Algebraic Number Theory

Johan Bosman
Notes by Florian Bouyer

Contents

1 Introduction and Motivations

Most of the ideas in this section will be made more formal and clearer in later sections.

1.1 Motivations

Definition 1.1. An element α of $\mathbb{C}$ is an *algebraic number* if it is a root of a non-zero polynomial with rational coefficients

A *number field* is a subfield K of $\mathbb{C}$ that has finite degree (as a vector space) over $\mathbb{Q}$. We denote the degree by $[K:\mathbb{Q}]$.

Example.

- $\mathbb{Q}$
- $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$
- $\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$
- $\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}[x]/(x^3 - 2)$

Note that every element of a number field is an algebraic number and every algebraic number is an element of some number field. The following is a brief explanation of this.

Let K be a number field, $\alpha \in K$. Then $\mathbb{Q}(\alpha) \subseteq K$and we will late see that $[\mathbb{Q}(\alpha) : \mathbb{Q}] | [K : \mathbb{Q}] < \infty$. So there exists a relation between $1, \alpha, \ldots, \alpha^n$ for some n. If α is algebraic then there exists a minimal polynomial f for which α is a root. $\mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(f)$ has degree $\deg(f)$ over $\mathbb{Q}$.

Consider $\mathbb{Z}[i] \subset \mathbb{Q}[i]$, also called the *Gaussian integers*. A question we may ask, is what prime number p can be written as the sum of 2 squares? That is $p = x^2 + y^2 = (x + iy)(x - iy)$, we "guess" that an odd prime p is $x^2 + y^2$ if and only if $p \equiv 2 \mod 4$. A square is always 0 or $1 \mod 4$, so the sum of two squares is either $0, 1$ or $2 \mod 4$. Hence no number that is $3 \mod 4$ is the sum of two squares. Therefore not all numbers that are $1 \mod 4$ can be written as the sum of two squares.

Notice that there exist complex conjugation in $\mathbb{Z}[i]$, that is the map $a + bi \mapsto a - bi = \overline{a + bi}$ is a ring automorphism. We can define the norm map $N : \mathbb{Z}[i] \to \mathbb{Z}$ by $\alpha \mapsto \alpha\overline{\alpha}$, more explicitly, $(a + bi) \mapsto (a + bi)(a - bi) = a^2 + b^2$. We will later see that $N(\alpha\beta) = N(\alpha)N(\beta)$.

Definition 1.2. Let K be a number field, a element $\alpha \in K$ is called a *unit* if it is invertible. That is there exists $\beta \in K$ such that $\alpha\beta = 1$.

Proposition 1.3. *The units of* $\mathbb{Z}[i]$ *are* $1, -1, i, -i$

Proof. Let $\alpha \in \mathbb{Z}[i]$ be a unit. Then $N(\alpha)$ is a unit in $\mathbb{Z}$, (since there exists $\beta \in \mathbb{Z}[i]$ such that $\alpha\beta = 1$, hence $1 = N(\alpha\beta) = N(\alpha)N(\beta)$) Now let $\alpha = a + bi$, then $N(\alpha) = a^2 + b^2 = \pm 1$. Now -1 is not the sum of two squares hence $\alpha \in \{\pm 1, \pm i\}$ □

Definition 1.4. Let K be a number field, an element $\alpha \in K$ is *irreducible* if α is not a unit, and for all $\beta, \gamma \in \mathbb{Z}[i]$ with $\alpha = \beta\gamma$, we have either β or γ is a unit.

Fact. $\mathbb{Z}[i]$ *is a unique factorization domain, that is every non-zero elements* $\alpha \in \mathbb{Z}[i]$ *can be written as a product of irreducible elements in a way that is unique up to ordering and multiplication of irreducible elements by units.*

Theorem 1.5. *If* $p \equiv 1 \mod 4$ *is a prime then there exists* $x, y \in \mathbb{Z}$ *such that* $p = x^2 + y^2 = (x + iy)(x - iy) = N(x + iy)$

Proof. First we show that there exists $a \in \mathbb{Z}$ such that $p | a^2 + 1$. Since $p \equiv 1 \mod 4$ we have $\left(\frac{-1}{p}\right) = 1$ (see Topics in Number Theory). Let $a = \frac{p-1}{2}!$, then $a^2 = \left(\frac{p-1}{2}\right)! \left(\frac{p-1}{2}\right)! = 1 \cdot \cdots \cdot \left(\frac{p-1}{2}\right) \cdot \left(\frac{p-1}{2}\right) \cdot \cdots \cdot 1 \equiv -1 \mod p$. Hence $p | a^2 + 1 = (a + i)(a - i)$.

Is p irreducible in $\mathbb{Z}[i]$? If p were indeed irreducible, then $p | (a + i)$ or $p | (a - i)$. Not possible since $a + i = p(c + di) = pc + pdi$ means $pd = 1$. So p must be reducible in $\mathbb{Z}[i]$. Let $p = \alpha\beta$, $\alpha, \beta \notin (\mathbb{Z}[i])^*$ and $N(p) = p^2 = N(\alpha)N(\beta) \Rightarrow N(\alpha) \neq \pm 1 \neq N(\beta)$. So $N(\alpha) = p = N(\beta)$. Write $\alpha = x + iy$, then $N(\alpha) = p = x^2 + y^2$ □

1.2 Finding Integer Solutions

Problem 1.6. Determine all integer solution of $x^2+1=y^3$

Answer. First note $x^2+1=(x+i)(x-i)=y^3$, we'll use this to show that if $x+i$ and $x-i$ are coprime then $x+i$ and $x-i$ are cubes in $\mathbb{Z}[i]$.

Suppose that they have a common factor, say δ. Then $\delta|(x+i)-(x-i)=2i=(1+i)^2$. So if $x+i$ and $x-i$ are not coprime, then $(1+i)|(x+i)$, i.e.,$(x+i)=(1+i)(a+bi)=(a-b)+(a+b)i$. Now $a+b$ and $a-b$ are either both even or both odd. We also know that $a+b=1$, so they must be both odd, hence x is odd. Now an odd square is always $1 \mod 8$. Hence $x^2+1\equiv 2 \mod 8$, so x^2+1 is even but not divisible by 8, contradicting the fact that is is a cube.

Hence $x+i$ and $x-i$ are coprime in $\mathbb{Z}[i]$. So let $x+i=\epsilon\pi_1^{e_1}\dots\pi_n^{e_n}$ where π_i are distinct up to units. Now $x-i=\overline{x+i}=\overline{\epsilon}\overline{\pi_1}^{e_1}\dots\overline{\pi_n}^{e_n}$. So $(x+i)(x-i)=\epsilon\overline{\epsilon}\pi_1^{e_1}\dots\pi_n^{e_n}\overline{\pi_1}^{e_1}\dots\overline{\pi_n}^{e_n}=y^3$. Let $y=\epsilon' q_1^{f_1}\dots q_n^{f_n}\Rightarrow y^3=\epsilon'^3 q_1^{3f_1}\dots q_n^{3f_n}$. The q_i are some rearrangement of $\pi_i,\overline{\pi}_i$ up to units. Hence we have $e_i=3f_j$, so $x+i=$unit times a cube, (Note in $\mathbb{Z}[i]$, $\pm1=(\pm1)^3$ and $\pm i=(\mp i)^3$). Hence $x+i$ is a cube in $\mathbb{Z}[i]$.

So let $x+i=(a+ib)^3$ for some $a,b\in\mathbb{Z}$. Then $x+i=a^3+3a^2bi-3ab^2-b^3i=a^3-3ab^2+(3a^2b-b^3)i$. Solving the imaginary part we have $1=3a^2b-b^3=b(3a^2-b^2)$. So $b=\pm1$ and $3a^2-b^2=3a^2-1=\pm1$. Now $3a^2=2$ is impossible, so we must have $3a^2=0$, i.e., $a=0$ and $b=-1$. This gives $x=a^3-3ab^2=0$.

Hence $y=1,x=0$ is the only integer solution to $x^2+1=y^3$ □

Theorem 1.7 (This is False)**.** *The equation $x^2+19=y^3$ has no solutions in $\mathbb{Z}$ (Not true as $x=18,y=17$ is a solution since $18^2+19=324+19=343=17^2$)*

Proof of False Theorem. This proof is flawed as we will explain later on. (Try to find out where it is flawed)

Consider $\mathbb{Z}[\sqrt{-19}]=\{a+b\sqrt{-19}:a,b\in\mathbb{Z}]$. Then we define the conjugation this time to be $\overline{a+b\sqrt{-19}}=a-b\sqrt{-19}$, and similarly we define a norm function $N:\mathbb{Z}[\sqrt{-19}]\to\mathbb{Z}$ by $\alpha\mapsto\alpha\overline{\alpha}$. Hence $N(a+b\sqrt{-19})=a^2+19b^2$. So we have $x^2+19=(x+\sqrt{-19})(x-\sqrt{-19})$.

