{\mathfrak{a}\subset\mathcal{O}_K} \frac{1}{\mathrm{N}(\mathfrak{a})^s}$$

where the the sum is over integral ideals of $\mathcal{O}_K$.

We then have the

Theorem 9.2 (Class Number Formula)**.**

$$\lim_{s\to 1^+}(s-1)\zeta_K(s)=\frac{2^{r_1+r_2}\pi^{r_2}R_K h_K}{w_k|D_K|^{1/2}}$$

where w_K is number of roots of unity contained in K, R_K is the regulator and D_K is the discriminant.

12.12.2019
Let

$$Z(T)\coloneqq\sum_{\substack{I\subset\mathcal{O}_K\\ \mathrm{N}(I)\leq T}}1.$$

Then $Z(T)$ is a non-negative increasing function. We ask for the rate of convergence as $T\to\infty$. We split this problem into h subproblems. Let C be an ideal class, then

$$Z(T;C)\coloneqq\sum_{\substack{I\in C\\ \mathrm{N}(I)\leq T}}1,$$

and hence

$$Z(T)=\sum_{C\in Cl_K}Z(T;C).$$

We will see that $Z(T;C)/T\to k$ for some constant k as $T\to\infty$, which is independent of C. Hence $Z(T)/T\to kh_k$ as $T\to\infty$.

To see the relation of this result to the behaviour of $\zeta_K(s)$, we need the following general result from the theory of Dirichlet series.

Proposition 9.3. *Let $(a_n)_{n=1}^\infty$ be a sequence of real numbers. Assume that*

$$\lim_{m\to\infty}\frac{S(m)}{m}=K,$$

where $S(m)=a_1+\cdots+a_m$. Then the Dirichlet series

$$\sum_{m=1}^{\infty}\frac{a_n}{n^s}$$

is convergent for $\mathrm{Re}(s)>1$ *and*

$$\lim_{s\to 1^+}(1-s)\sum_{n=1}^{\infty}\frac{a_n}{n^s}=K.$$

Proof. Literature. (Neukirch, Hecke, ...) □

Assuming this proposition, we can write

$$\begin{aligned}\zeta_K(C;s)&=\sum_{I\subset C}\frac{1}{(\mathrm{N}(I))^s}\\&=\sum_{n=1}^{\infty}\frac{a(n)}{n^s},\end{aligned}$$

where $a(n)=|\{I\subset C\mid \mathrm{N}(I)=n\}|$ and $S(m)=Z(m;C)$.

The idea is to count the ideals in a class C by counting elements in an ideal $J\in C^{-1}$. This will allow us to interpret $Z(T;C)$ as a certain lattice point. We have the following lemma.

Lemma 9.4. *Let $C \in Cl_K$ be an ideal class. Fix a representative J of C^{-1}. Then*

$$Z(T;C) = |\{\textit{principal ideals } (\alpha) \mid \alpha \in J, |\,\mathrm{N}(\alpha)| \leq \mathrm{N}(J)T\}|.$$

Proof. There is a 1-1 correspondence

$$\{\text{Ideals } I \text{ in } C \text{ with } \mathrm{N}(I) \leq T\} \longleftrightarrow \{\text{principal ideals } (\alpha) \subset J \text{ with } |\,\mathrm{N}(\alpha) \leq |\,\mathrm{N}(J)|T\}.$$

To see this, if $I \subset C$ and $\mathrm{N}(I) \leq T$, then $IJ = (\alpha)$ where $\alpha \in J$ and $|\,\mathrm{N}(\alpha)| = \mathrm{N}(I)\,\mathrm{N}(J) \leq \mathrm{N}(J)T$.

Conversely suppose $\alpha \in J$ and $|\,\mathrm{N}(\alpha)| \leq \mathrm{N}(J)T$. Then $(\alpha) = IJ$ for some I. Moreover, $I \in C$ and $\mathrm{N}(I) = |\,\mathrm{N}(\alpha)|/\,\mathrm{N}(J)K \leq \mathrm{N}(J)T/\,\mathrm{N}(J) = T$.

Counting principal ideals is "almost" counting elements α, but up to units. If K contains only finitely many units, i. e. K is an imaginary quadratic field, then $|\mathcal{O}_K^\times| Z(T;C) = |\{\alpha \in J \mid |\,\mathrm{N}(\alpha)| \leq \mathrm{N}(J)T\}|$. This can be established by a basic lattice point counting principle.