Suppose that these two factors have a common divisor, say δ. Then $\delta|2\sqrt{-19}$. Now $\sqrt{-19}$ is irreducible since $N(\sqrt{-19})=19$ which is a prime. If $2=\alpha\beta$ with $\alpha,\beta\notin\left(\mathbb{Z}[\sqrt{-19}\right)^*$, then $N(\alpha)N(\beta)=N(2)=2^2$, so $N(\alpha)=2$ which is impossible. So 2 is also irreducible. Hence we just need to check where $2|x+\sqrt{-19}$ or $\sqrt{-19}|x+\sqrt{-19}$ is possible.

Suppose $\sqrt{-19}|x+\sqrt{-19}$, then $x+\sqrt{-19}=\sqrt{-19}(a+b\sqrt{-19})=-19b+a\sqrt{-19}$, so $a=1$ and $19|x$. Hence $x^2+19\equiv19 \mod 19^2$, i.e., x^2+19 is divisible by 19 but not by 19^2 so it can't be a cube. Suppose $2|x+\sqrt{-19}$, then $x+\sqrt{-19}=2a+2b\sqrt{-19}$, which is impossible.

Hence we have $x+\sqrt{-19}$ and $x-\sqrt{-19}$ are coprime, and let $x+\sqrt{-19}=\epsilon\pi_1^{e_1}\dots\pi_n^{e_n}$. Then $x-19=\overline{x+\sqrt{-19}}=\overline{\epsilon}\overline{\pi_1}^{e_1}\dots\overline{\pi_n}^{e_n}$, so $(x+\sqrt{-19})(x-\sqrt{-19})=\epsilon\overline{\epsilon}\pi_1^{e_1}\dots\pi_n^{e_n}\overline{\pi_1}^{e_1}\dots\overline{\pi_n}^{e_n}=y^3$. If we let $y=\epsilon' q_1^{f_1}\dots q_n^{f_n}$, then $y^3=\epsilon'^3q_1^{3f_1}\dots q_n^{3f_n}$, so the q_i are some rearrangements of $\pi_i,\overline{\pi_i}$ up to units. Hence corresponding $e_i=3f_i$ and so $x+\sqrt{-19}=$unit times a cube. Now units of $\mathbb{Z}[\sqrt{-19}]=\{\pm1\}$.

So $x+\sqrt{-19}=(a+b\sqrt{-19})^3=(a^3-19ab^2)+(3a^2b-19b^3)\sqrt{-19}$. Again comparing $\sqrt{-19}$ coefficients we have $b(3a^2-19b^2)=1$, so $b=\pm1$ and $3a^2-19=\pm1$. But $3a^2=20$ is impossible since $3\nmid 20$, and $3a^2=18=3\cdot6$ is impossible since 6 is not a square. So no solution exists. □

This proof relied on the fact that $\mathbb{Z}[\sqrt{-19}]$ is a UFD, which it is not. We can see this by considering $343=7^3=(18+\sqrt{-19})(18-\sqrt{-19})$. Now $N(7)=7^2$. Suppose $7=\alpha\beta$ with $\alpha,\beta\notin\left(\mathbb{Z}[\sqrt{-19}]\right)^*$. Then $N(\alpha)N(\beta)=7^2$, so $N(\alpha)=7$, but $N(a+b\sqrt{-19})=a^2+19b^2\neq7$. So 7 is irreducible in $\mathbb{Z}[\sqrt{-19}]$. On the other hand $N(18+\sqrt{19})=7^3$, and suppose that $N(\alpha)N(\beta)=7^3$, then without loss of generality $N(\alpha)=7$ and $N(\beta)=7^2$. But we have just seen no elements have $N(\alpha)=7$, so $18+\sqrt{-19}$ is irreducible in $\mathbb{Z}[\sqrt{-19}]$. The same argument shows that $18=\sqrt{-19}$ is also irreducible in $\mathbb{Z}[\sqrt{-19}]$

1.3 Pell's Equations

Fix $d\in\mathbb{Z}_{>0}$ with $d\neq a^2$ for any $a\in\mathbb{Z}$. Then Pell's equation is $x^2-dy^2=1$, with $x,y\in\mathbb{Z}$.

Now $\mathbb{Z}[\sqrt{d}]=\{a+b\sqrt{d}:a,b\in\mathbb{Z}\}$. This has an automorphism $a+b\sqrt{d}\mapsto a-b\sqrt{d}=\overline{a+b\sqrt{d}}$. (Note that $^{-}$ is just notation, and it does not mean complex conjugation). Again we can define a function called the norm, $N:\mathbb{Z}[\sqrt{d}]\to\mathbb{Z}$ defined by $\alpha\mapsto\alpha\overline{\alpha}$, and explicitly $(a+b\sqrt{d})\mapsto a^2-db^2$. Hence Pell's equation comes down to solving $N(x+y\sqrt{d})=1$.

Now recall that $\alpha \in \left(\mathbb{Z}[\sqrt{d}]\right)^*$, then there exists β such that $\alpha\beta = 1$. So $N(\alpha)N(\beta) = 1$, so $N(\alpha) = \pm 1$. On the other hand if $N(\alpha) = \pm 1$, then $\alpha\overline{\alpha} = \pm 1$, so $\pm\overline{\alpha} = \alpha^{-1}$, hence α is a unit.

Example. $d = 3$. Then $x^2 - 3y^2 = 1 \Rightarrow 3y^2 + 1 = x^2$

$y = 0$ $3y^2 + 1 = 1$. This is ok, it leads to $(1, 0)$ which correspond to $1 \in \mathbb{Z}[\sqrt{3}]$

$y = 1$ $3y^2 + 1 = 4$. This is ok, it leads to $(2, 1)$ which gives $2 + \sqrt{3} \in \mathbb{Z}[\sqrt{3}]$

$y = 2$ $3y^2 + 1 = 13$

$y = 3$ $3y^2 + 1 = 28$

$y = 4$ $3y^2 + 1 = 49$. This is ok, it leads to (7,4) which gives $7 + 4\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$

Note that if ϵ is a unit in $\mathbb{Z}[\sqrt{d}]$, then $\pm\epsilon^n$ is a unit for all $n \in \mathbb{Z}$. (For example $(2+\sqrt{3})^2 = 2^2+2\cdot 2\sqrt{3}+3 = 7+4\sqrt{3}$. If x, y is a solution, then of course $(-x, -y)$ is a solution as well. Hence there are infinitely many solutions

Theorem 1.8. *Let $d \in \mathbb{Z}_{>0}$ with $d \neq a^2$. Then there exists $\epsilon_d \in \mathbb{Z}[\sqrt{d}]$, $\epsilon_d \neq \pm 1$ such that every unit can be written as $\pm\epsilon_d^n$, $n \in \mathbb{Z}$. Such an ϵ_d is called a* Fundamental Unit *of $\mathbb{Z}[\sqrt{d}]$. If ϵ_d is a fundamental unit, then so is $\pm\epsilon_d^{-1}$.*

Proof. This is a consequence of Dirichlet's Unit Theorem, which we will prove at the end of the course. □

Example. We will show that $\epsilon_3 = 2 + \sqrt{3} \in \mathbb{Z}[\sqrt{3}]$

Let $x_1 + y_1\sqrt{3} \in \mathbb{Z}[\sqrt{d}]$ be a fundamental unit. Without any lost of generality we can assume that $x_1 \geq 0$. Now $(x_1 + y_1\sqrt{3})^{-1} = \frac{x_1 - y_1\sqrt{3}}{(x_1+y_1\sqrt{3})(x_1-y_1\sqrt{3})} = \pm(x_1 - y_1\sqrt{3})$. So without loss of generality we can also assume $y_1 \geq 0$.

Put $x_n + y_n\sqrt{3} = (x_1 + y_1\sqrt{3})^2 = x_1^n + nx_1^{n-1}y\sqrt{3} + \dots$. So $x_n = x_1^n + \cdots \geq x_1^n$ and $y_n = nx_1^{n-1}y_1$. If $x_1 = 0$ then $3y_1^2 = \pm 1$ which is not possible. Similarly if $y_1 = 0$ then $x_1^2 = 1 \Rightarrow x_1 = \pm 1$ and $\epsilon_3 = \pm 1$ which is impossible by definition. So $x_1 \geq 1, y_1 \geq 1$. For $n \geq 2 : x_n \geq x_1^n \geq x_1$ and $y_n = nx_1^{n-1}y_1 >\geq ny_1 > y_1$

Conclusion: A solution (x, y) of $x^2 - 3y^2 = \pm 1$ with $y \geq 1$ minimal is a Fundamental unit for $\mathbb{Z}[\sqrt{3}]$. Hence $2+\sqrt{3}$ is a fundamental unit for $\mathbb{Z}[\sqrt{3}]$, so all solution for $x^2+3y^2 = \pm 1$ are obtained by $(x, y) = (\pm x_n, \pm y_n)$ where $x_n + y_n\sqrt{3} = (2 + \sqrt{3})^n$.

2 Fields, Rings and Modules

2.1 Fields

Definition 2.1. If K is a field then by a *field extension* of K, we mean a field L that contains K. We will denote this by L/K.

If L/K is a field extension, then multiplication of K on L defines a K-vector space structure on L. The *degree* $[L : K]$ of L/K is the dimension $\dim_K(L)$

Example.
- $[K : K] = 1$
- $[\mathbb{C} : \mathbb{R}] = 2$
- $[\mathbb{R} : \mathbb{Q}] = \infty$ (uncountably infinite)

The Tower Law. *If L/K and M/K are fields extensions with $L \subseteq M$, then $[M : K] = [M : L][L : K]$*

Proof. Let $\{x_\alpha : \alpha \in I\}$ be a basis for L/K and let $\{y_\beta : \beta : J\}$ be a basis for M/L. Define $z_{\alpha\beta} = x_\alpha y_\beta \in M$. We claim that $\{z_{\alpha\beta}\}$ is a basis for M/K.

We show that they are linearly independent. If $\sum_{\alpha,\beta} a_{\alpha\beta} z_{\alpha\beta} = 0$ with finitely many $a_{\alpha\beta} \in K$ non-zero. Then $\sum_\beta (\sum_\alpha a_{\alpha\beta} x_\alpha) y_\beta = 0$, since the y_β are linearly independent over L we have $\sum_\alpha a_{\alpha\beta} x_\alpha = 0$ for all β. Since the x_α are linearly independent over K we have $a_{\alpha\beta} = 0$ for all α, β.

We show spanning. If $z \in M$, then $z = \sum \lambda_\beta y_\beta$ for $\lambda_\beta \in L$. For each $\lambda_\beta = \sum a_{\alpha\beta} x_\alpha$. So $x = \sum_\beta (\sum_\alpha a_{\alpha\beta} x_\alpha) y_\beta = \sum_{\alpha,\beta} a_{\alpha\beta} x_\alpha y_\beta = \sum a_{\alpha\beta} x_{\alpha\beta}$.

So $\{z_{\alpha\beta}\}$ is a basis for M over K, so $[M : K] = [M : L][L : K]$ □

Corollary 2.2. *If $K \subset L \subset M$ are fields with $[M : K] < \infty$ then $[L : K] | [M : K]$.*

Definition. L/K is called *finite* if $[L : K] < \infty$

If K is a field and x is an indeterminate variable, then $K(x)$ denotes the field of rational functions in x with coefficients in K. That is

$$K(x) = \left\{ \frac{f(x)}{g(x)} : f, g \in K[x], g \neq 0 \right\}$$

If L/K is a field extension, $\alpha \in L$. Then $K(\alpha)$ is the subfield of L generated by K and α.

$$K(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} : f, g \in K[x], g(\alpha) \neq 0 \right\} = \bigcap_{K \subset M \subset L, \alpha \in M} M$$

Let L/K be a field extension, $\alpha \in L$. We say that α is *algebraic* over K if there exists a non-zero polynomial $f \in K[x]$ with $f(\alpha) = 0$

Theorem 2.3. *Let L/K be a field extension and $\alpha \in L$. Then α is algebraic over K if and only if $K(\alpha)/K$ is a finite extension.*

Proof. $\Leftarrow$) Let $n = [K(\alpha) : K]$ and consider $1, \alpha, \dots, \alpha^n \in K(\alpha)$. Notice that there are $n + 1$ of them, so they must be linearly dependent since the dimension of the vector space is n. So there exists $a_i \in K$ such that $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$ with a_i not all zero. Hence by definition α is algebraic.

$\Rightarrow$) Assume that there exists $f \neq 0 \in K[x]$ such that $f(\alpha) = 0$, and assume that f has minimal degree n. We claim that $f \in K[x]$ is irreducible.

Suppose that $f = gh$, with g, h non-constant. Then $0 = f(\alpha) = g(\alpha)h(\alpha)$, so without loss of generality $g(\alpha) = 0$, but $\deg(g) < \deg(f)$. This is a contradiction. Let $f = a_n x^n + \cdots + a_0$ with $a_n \neq 0$. Then $f(\alpha) = 0 \Rightarrow a_n\alpha^n + \cdots + a_0 = 0 \Rightarrow \alpha^n = -\frac{1}{a_n}(a_{n-1}\alpha^{n-1} + \cdots + a_0)$. So we can reduce any polynomial expression in α of degree $\geq n$ to one of degree $\leq n - 1$.

Hence $K(\alpha) = \left\{ \frac{b_0 + \cdots + b_{n-1}\alpha^{n-1}}{c_0 + \cdots + c_{n-1}\alpha^{n-1}} : b_i, c_i \in K \right\}$. Pick $\frac{b(\alpha)}{c(\alpha)} \in K(\alpha)$, now $\deg(c) \leq n - 1 < \deg f$ and $c(\alpha) \neq 0$. Hence $\gcd(c, f) = 1$, so there exists $\lambda, \mu \in K[x]$ with $\lambda(x)c(x) + \mu(x)f(x) = 1$. In particular $1 = \lambda(\alpha)c(\alpha) + \mu(\alpha)f(\alpha) = \lambda(\alpha)c(\alpha)$, hence $\lambda(\alpha) = \frac{1}{c(\alpha)} \in K[\alpha]$

Any elements of $K(\alpha)$ is a polynomial in α of degree $\leq n - 1$. So if α is algebraic over K, we have just shown that $K(\alpha) = K[\alpha]$ and $1, \alpha, \dots, \alpha^{n-1}$ is a basis for $K[\alpha]/K$, hence $[K(\alpha) : K] = n$ □

Theorem 2.4. *Let L/K be a field extension, then the set M of all $\alpha \in L$ that are algebraic over K is a subfield of L containing K.*

Proof. First $K \subseteq M$, as $\alpha \in K$ is a root of $x - \alpha \in K[x]$

So take $\alpha, \beta \in M$, we need to show that $\alpha - \beta \in M$ and $\frac{\alpha}{\beta} \in M$ if $\beta \neq 0$. Consider the subfield $K(\alpha, \beta) \subseteq L$. Now $[K(\alpha)(\beta) : K] = [K(\alpha, \beta) : K(\alpha)][K(\alpha) : K]$. We have $[K(\alpha)(\beta) : K(\alpha)] \leq [K(\beta) : K]$ since the first one is the degree of the minimal polynomial of β over $K(\alpha)$, and β is algebraic, so there is $f \in K[x] \subset K[\alpha]$ such that $f(\beta) = 0$. Now $\alpha - \beta \in K(\alpha)(\beta)$ and if $\beta \neq 0$, $\frac{\alpha}{\beta} \in K(\alpha)(\beta)$. This implies that $K(\alpha - \beta) \subseteq K(\alpha, \beta) \Rightarrow [K(\alpha - \beta) : K] | [K(\alpha, \beta) : K] < \infty$ and $K\left(\frac{\alpha}{\beta}\right) \subseteq K(\alpha, \beta) \Rightarrow [K\left(\frac{\alpha}{\beta}\right) : K] | [K(\alpha, \beta) : K] < \infty$. Hence $\alpha - \beta$ and $\frac{\alpha}{\beta}$ are algebraic over K □

Corollary 2.5. *The set of algebraic number is a field. We denote this with $\overline{\mathbb{Q}}$*

For any subfield $K \subset \mathbb{C}$, we let $\overline{K}$ denote the algebraic closure of K in $\mathbb{C}$, i.e., the set of $\alpha \in \mathbb{C}$ that are algebraic over K.

For example $\overline{\mathbb{R}} = \mathbb{C} = \mathbb{R}(i)$.