Recall using Minkowski's embedding we can identify J with a lattice Λ_J in $K_\mathbb{R} \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. In $K = \mathbb{Q}(\sqrt{d})$ with $d < 0$,

$$i\colon K \to \mathbb{R}^2, \quad \alpha \mapsto (\mathrm{Re}(\alpha), \mathrm{Im}(\alpha))$$

and $\mathrm{N}(\alpha) = \|i(\alpha)\|^2$. Then

$$|\{\alpha \in J \mid |\,\mathrm{N}(\alpha)| < \mathrm{N}(J)T\}| = \sum_{v \in \Lambda_J \cap B(T)} 1,$$

where $B(T) = \{v \in \mathbb{R}^2 \mid 0 \leq \|v\|^2 \leq \mathrm{N}(J)T\}$.

Let us look first at the most basic lattice $\mathbb{Z}^n$. Given a bounded region B in $\mathbb{R}^n$, we want to estimate the number of lattice points in B. We expect that this is about $\mathrm{vol}(B)$. To make a more precise statement, we take a family of expanding regions rather than just one. For each $t > 0$ let $tB = \{tx \mid x \in B\}$. If B is "nice" enough, then

$$\int_{r^n} \mathbb{1}_B \mathrm{d}x$$

exists. The most basic result is

Lemma 9.5. *Let B be a bounded Jordan measurable set in $\mathbb{R}^n$. Then*

$$\frac{1}{t^n} \sum_{v \in \mathbb{Z}^n} \mathbb{1}_{tB}(v) \xrightarrow{t\to\infty} \mathrm{vol}(B).$$

Proof. We have

$$\frac{1}{t^n} \sum_{v \in \mathbb{Z}^n} \mathbb{1}_{tB}(v) = \frac{1}{t^n} \sum_{v \in (\mathbb{Z}/t)^n} \mathbb{1}_B(v),$$

and the sum on the right hand side is just a Riemann sum for $\int\limits_{\mathbb{R}^n} \mathbb{1}_B \mathrm{d}x$.

□

For a general lattice Λ with basis $v_1, \ldots, v_n$ let

$$L\colon \mathbb{R}^n \to r^n, \quad v_i \mapsto e_i,$$

then $L(\mathbb{Z}^n) = \Lambda$ and $B \subset \mathbb{R}^n$ has a well defined volume if and only if $L(B)$ has. Then $\mathrm{vol}(L(B)) = \mathrm{vol}(B) \cdot \mathrm{vol}(\mathbb{R}^n/\Lambda)$ and we have the following corollary:

Corollary 9.6. *Let $B \subset \mathbb{R}^n$ be nice enough. Then*

$$\frac{1}{t^n} \sum_{v \in \Lambda} \mathbb{1}_{tB}(v) \xrightarrow{t\to\infty} \frac{\mathrm{vol}(B)}{\mathrm{vol}(\Lambda)}.$$

So the problem we are looking at is

$$|\mathcal{O}_K^\times| Z(T;C) = \sum_{v \in \Lambda_J \cap B(T)} 1,$$

where $B(T) = \{v \in \mathbb{R}^2 \mid 0 \leq \|v\|^2 \,\mathrm{N}(J)T\} = tB$ with $t = (\mathrm{N}(J)T)^{1/2}$. We get

$$\frac{1}{\mathrm{N}(J)T} \sum_{v \in \Lambda_J \cap (tB)} 1 \to \frac{\mathrm{vol}(B)}{\mathrm{vol}(\Lambda_J)}.$$

Recall $\mathrm{vol}(\Lambda_J) = \mathrm{vol}(\mathbb{R}^2/\Lambda_J) = 2^{-1}\,\mathrm{N}(J)|D_K|^{1/2}$. Putting everything together $\mathrm{vol}(B) = \pi$:

$$\frac{Z(T;C)}{T} \to \frac{2\pi}{|\mathcal{O}_K^\times||D_K|^{1/2}} = \frac{2\pi}{w|D_K|^{1/2}}$$

and hence

$$\frac{Z(T)}{T} \to \frac{2\pi h_k}{w|D_K|^{1/2}}$$

and $\lim_{s\to 1^+}(s-1)\zeta_K(s) = \frac{2\pi h_k}{w|D_K|^{1/2}}$, which finishes the proof of the class number formula for the imaginary quadratic case.