We also conclude that $\overline{\mathbb{Q}} = \cup_{K \text{ number field}} K$. Also $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$ so $\overline{\mathbb{Q}}$ itself is not a number field.

2.2 Rings and Modules

In this course we use the following convention for rings. Every ring R is assumed to be commutative and has 1. We also allow 1 to be 0, in which case $R = 0 = \{0\}$. A ring homomorphism $\phi : R \to S$ is assumed to send 1_R to 1_S. A subring R of a ring S is assumed to satisfy $1_R = 1_S$

Example. Let R_1 and R_2 be two non-zero rings. Then we have a ring $R = R_1 \times R_2$ with $1_R = (1_{R_1}, 1_{R_2})$. Note that $R_1' = R_1 \times \{0\} \subset R$ is a ring, but $1'_{R_1} = (1, 0) \neq 1_R$ so R_1' is not a subring of R. Finally $\phi : R_1 \to R$ defined by $r \mapsto (r, 0)$ is not a ring homomorphism.

Definition 2.6. Let R be a ring then a *module* over R is an abelian group M with scalar multiplication by R, satisfying

- $1 \cdot m = m$
- $(r + s)m = rm + sm$
- $r(m + n) = rm + rn$
- $(rs)m = r(sm)$

For all $r, s \in R, m, n \in M$

An *homomorphism* of R-modules is a homomorphism of abelian group that satisfies $\phi(rm) = r\phi(m)$ for all $r \in R, m \in M$

Example. If R is a field, then modules are the same as vector spaces.

Any ideal I of R is an R-module

Any quotient R/I is an R-module

If $R \subseteq S$ are both rings, then S is an R-module

Let $R = \mathbb{Z}$. Then any abelian group is a $\mathbb{Z}$-module

Definition 2.7. A module is *free of rank* n if it is isomorphism to R^n.

Theorem 2.8. *If $R \neq 0$, the rank of a free module over R is uniquely determined, i.e., $R^m \cong R^n \Rightarrow m = n$*

Proof. This is not proven in this module □

Definition 2.9. If R is a ring then an R-module M is *finite* if it can be generated by finitely many elements.

Example. $R = \mathbb{Z}, M = \mathbb{Z}[i]$ is finite with generators 1 and i

$R = \mathbb{Z}[2i]$, $M = \mathbb{Z}[i]$. This is also finite with generators 1 and i, but it is not free.

$R = \mathbb{Z}$, $M = \mathbb{Z}\left[\frac{1}{2}\right] = \left\{\frac{n}{2^m} : x \in \mathbb{Z}, m \geq 0\right\} \subseteq \mathbb{Q}$. This is not finite as any finite set has a maximum power of 2 occurring in the denominator.

2.3 Ring Extensions

Definition 2.10. Let R be a ring, then a *ring extension* of R is a ring S that has R as a subring.

A ring extension $R \subset S$ is *finite* if S is finite as an R-module

Let $R \subset S$ be a ring extension, $s \in S$. Then s is said to be *integral* over R if there exists a monic polynomial $f = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in R[x]$ with $f(s) = 0$

Theorem 2.11. *Let $R \subset S$ be a ring extension, $s \in S$. Then the following are equivalent:*

1. *s is integral over R*
2. *$R[s]$ is a finite extension of R*
3. *There exists a ring S' such that $R \subset S' \subset S$, S' is finite over R and $s \in S'$*

Proof. Not proven in this modules. Some of these are obvious. (See Commutative Algebra Theorem 4.2) □

Theorem 2.12. *If $R \subset S$ is a ring extension, then the set S' of $s \in S$ that are integral over R is a ring extension of R inside S.*

Proof. Note that $R \subseteq S'$ since $r \in R$ is a root of $x - r \in R[x]$.

Given $s_1, s_2 \in S'$ we want to prove that $s_1 - s_2, s_1s_2 \in S'$. We have $R \subset R[s_1] \subset R[s_1, s_2] \subset S$, now the first ring extension is finite since s_1 is integral over R. We also have s_2 is integral over R so in particular it is integral over $R[s_1]$. Take the generators for $R[s_1]$ as an R-module: $1, \ldots, s_1^n$ and take the generators for $R[s_1, s_2]$ as an $R[s_1]$-module: $1, \ldots, s_2^m$. Then $\left\{s_1^i s_2^j : 1 \leq j \leq m, 1 \leq i \leq n\right\}$ is a set of generators for $R[s_1, s_2]$ as an R-module. Hence we conclude that $R[s_1, s_2]$ is a finite extension of R. Now $s_1 - s_2, s_1s_2 \in R[s_1, s_2]$. So if we apply the previous theorem, we have $s_1 - s_2, s_1s_2$ are integral over R. □

Definition 2.13. Let $R \subset S$ be an extension of rings, then the ring of R integral elements of S is called the *integral closure* of R in S

Given an extension of rings $R \subset S$ then we say that R is *integrally closed* in S if the integral closure of R in S is R itself

Theorem 2.14. *Let $R \subset S$ be a ring extension and let $R' \subset S$ be the integral closure of R in S. Then R' is integrally closed in S.*

Proof. Take $s \in S$ integral over R'. We want to show that s is integral over R. Take $f = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in R'[x]$ with $f(s) = 0$. Consider a subring of $R \subset R[a_0, a_1, \ldots, a_{n-1}] \subset R'$. Now $R \subset R[a_0] \subset R[a_0, a_1] \subset \cdots \subset R[a_0, \ldots, a_{n-1}]$. Now $f \in R[a_0, \ldots, a_{n-1}][x]$. So s is integral over $R[a_0, \ldots, a_{n-1}]$, hence $R[a_0, \ldots, a_{n-1}][s]$ is finite over $R[a_0, \ldots, a_{n-1}]$ and hence finite over R. So by Theorem 2.12, we have that s is integral over R. □

Definition 2.15. An element $\alpha \in \mathbb{C}$ is an *algebraic integer* if it is integral over $\mathbb{Z}$.

The ring of algebraic integers is denoted by $\overline{\mathbb{Z}}$

If K is a number field, then the *ring of integers* in K is denoted $\mathcal{O}_K = \overline{\mathbb{Z}} \cap K =$ integral closure of $\mathbb{Z}$ in K.

Example. Let $K = \mathbb{Q}$. Take $p/q \in \mathbb{Q}$ integral over $\mathbb{Z}$ (assume that $\gcd(p, q) = 1$), then there exists $f(x) \in \mathbb{Z}[x]$ such that $f(p/q) = 0$. So $x - p/q$ is a factor of f in $\mathbb{Q}[x]$, but Gauss' Lemma states "if $f \in \mathbb{Z}[x]$ is monic and $f = g \cdot h$ with $g, h \in \mathbb{Q}[x]$ then $g, h \in \mathbb{Z}[x]$". So $x - p/q \in \mathbb{Z}[x]$, that is $p/q \in \mathbb{Z}$. So $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.

Consider $K = \mathbb{Q}(\sqrt{d})$, with $d \neq 1$ and d is square free. Consider $\alpha \in K$, $\alpha = a + b\sqrt{d}, a, b \in \mathbb{Q}$ and suppose that α is an algebraic integer. Assume that $\deg(\alpha) = 2$, that is the minimum monic polynomial f of α in $\mathbb{Q}[x]$ has degree 2. Then by Gauss, we know $f \in \mathbb{Z}[z]$, furthermore $f = (x - (a + b\sqrt{d}))(x - (a - b\sqrt{d})) = x^2 - 2ax + a^2 - db$. So we want $2a \in \mathbb{Z}$ and $a^2 - db \in \mathbb{Z}$.

So $2a \in \mathbb{Z} \Rightarrow a = \frac{a'}{2}$ with $a' \in \mathbb{Z}$. Then $a^2 - b^2 d = \left(\frac{a'}{2}\right)^2 - b^2 d = (a')^2 - d(2b)^2 \in 4\mathbb{Z}$. So (using the fact that d is square-free) $d(2b)^2 \in \mathbb{Z} \Rightarrow 2b \in \mathbb{Z}$ and $(a')^2 \equiv d(b')^2 \mod 4$. So we conclude:

- If a' is even, then $a \in \mathbb{Z}$, so b' is even and thus $b \in \mathbb{Z}$
- If a' is odd, then $(a')^2 \equiv 1 \mod 4$, so b' is odd as well and $d \equiv 1 \mod 4$

We have just proven the following:

Theorem 2.16. *Let $d \in \mathbb{Z}$, with $d \neq 1$ and square free. Then* $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \mathbb{Z}[\sqrt{d}] & d \not\equiv 1 \mod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & d \equiv 1 \mod 4 \end{cases}$

Theorem 2.17. *Let R be a UFD. Then R is integrally closed in its fraction field (the converse does not hold)*

Proof. Take $s = \frac{r_1}{r_2}$ integral over R, and assume that r_1, r_2 are coprime (well defined since R is a UFD), we have to show that $r_2 \in R^*$.

If $r_2 \notin R^*$, then let $\pi \in R$ be any factor of r_2. Now s is integral, so there exists a_i and n such that $s^n + a_{n-1}s^{n-1} + \cdots + a_0 = 0$. Multiplying through by r_2^n we have $r_1^n + a_{n-1}r_1^{n-1}r_2 + \cdots + a_0 r_2^n = 0$. Now since $r_2 \equiv 0 \mod \pi$, if we take mod both side we have $r_1^n \equiv 0 \mod \pi$. Hence $\pi | r_1^n \Rightarrow \pi | r_1$. This is a contradiction. $\square$

The converse of this theorem is not true, as an example $\mathcal{O}_{\mathbb{Q}(\sqrt{-5})} = \mathbb{Z}[\sqrt{-5}]$ is integrally closed but not a UFD since $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$

3 Norms, Discriminants and Lattices

3.1 Conjugates, Norms and Traces

The Theorem of Primitive Elements. *Any number field K can be generated by a single elements $\theta \in K$. That is $K = \mathbb{Q}(\theta)$*

Proof. See any courses in Galois Theory $\square$

Consider a number field $K = \mathbb{Q}(\theta)$. This θ has a monic minimal polynomial, say $f_\theta \in \mathbb{Q}[x]$. We can factor f_θ over $\mathbb{C}$, say $f_\theta = (x - \theta_1)(x - \theta_2)\dots(x - \theta_n)$, where $\theta_1 = \theta$ and all the θ_i are distinct. For each i we have a field embedding, which we denote $\sigma_i : K \hookrightarrow \mathbb{C}$ defined by $\theta \mapsto \theta_i$. These are all possible embedding of $K \hookrightarrow \mathbb{C}$

Example. $K = \mathbb{Q}[\sqrt{d}]$, then $f_\theta = x^2 - d = (x - \sqrt{d})(x + \sqrt{d})$. So we have $\sigma_1 = \text{id}$ and $\sigma_2 = a + b\sqrt{d} \mapsto a - b\sqrt{d}$

$K = \mathbb{Q}[\sqrt[3]{2}]$, then $f_\theta = x^3 - 2 = (x - \sqrt[3]{2})(x - \zeta_3\sqrt[3]{2})(x - \zeta_3^2\sqrt[3]{2})$ where $\zeta_3 = e^{\frac{2\pi i}{3}}$ a third root of unity. So we have:

- $\sigma_1 : \sqrt[3]{2} \mapsto \sqrt[3]{2}$ (i.e., the identity map),
- $\sigma_2 : \sqrt[3]{2} \mapsto \zeta_3\sqrt[3]{2}$
- $\sigma_3 : \sqrt[3]{2} \mapsto \zeta_3^2\sqrt[3]{2}$

Definition 3.1. Let K be a number field and $\sigma_1, \dots, \sigma_n$ all the embeddings $K \hookrightarrow \mathbb{C}$. Let $\alpha \in K$. Then the elements $\sigma_i(\alpha)$ are called the *conjugates* of α.

Theorem 3.2. *Let K be a number field, $n = [K : \mathbb{Q}]$. Take $\alpha \in K$, consider the multiplication by α as a linear map from the $\mathbb{Q}$-vector space K to itself. That is $\alpha : K \to K$ is defined by $\beta \mapsto \alpha\beta$. Then the characteristic polynomial of this map is equal to $P_\alpha(x) = \prod_{i=1}^n (x - \sigma_i(\alpha))$*

Proof. Let $K = \mathbb{Q}(\theta)$ and consider the basis: $1, \theta, \theta^2, \dots, \theta^{n-1}$. Let M_α be the matrix that describes the linear map α relative to this basis.

First consider $\alpha = \theta$. Let $f_\theta = x^n + a_{n-1}x^{n-1} + \dots + a_0$. Then we have

$$M_\theta = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & -a_{n-1} \end{pmatrix}$$

We now calculated the characteristic polynomial of M_θ:

$$\det(X \cdot I_n - M_\theta) = \det \begin{pmatrix} x & 0 & \cdots & 0 & a_0 \\ -1 & x & \cdots & 0 & a_1 \\ 0 & -1 & \cdots & 0 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & x + a_{n-1} \end{pmatrix} = \sum a_k x^k$$

Hence the characteristic polynomial of $M_\theta = f_\theta = \prod_{i=1}^n (x - \sigma_i(\theta))$ as required. Hence we know from Linear Algebra that there exists an invertible matrix A such that:

$$M_\theta = A \begin{pmatrix} \sigma_1(\theta) & 0 & \cdots & 0 \\ 0 & \sigma_2(\theta) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \sigma_n(\theta) \end{pmatrix} A^{-1}$$

Now note that $M_{\alpha\pm\beta} = M_\alpha \pm M_\beta$ and $M_{\alpha\beta} = M_\alpha M_\beta$ (basic linear algebra). So if we have a polynomial $g \in \mathbb{Q}[x]$, then $M_{g\alpha} = g(M_\alpha)$. Now we can write any $\alpha \in K$ as $g(\theta)$ for some $g \in \mathbb{Q}[X]$. Hence we have

$$\begin{aligned}
M_\alpha = g(M_\theta) &= A \begin{pmatrix} g(\sigma_1(\theta)) & 0 & \cdots & 0 \\ 0 & g(\sigma_2(\theta)) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & g(\sigma_n(\theta)) \end{pmatrix} A^{-1} \\
&= A \begin{pmatrix} \sigma_1(g(\theta)) & 0 & \cdots & 0 \\ 0 & \sigma_2(g(\theta)) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \sigma_n(g(\theta)) \end{pmatrix} A^{-1} \\
&= A \begin{pmatrix} \sigma_1(\alpha) & 0 & \cdots & 0 \\ 0 & \sigma_2(\alpha) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \sigma_n(\alpha) \end{pmatrix} A^{-1}
\end{aligned}$$

Hence, the characteristic polynomial of M_α is $\prod_{i=1}^n (x - \sigma_i(\alpha))$ as required. □

Corollary 3.3. *For $\alpha \in K$, the coefficients of $\prod_{i=1}^n (x - \sigma_i(\alpha))$ are in $\mathbb{Q}$.*

Definition 3.4. Let K be a number field, $\alpha \in K$. We define the *norm* of α as $N(\alpha) = N_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^n \sigma_i(\alpha) \in \mathbb{Q}$.

Corollary 3.5. $N(\alpha) = \det(\cdot\alpha) = \det(M_\alpha)$

We can see that the norm is a multiplicative function, i.e., $N(\alpha\beta) = N(\alpha)N(\beta)$.

Definition 3.6. Let K be a number field and $\alpha \in K$. We define the *trace* of α as $\mathrm{Tr}(\alpha) = \mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \sum_{i=1}^n \sigma_i(\alpha) \in \mathbb{Q}$.

Corollary 3.7. $\mathrm{Tr}(\alpha) = \mathrm{Tr}(\cdot\alpha) = \mathrm{Tr}(M_\alpha)$

We can see that the trace is an additive function, i.e, $\mathrm{Tr}(\alpha + \beta) = \mathrm{Tr}(\alpha) + \mathrm{Tr}(\beta)$.