□

Let us now look at the *real quadratic* case. In this case the Minkowski embedding is given by

$$i\colon K \to K_{\mathbb{R}} = \mathbb{R}^2, \quad \alpha \mapsto (\alpha, \alpha'),$$

where α' is a Galois conjugate of α. Then $Z(T;C)$ counts $\alpha \in J$ for which $i(\alpha)$ lies in the region $\{(x,y) \in \mathbb{R}^2 \mid 0 < |xy| \leq \mathrm{N}(J)T\}$. **But** with the important point that we want to count each associate of α only once.

(Exam: She makes a box with the *Exercise* questions and chooses some randomly. Then some theory kind of question. Typically she asks two or three questions, since there isn't that much time.)

We count those points by constructing a subset D in which no 2 members of $\mathcal{O}_K$ differ by a unit, so no associates, and each non-zero element of $\mathcal{O}_K$ has a representative modulo units. Then we count the elements of J in that set. We can actually use just the free part of the unit group, i. e. the action of the fundamental unit ε. Recall $\mathcal{O}_K^\times = \{\pm 1\} \times \varepsilon^{\mathbb{Z}}$. Then

$$2Z(C;T) = |\{v = (x,y) \in i(J) \cap D \mid |\,\mathrm{N}(v)| \leq \mathrm{N}(J)T\}.$$

Define $D(T) \coloneqq \{v \in D \mid |\,\mathrm{N}(v)| \leq \mathrm{N}(J)T\}$.

Lemma 9.7. *Let ε be the fundamental unit of $\mathcal{O}_K^\times$. Every non-zero $\alpha \in \mathcal{O}_K$ has an associate β satisfying*

$$1 \leq |\beta'/\beta| \leq \varepsilon^2.$$

These inequalities determine β up to sign.

Proof. Recall that all associates β of α are of the form

$$\beta = \pm\varepsilon^j \alpha$$

by Dirichlet's Unit theorem, $1 = |\,\mathrm{N}(\varepsilon)|$ and $|\beta'/\beta| = |\varepsilon'^j \alpha'/(\varepsilon^j \alpha)| = \varepsilon^{-2j}|\alpha'/\alpha|$. The conditions $1 \leq |\beta'/\beta| \leq \varepsilon^2$ determine j uniquely up to sign of β. □

Let $D = \{v = (x, y) \mid 1 \leq |y/x| < \varepsilon^2\}$ and $D(T) = \{(x, y) \mid 1 \leq |y/x| < \varepsilon^2, 0 < |xy| \leq \mathrm{N}(J)T\}$. Then

$$2Z(T; C) = \sum_{v \in \Lambda_J \cap D(T)} 1.$$

Put $D_1 = \{(x, y) \mid 0 < |xy| \leq 1, 1 \leq |y/x| < \varepsilon^2\}$, then $D(T) = (\mathrm{N}(J)T)^{1/2} D_1$. By the same lattice counting principle as above,

$$\frac{1}{\mathrm{N}(J)T} \sum_{v \in \Lambda_J \cap D(T)} 1 \to \frac{\mathrm{vol}(D_1)}{\mathrm{vol}(\mathbb{R}^2/\Lambda_J)},$$

where $\mathrm{vol}(\Lambda_J) = \mathrm{N}(J)|D_K|^{1/2}$. What we need is $\mathrm{vol}(D_1)$.

$$\begin{aligned} \frac{1}{4}\,\mathrm{vol}(D_1) &= \int_0^{\varepsilon^{-1}} (\varepsilon^2 x - x)\mathrm{d}x + \int_{\varepsilon^{-1}}^1 (\frac{1}{x} - x)\mathrm{d}x \\ &= \log(\varepsilon). \end{aligned}$$

Hence

$$\frac{Z(T; C)}{T} \xrightarrow{T \to \infty} \frac{2\log(\varepsilon)}{|D_K|^{1/2}}.$$

The general case is similar.

Proof of the Class Number Formula. Let $U = \mathcal{O}_K^\times = W \times V$, where $W = \mu_k$ consists of the roots of unity in K and V is the free part of $\mathcal{O}_K^\times$ of rank $r_1 + r_2 - 1$. Recall the maps

$$V \subset \mathcal{O}_K \setminus \{0\} \overset{i}{\hookrightarrow} \Lambda_K \setminus \{0\} \overset{\ell}{\to} \mathbb{R}^{r_1 + r_2}.$$

Under $\lambda = l \circ i$ the units map onto a lattice $\lambda_U \subset H \subset \mathbb{R}^{r_1+r_2}$, where $H = \{y \in \mathbb{R}^{r_1+r_2} \mid y_1 + \cdots y_{r_1+r_2} = 0\}$ and $\ker \lambda = W$. The restriction of λ to V is an isomorphism. Under the embedding i, let $i(V) = \tilde{V}$. We can use a set of coset representatives of $\tilde{V}$ in $K_{\mathbb{R}}^\times = (\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2}$ to count members of J such that $(\alpha) \subset J$ with $|\mathrm{N}(\alpha)| < \mathrm{N}(J)T$ by counting numbers $x \in \Lambda_J \cap D$ which satisfy $|\mathrm{N}(\alpha)| < \mathrm{N}(J)T$. To find D, we use the following general lemma.

Lemma 9.8. *Suppose $f\colon G \to G'$ is a homomorphism of Abelian groups. Let S be a subgroup of G which is carried isomorphically onto a subgroup S' of G'. Suppose D' is a set of coset representatives for S' in G'. Then $D \coloneqq f^{-1}(D')$ is a set of representatives for S in G.*

Proof. Marcus, Number Fields, last chapter. □

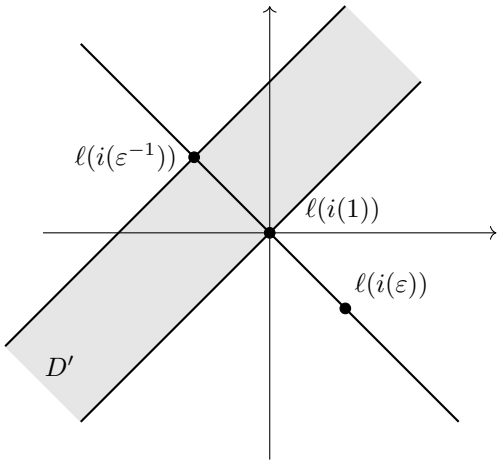
We apply this to the homomorphism

$$\ell\colon K_{\mathbb{R}}^\times \to \mathbb{R}^{r_1+r_2}, \quad \tilde{V} \to \Lambda_U \subset H.$$

So we want D', a set of representatives of Λ_U in $\mathbb{R}^{r_1+r_2}$.

In the case of a real quadratic, i. e. $K = \mathbb{Q}(\sqrt{d})$ with $d > 0$, we have $H = \{(x, y) \mid x + y = 0\}$ and a set of representatives is depicted by the shaded region in the figure below:
In general fix a set of fundamental units $\varepsilon_1, \ldots, \varepsilon_r$ and let $\{\lambda(\varepsilon_1), \ldots, \lambda(\varepsilon_r)\} =: \{v_1, \ldots, v_r\} \subset H$. Put $F = \{t_1 v_1 + \ldots t_r v_r \mid 0 \leq t_i < 1\}$ and take $D' = F \oplus L$, where L is a line through the origin not in H. A particularly good choice is $v = \{\underbrace{1, \ldots, 1}_{r_1}, \underbrace{2, \ldots, 2}_{r_2}\}$ with this choice of v D becomes a cone i. e. if $x \in D$, then $tx \in D$ for all $t > 0$.

□



10 Cyclotomic Fields

Consider $K = \mathbb{Q}(\zeta_n)$ with ζ_n a primitive n th root of unity. (Remark: if $n \equiv 2 \mod 4$ then $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{n/2})$.) Then $K/\mathbb{Q}$ is Galois and Abelian. Put

$$d = \varphi(n) \text{ and } n = \prod_p p^{\nu_p},$$

then

$$\varphi(n) = \prod_p \varphi(p^{1/p}) = \prod_p p^{\nu_p - 1}(p-1).$$

The ring of integers is $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$ for all n. The discriminant is

$$\operatorname{disc}(K) = \prod_{p|n} p^{s_p}$$

The ramification of a prime p depends only on $p \mod n$. It is totally split if and only if $p \equiv 1 \mod n$.

What about the class number $h_n = \#Cl_K$ and $E_n = \mathcal{O}_K^\times$?

Kummer: $h_n = h_n^+ h_n^-$ where h_n^+ is the class number of the maximal totally real subfield $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ and we have a formula for h_n^-.