Example. Let $K = \mathbb{Q}(\sqrt{d})$. Then we have:

- $\mathrm{Tr}(a + b\sqrt{d}) = (a + b\sqrt{d}) + (a - b\sqrt{d}) = 2a$
- $N(a + b\sqrt{d}) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2$

Let $K = \mathbb{Q}(\sqrt[3]{2})$ and recall that $x^3 - 2 = (x - \sqrt[3]{2})(x - \zeta_3\sqrt[3]{2})(x - \zeta_3^2\sqrt[3]{2})$ where $\zeta_3 = e^{\frac{2\pi i}{3}}$ a third root of unity. Then we have:

- $\mathrm{Tr}(a + b\sqrt[3]{2} + c\sqrt[3]{4}) = 3a + b\sqrt[3]{2}(1 + \zeta_3 + \zeta_3^2) + c\sqrt[3]{4}(1 + \zeta_3 + \zeta_3^2) = 3a$
- $N(a + b\sqrt[3]{2} + c\sqrt[3]{4}) = (a + b\sqrt[3]{2} + c\sqrt[3]{4})(a + b\zeta_3\sqrt[3]{2} + c\zeta_3^2\sqrt[3]{4})(a + b\zeta_3^2\sqrt[3]{2} + c\zeta_3\sqrt[3]{4}) = a^3 + 2b^2 + 4c^3 + 6abc$

3.2 Discriminant

Definition 3.8. Let K be a number field and $\alpha_1, \ldots, \alpha_n$ be a basis for K. Let $\sigma_1, \ldots, \sigma_n : K \to \mathbb{C}$ be all the embeddings. The *discriminant* of $(\alpha_1, \ldots, \alpha_n)$ is defined as

$$\left(\det \begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \cdots & \sigma_2(\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \cdots & \sigma_n(\alpha_n) \end{pmatrix}\right)^2$$

We denote this by $\Delta(\alpha_1, \ldots, \alpha_n)$ or by $\mathrm{disc}(\alpha_1, \ldots, \alpha_n)$

Theorem 3.9. *We have*

$$\Delta(\alpha_1,\dots,\alpha_n) = \det\begin{pmatrix} \mathrm{Tr}(\alpha_1\alpha_1) & \mathrm{Tr}(\alpha_1\alpha_2) & \cdots & \mathrm{Tr}(\alpha_1\alpha_n) \\ \mathrm{Tr}(\alpha_2\alpha_1) & \mathrm{Tr}(\alpha_2\alpha_2) & \cdots & \mathrm{Tr}(\alpha_2\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{Tr}(\alpha_n\alpha_1) & \mathrm{Tr}(\alpha_n\alpha_2) & \cdots & \mathrm{Tr}(\alpha_n\alpha_n) \end{pmatrix}$$

Proof. Let $M = (\sigma_i(\alpha_j))_{ij}$. Then we have $\Delta(\alpha_1,\dots,\alpha_n) = \det(M)^2 = \det(M^2) = \det(M^TM)$. But note that the entries of M^TM at (i,j) is $\sum_{k=1}^n \sigma_k(\alpha_i)\cdot\sigma_k(\alpha_j) = \sum_{k=1}^n \sigma_k(\alpha_i\alpha_j) = \mathrm{Tr}(\alpha_i\alpha_j)$. □

Corollary 3.10. *We have* $\Delta(\alpha_1,\dots,\alpha_n) \in \mathbb{Q}$

Theorem 3.11. *We have* $\Delta(\alpha_1,\dots,\alpha_n) \neq 0$

Proof. Suppose that $\Delta(\alpha_1,\dots,\alpha_n) = 0$. Then there exists not all zero $c_1,\dots,c_n \in \mathbb{Q}$ with $c_1\begin{pmatrix}\mathrm{Tr}(\alpha_1\alpha_1)\\ \vdots \\ \mathrm{Tr}(\alpha_n\alpha_1)\end{pmatrix} + \cdots + c_n\begin{pmatrix}\mathrm{Tr}(\alpha_n\alpha_1)\\ \vdots \\ \mathrm{Tr}(\alpha_n\alpha_n)\end{pmatrix} = 0$. Hence $\begin{pmatrix}\mathrm{Tr}(\alpha_1\sum c_j\alpha_j)\\ \vdots \\ \mathrm{Tr}(\alpha_n\sum c_j\alpha_j)\end{pmatrix} = 0$. Put $\alpha = \sum c_j\alpha_j$, we have just shown that $\mathrm{Tr}(\alpha_i\alpha) = 0\,\forall i$. But we have that α_i forms a basis for K over $\mathbb{Q}$, hence $\mathrm{Tr}(\beta\alpha) = 0\,\forall\beta\in K$. We have $\alpha \neq 0$, so let $\beta = \alpha^{-1}$, then $\mathrm{Tr}(\beta\alpha) = \mathrm{Tr}(1) = n = [K:\mathbb{Q}]$ which is a contradiction. □

Definition 3.12. The map $K\times K \to \mathbb{Q}$ defined by $(\alpha,\beta)\mapsto \mathrm{Tr}(\alpha\beta)$ is know as the *trace pairing* on K. It is bilinear.

Let $K = \mathbb{Q}(\theta)$, this has basis $1,\dots,\theta^{n-1}$. In general $\det\begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1}\end{pmatrix}$ is called a *Vandemonde determinant* and it is equal to $\prod_{1\le i<j\le n}(x_j - x_i)$. (See Linear Algebra or Algebra I for a proof by induction). So in our case, $\Delta(1,\theta,\dots,\theta^{n-1}) = \prod_{1\le i<j\le n}(\sigma_i(\theta)-\sigma_j(\theta))^2$. Also note that $\Delta(f_\theta) := \Delta(1,\theta,\dots,\theta^{n-1})$. (Generally, if $f = (x-\alpha_1)\dots(x-\alpha_n)$ then $\Delta(f) := \prod_{1\le i<j\le n}(\alpha_i-\alpha_j)^2$, check with the definition of a discriminant of a quadratic)

Example. Let $K = \mathbb{Q}(\sqrt{d})$. Consider the basis $1, \sqrt{d}$. We calculate the discriminant in two ways:

- $\Delta(1,\sqrt{d}) = \det\begin{pmatrix}1 & \sqrt{d}\\ 1 & -\sqrt{d}\end{pmatrix}^2 = (-2\sqrt{d})^2 = 4d$
- $\Delta(1,\sqrt{d}) = \det\begin{pmatrix}\mathrm{Tr}(1) & \mathrm{Tr}(\sqrt{d})\\ \mathrm{Tr}(\sqrt{d}) & \mathrm{Tr}(d)\end{pmatrix} = \det\begin{pmatrix}2 & 0\\ 0 & 2d\end{pmatrix} = 4d$

Now consider the basis $1, \frac{1+\sqrt{d}}{2}$. Then $\Delta(1,\frac{1+\sqrt{d}}{2}) = (-\sqrt{d})^2 = d$

Let $K = \mathbb{Q}(\sqrt[3]{d})$, with basis $1, \sqrt[3]{d}, \sqrt[3]{d^2}$.Then we have

$$\begin{aligned}\Delta(1,\sqrt[3]{d},\sqrt[3]{d^2}) &= \det\begin{pmatrix}\mathrm{Tr}(1) & \mathrm{Tr}(\sqrt[3]{d}) & \mathrm{Tr}(\sqrt[3]{d^2})\\ \mathrm{Tr}(\sqrt[3]{d}) & \mathrm{Tr}(\sqrt[3]{d^2}) & \mathrm{Tr}(d)\\ \mathrm{Tr}(\sqrt[3]{d^2}) & \mathrm{Tr}(d) & \mathrm{Tr}(\sqrt[3]{d})\end{pmatrix}\\ &= \det\begin{pmatrix}3 & 0 & 0\\ 0 & 0 & 3d\\ 0 & 3d & 0\end{pmatrix}\\ &= -27d^2\end{aligned}$$

3.3 Lattices

Definition 3.13. Let K be a number field. A *lattice* Λ in K is a subgroup generated by $\mathbb{Q}$-linearly independent elements of K. That is $\Lambda = \{n_1\alpha_1 + \cdots + n_r\alpha_r | n_i \in \mathbb{Z}\}$ where α_i are linearly independent over $\mathbb{Q}$. We always have $r \leq [K : \mathbb{Q}]$. The number r is called the *rank* of the lattice, this is sometimes denoted $\mathrm{rk}(\Lambda)$.

Example. $\mathbb{Z}[i]$ is a lattice in $\mathbb{Q}(i)$

Theorem 3.14. *Any finitely generated subgroup of a number field K is a latice.*

Proof. Let Λ be a finitely generated subgroup of K. By the Fundamental Theorem of Finitely Generated Abelian Group, we have $\Lambda \cong T \oplus \mathbb{Z}^r$, where T is the torsion. As K is a $\mathbb{Q}$-vector space, we have $T = 0$, so $\Lambda \cong \mathbb{Z}^r$. Let $\phi : \mathbb{Z}^r \to \Lambda$ be an isomorphism.