Lemma 10.1. *Let $n = p^\nu$ for a prime number p and $\lambda = 1 - \zeta$. Then*

1. *(λ) is a prime ideal of inertia degree 1, i.e. $\left(\mathcal{O}_K \Big/ (\lambda) \cong \mathbb{Z} \Big/ p\mathbb{Z}\right)$.*
2. $$(\lambda)^{\varphi(p^\nu)} = (p)$$
3. *The discriminant is*
$$\operatorname{disc}(1, \zeta, \ldots, \zeta^{d-1}) = \pm p^{p^{\nu-1}(\nu p - \nu - 1)}$$

Proof. We prove 2. first. Recall that

$$\Phi_n(x) = \prod_{\xi \text{ prim. } n\text{-th root of unity}} (x - \xi).$$

In particular

$$\Phi_{p^\nu}(x) = \frac{x^{p^\nu} - 1}{x^{p^{\nu-1}} - 1} = 1 + x^{p^{nu-1}} + \cdots + x^{(p-1)p^{\nu-1}}$$

then

$$p = \varphi_{p^\nu}(1) = \prod_{\xi}(1-\xi) = \prod_{g \not\equiv 0 \mod p}(1-\zeta^g) = e \cdot (1-\zeta)^{\varphi(p^\nu)} = e \cdot \lambda^{\varphi(p^\nu)},$$

where $e_g = (1-\zeta^g)/(1-\zeta)$ is a unit. This proves 2.

Now for 3.

$$\operatorname{disc}(1, \ldots, \zeta^{d-1}) = \pm \prod_{i \neq j}(\zeta_i - \zeta_j) = \pm \prod_{i=1}^{K} \varphi_n'(\zeta_i) = \pm \operatorname{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\varphi_n'(\zeta)).$$

Next note that

$$(X^{p^{v-1}} - 1)\Phi_n(X) = X^{p^v} - 1$$

and so taking the derivative at ζ gives

$$(\zeta^{p^v} - 1)\varphi_n'(\zeta) = p^v \zeta^{p^v - 1}.$$

This implies $\operatorname{N}(\Phi_n'(\zeta)) = \operatorname{N}(p^v)/\operatorname{N}(\zeta^{p^v-1})$. So if $\operatorname{N}(\zeta^{p^v-1} - 1) = \pm p^{p^v-}$, then 3. follows, which we leave as an exercise. □

Proposition 10.2. *$\mathcal{O}_K = \mathbb{Z}[\zeta]$, i.e. $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\zeta \oplus \cdots \oplus \mathbb{Z}\zeta^{d-1}$*

Proof. Reduce to the case $n = p^v$ (e.g. by induction on $p \mid n$) and show that $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$ and $\operatorname{disc}(K) \mid n$. Then use the following fact: If $K = \mathbb{Q}(\alpha)$ and $L = \mathbb{Q}(\beta)$ have coprime discriminant and $\alpha_1, \ldots, \alpha_n$ generate O_K and $\beta_1, \ldots, \beta_m$ generate $\mathcal{O}_L$, then $\{\alpha_i\beta_j\}$ generate $\mathcal{O}_{KL}$.

Now we turn to the case $n = p^v$. Clearly $\mathbb{Z}[\zeta] \subset \mathcal{O}_K$ and we know $\operatorname{disc}(K) = \pm p^s$ for some $s \geq 1$. Hence $p^s\mathcal{O}_K \subset \mathbb{Z}[\zeta]$. From the previous lemma we know that $\lambda = 1 - \zeta$ has norm p. Hence $\mathbb{Z} + (\lambda) = \mathcal{O}_K$ and in particular $\mathbb{Z}[\zeta] + (\lambda) = \mathcal{O}_K$. We get $\lambda\mathbb{Z}[\zeta] + (\lambda)^2 = (\lambda)$ and thus $\mathbb{Z}[\zeta] + (\lambda)^2 = \mathcal{O}_K$. Continuing in this fashion yields $(\lambda)^r + \zeta[\zeta] = \mathcal{O}_K$ for all $t \geq 1$. Choosing t appropriately (p) is a power of (λ)) gives $\mathcal{O}_K = \mathbb{Z}[\zeta] + (p^s) \subset \mathbb{Z}[\zeta]$. □

Proposition 10.3. *Let $f_p > 1$ be the smallest integer such that $p^{f_p} \equiv 1 \mod (n/p^{v_p})$. Then $(p) = (\mathfrak{B}_1 \cdots \mathfrak{B}_\mathfrak{r})^{\varphi(p^v)}$ where the inertia degree of $\mathfrak{B}_i = f_p$.*