Claim: $\alpha_i = \phi(e_i)$ is a basis (i.e., linearly independent generating set) for Λ, where e_i is the standard basis for $\mathbb{Z}^r$. Now $\phi(c_1, \ldots, c_r) = \sum_{i=1}^n c_i\alpha_i$. Since ϕ is surjective, all elements of Λ are reached. If $\sum c_i\alpha_i = 0$ for $c_i \in \mathbb{Q}$ multiply c_i by the common denominator, then without loss of generality, we can assume $c_i \in \mathbb{Z}$. But we know that ϕ is injective, so for all i, $c_i = 0$. $\square$

Definition 3.15. A lattice of K is said to be *full rank* if its rank $r = [K : \mathbb{Q}]$

Theorem 3.16. *Let $\Lambda \subseteq K$ be a full rank lattice. Then $\Delta(\alpha_1, \ldots, \alpha_r)$ is the same for every basis $\alpha_1, \ldots, \alpha_r$ of Λ*

Proof. Suppose $(\alpha_i)_i$ and $(\beta_i)_i$ are basis for Λ. Then each β_i can be written as a linear combination of α_j with coefficients in $\mathbb{Z}$, i.e. $\begin{pmatrix}\beta_1\\ \vdots\\ \beta_r\end{pmatrix} = A\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_r\end{pmatrix}$ with A an $r \times r$ matrix with coefficients in $\mathbb{Z}$. Similarly $\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_r\end{pmatrix} = B\begin{pmatrix}\beta_1\\ \vdots\\ \beta_r\end{pmatrix}$. Hence we have $AB = I_r$, so $A \in \mathrm{GL}_r(\mathbb{Z})$, so $\det(A) = \pm 1$. Put $S = \begin{pmatrix}\mathrm{Tr}(\alpha_1\alpha_1) & \cdots & \mathrm{Tr}(\alpha_1\alpha_r)\\ \vdots & \ddots & \vdots\\ \mathrm{Tr}(\alpha_r\alpha_1) & \cdots & \mathrm{Tr}(\alpha_r\alpha_r)\end{pmatrix}$. Then $\begin{pmatrix}\mathrm{Tr}(\beta_1\beta_1) & \cdots & \mathrm{Tr}(\beta_1\beta_r)\\ \vdots & \ddots & \vdots\\ \mathrm{Tr}(\beta_r\beta_1) & \cdots & \mathrm{Tr}(\beta_r\beta_r)\end{pmatrix} = A^TSA$. (Base change for matrices describing symmetric bilinear forms, see Algebra I)

So we have $\Delta(\beta_1, \ldots, \beta_r) = \det(A^TSA) = \det(A^2)\det(S) = \det(S) = \Delta(\alpha_1, \ldots, \alpha_r)$ $\square$

Definition 3.17. Let $\Lambda \subset K$ be a full rank lattice, then we define $\Delta(\Lambda)$ to be the discriminant of any basis of Λ.

Theorem 3.18. *Let K be a number field and $\Lambda \subset K$ be a full rank lattice with $\Lambda \subset \mathcal{O}_K$. Then $\Delta(\Lambda) \in \mathbb{Z}$.*

Proof. We have $\Delta(\Lambda) = \det((\mathrm{Tr}(\alpha_i\alpha_j)_{ij})$ with $\alpha_i \in \mathcal{O}_K$. If $\alpha \in \mathcal{O}_K$, then $\mathrm{Tr}(\alpha) = \sum_{i=1}^n \sigma_i(\alpha) \in \overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$. Hence $\Delta(\Lambda) \in \mathbb{Z}$. $\square$

Theorem 3.19. *Let K be a number field and $\Lambda \subset \Lambda'$ be two full rank lattices. Then the index $(\Lambda' : \Lambda)$ is finite and $\Delta(\Lambda) = (\Lambda' : \Lambda)^2\Delta(\Lambda')$*

Proof. All the elements of Λ can be written as an integral linear combination of some chosen basis of Λ'. So there exists $A \in M_n(\mathbb{Z})$ with $\Lambda = A\Lambda'$. Consider $\Lambda'/\Lambda \cong \mathbb{Z}^n/A\mathbb{Z}^n$, this is a finitely generated abelian group so by FTFGAG $\Lambda'/\Lambda \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_m\mathbb{Z} \oplus \mathbb{Z}^r$ with $d_1|d_2|\ldots|d_m$. So (by Smith Normal Form from Algebra I) there exists $B, B' \in \mathrm{GL}_n(\mathbb{Z})$ with $BAB' = \begin{pmatrix}d_1 & 0 & \cdots & 0\\ 0 & d_2 & & \\ \vdots & & \ddots & \\ 0 & & & d_n\end{pmatrix}$. As we have $\mathrm{rk}(\Lambda') = \mathrm{rk}(\Lambda)$, we have that $r = 0$, and thus $\det(A) = d_1 \ldots d_m = |\mathbb{Z}^n/A\mathbb{Z}^n| = (\Lambda' : \Lambda)$.

Furthermore $\Delta(\Lambda) = \Delta(A\Lambda') = (\det A)^2\Delta(\Lambda')$. $\square$

Theorem 3.20. *Let K be a number field with $n = [K : \mathbb{Q}]$. Then there exists a basis $\omega_1, \ldots, \omega_n$ of $K/\mathbb{Q}$ such that $\mathcal{O}_K = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n = \{\sum a_i\omega_i | a_i \in \mathbb{Z}\}$. (That is $\mathcal{O}_K$ is a full rank lattice in K)*

Proof. We consider all $\Lambda \subset \mathcal{O}_K$ that are full rank lattices in K.

The first question is: do such Λ exists? Write $K = \mathbb{Q}(\theta)$, $\theta \in K$ and $f_\theta = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ with $a_i \in \mathbb{Q}$. Now let d be a common denominator of the a_i, then $d\theta \in \mathcal{O}_K$. Also note that $\mathbb{Q}(\theta) = \mathbb{Q}(d\theta)$, so without loss of generality we can assume $\theta \in \mathcal{O}_K$. Then $\mathbb{Z}[\theta] \subseteq \mathcal{O}_K$, furthermore $1, \theta, \ldots, \theta^{n-1}$ are linearly independent over $\mathbb{Z}$, hence $\mathbb{Z}[\theta]$ is a full rank lattice.

Of all such Λ, we have that $\Delta(\Lambda) \in \mathbb{Z}$ (by Theorem 3.18). So consider Λ with $|\Delta(\Lambda)|$ minimal. Claim: $\Lambda = \mathcal{O}_K$.

Suppose $\Lambda \neq \mathcal{O}_K$. We do have $\Lambda \subset \mathcal{O}_K$, so take $\alpha \in \mathcal{O}_K \setminus \Lambda$. Then $\Lambda' := \Lambda + \mathbb{Z}\alpha$ is finitely generated as an abelian group of K and thus Λ' is a lattice of full rank. Also $\Lambda' \subset \mathcal{O}_K$. But we have $|\Delta(\Lambda)| = (\Lambda' : \Lambda)^2 |\Delta(\Lambda)|$, and since $\Lambda \neq \Lambda'$, we find $|\Delta(\Lambda)| > |\Delta(\Lambda')|$, which is a contradiction. $\square$

Definition 3.21. The *discriminant of a number field* $K/\mathbb{Q}$ is defined as $\Delta(K/\mathbb{Q}) = \Delta(\mathcal{O}_K)$

Example. Let $K = \mathbb{Q}(\sqrt{d})$ with $d \neq 1$ and square free. Then $\Delta(K/\mathbb{Q}) = \Delta(\mathcal{O}_K) = \begin{cases} 4d & d \not\equiv 1 \mod 4 \\ d & d \equiv 1 \mod 4 \end{cases}$

Note that if $\Lambda \subset \mathcal{O}_K$ is a full rank sublattice, then $\Delta(\Lambda) = (\mathcal{O}_K : \Lambda)^2 \Delta(\mathcal{O}_K)$ by Theorem 3.19

Corollary 3.22. *If $\Lambda \subset \mathcal{O}_K$ and $\Delta(\Lambda)$ is square free then $\Lambda = \mathcal{O}_K$.*

4 Cyclotomic Fields

Definition 4.1. Let n be a positive integer. Then the *n-cyclotomic* field is $\mathbb{Q}(\zeta_n)$ where $\zeta_n = e^{\frac{2\pi i}{n}}$

For simplicity we are going to assume that $n = p^r$ with p being a prime.

Theorem 4.2. *The minimal polynomial of ζ_{p^r} is*

$$\Phi_{p^r} = \prod_{k=1, p\nmid k}^{p^r} (x - \zeta_{p^r}^k)$$

Proof. Firs note that $\Phi_{p^r}(\zeta_{p^r}) = 0$

In general, $\prod_{k=1}^{n}(x - \zeta_n^k) = x^n - 1$. We see this by noticing that every zero of the LHS is a zero of the RHS, the degree of both sides are the same and they both have the same leading coefficients. Consider

$$\Phi_{p^r} = \prod_{k=1, p\nmid k}^{p^r} (x - \zeta_{p^r}^k) = \frac{\prod_{k=1}^{p^r}(x - \zeta_{p^r}^k)}{\prod_{k=1}^{p^{r-1}}(x - \zeta_{p^r}^{pk})}$$

and notice that $\zeta_{p^r}^p = \zeta_{p^{r-1}}$. This means we can rewrite

$$\Phi_{p^r} = \frac{\prod_{k=1}^{p^r}(x - \zeta_{p^r}^k)}{\prod_{k=1}^{p^{r-1}}(x - \zeta_{p^{r-1}}^k)} = \frac{x^{p^r} - 1}{x^{p^{r-1}} - 1} = x^{(p-1)p^{r-1}} + x^{(p-2)p^{r-1}} + \cdots + 1$$

Hence we have $\Phi_{p^r} \in \mathbb{Z}[x]$.

We finally show that Φ_{p^r} is irreducible. Suppose that $\Phi_{p^r} = fg$ with $f, g \in \mathbb{Z}[x]$, f, g are both monic and non constant. Consider this $\mod p$, we have

$$\Phi_{p^r} = \frac{x^{p^r} - 1}{x^{p^{r-1}} - 1} \equiv \frac{(x-1)^{p^r}}{(x-1)^{p^{r-1}}} \equiv (x-1)^{(p-1)(p^{r-1})} \mod p$$

(using Fermat's Little Theorem). Let $\overline{f}, \overline{g}$ denoted the reduction of $f, g \mod p$, hence we have $\overline{f}\overline{g} = (x-1)^{(p-1)p^{r-1}} \mod p$. Now $\mathbb{F}_p$ is a UFD, so we have $\overline{f} = (x-1)^m$ and $\overline{g} = (x-1)^k$ such that $m + k = (p-1)p^{r-1}$. Hence we have $f = (x-1)^m + pF$ and $g = (x-1)^k + pG$ for some $F, G \in \mathbb{Z}[x]$, that is, $fg = (x-1)^{m+k} + p(x-1)^k F + p(x-1)^m G + p^2 FG$.

Now consider $x = 1$, we get $f(1)g(1) = p^2 F(1)G(1)$ on one hand and $\Phi_{p^r}(1) = 1^{(p-1)p^{r-1}} + \cdots + 1 = p$ on the other hand. But $p^2 \nmid p$, so we have a contradiction and Φ_{p^r} is irreducible. $\square$

Note that $\mathbb{Z}[\zeta_{p^r}] \subset \mathcal{O}_{\mathbb{Q}(\zeta_{p^r})}$.

Problem. What is $\Delta(\mathbb{Z}[\zeta_{p^r}])$?

Let us denote ζ_{p^r} by ζ. By definition we have

$$|\Delta(\mathbb{Z}[\zeta])| = \left| \prod_{k=1, p\nmid k}^{p^r} \prod_{m=1, p\nmid m, m\neq k}^{p^r} (\zeta^k - \zeta^m) \right|$$

Let us fix k, we want to compute $\prod_{m=1, p\nmid m, m\neq k}^{p^r}(\zeta^k - \zeta^m)$. We do this by considering

$$F_k = \prod_{m=1, p\nmid m, m\neq k}^{p^r} (x - \zeta^m) = \frac{\Phi_{p^r}(x)}{x - \zeta^k} = \frac{x^{p^r} - 1}{(x^{p^{r-1}} - 1)(x - \zeta^k)}$$

Now $F_k(\zeta^k) = \frac{0}{0}$, so we need to use l'Hospital's rule. We calculate

$$\Phi_{p^r}'(x) = \frac{p^r x^{p^r - 1}(x^{p^{r-1}} - 1) - p^{r-1} x^{p^{r-1} - 1}(x^{p^r} - 1)}{(x^{p^{r-1}} - 1)^2}$$

Now the roots of $x^{p^{r-1}} - 1$ are powers of $\zeta_{p^{r-1}} = \zeta^p$, so ζ^k is not a root of $(x^{p^{r-1}} - 1)$. Hence

$$F_k(\zeta^k) = \Phi_{p^r}'(\zeta^k) = \frac{p^r \zeta^{k(p^r - 1)}}{\zeta^{kp^{r-1}} - 1}$$

Hence $|\Phi'_{p^r}(\zeta_k)| = \frac{p^r}{|\zeta^{kp^{r-1}}-1|}$, so we have

$$|\Delta(\mathbb{Z}[\zeta]) = \prod_{k=1,p\nmid k}^{p^r} \frac{p^r}{|\zeta^{kp^{r-1}}-1|} = \frac{p^{r(p^r-p^{r-1})}}{\prod |\zeta^{kp^{r-1}}-1|}$$

Hence we finally compute

$$\prod_{k=1,p\nmid k}^{p^r} (x-\zeta^{kp^{r-1}}) = \prod_{k=1,p\nmid k}^{p^r} (x-\zeta_p^k) = \left(\prod_{k=1}^{p-1}(x-\zeta_p^k)\right)^{p^{r-1}} = (\Phi_p(x))^{p^{r-1}}$$

Plucking in $x=1$, we get $\Phi_p(x)^{p^{r-1}} = p^{p^{r-1}}$. Hence we conclude $|\Delta(\mathbb{Z}[\zeta])| = p^{rp^r-rp^{r-1}-p^{r-1}} = p^{p^{r-1}(rp-r-1)}$

Now it is not important to remember what exactly it is, the key idea is that it is a power of p, the exact exponent does not matter.

In particular if $r=1$ we get $|\Delta(\mathbb{Z}[\zeta_p])| = p^{p-2}$

Theorem 4.3. *For any n we have $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$.*

Proof. We will only prove this for $n=p$, with p prime.

We already know that $\mathbb{Z}[\zeta_p] \subset \mathcal{O}_{\mathbb{Q}(\zeta_p)}$. We also know that $p^{p-2} = \Delta(\mathbb{Z}[\zeta_p]) = \left(\mathcal{O}_{\mathbb{Q}(\zeta_p)} : \mathbb{Z}[\zeta_p]\right)^2 \Delta(\mathcal{O}_{\mathbb{Q}(\zeta_p)})$ (by Theorem 3.19).

Suppose that $\mathbb{Z}[\zeta_p] \neq \mathcal{O}_{\mathbb{Q}(\zeta_p)}$ then $(\mathcal{O}_{\mathbb{Q}(\zeta_p)} : \mathbb{Z}[\zeta_p]) = p^*$, where $*$ is an unknown exponent. Then $\mathcal{O}_{\mathbb{Q}(\zeta_p)}/\mathbb{Z}[\zeta_p]$ is an abelian group of order divisible by p. Hence there exists $\overline{\alpha} \in \mathcal{O}_{\mathbb{Q}(\zeta_p)}/\mathbb{Z}[\zeta_p]$ with order p, i.e., there exists $\alpha \in \mathcal{O}_{\mathbb{Q}(\zeta_p)}$ with $p\alpha \in \mathbb{Z}[\zeta_p]$. We want to show that for any $\alpha \in \mathcal{O}_{\mathbb{Q}(\zeta_p)}$ such that $p\alpha \in \mathbb{Z}[\zeta_p]$ then we already have $\alpha \in \mathbb{Z}[\zeta_p]$.

Note that $\mathbb{Z}[\zeta_p] = \mathbb{Z}[1-\zeta_p]$. Now $N(1-\zeta_p) = \prod_{i=1}^{p-1}\sigma_i(1-\zeta_p) = \prod_{i=1}^{p-1}(1-\zeta_p^i) = \Phi_p(1) = p$. Hence we have that p factors as $\prod_{i=1}^{p-1}(1-\zeta_p^i)$. Now for all i, we have $N(1-\zeta_p^i) = \prod_{j=1}^{p-1}(1-\sigma_j(\zeta_p^i)) = \prod_{j=1}^{p-1}(1-\zeta_p^{ij}) = N(1-\zeta_p) = p$, hence in particular we have $N\left(\frac{1-\zeta_p^i}{1-\zeta_p}\right) = 1$, so $\frac{1-\zeta_p^i}{1-\zeta_p}$ is a unit for all i. Putting all of this together we have $p = \frac{\prod(1-\zeta_p^i)}{(1-\zeta_p)^{p-1}}(1-\zeta_p)^{p-1} = \text{unit}\cdot(1-\zeta_p)^{p-1}$.

We can write $p\alpha$ as $a_0 + a_1(1-\zeta_p) + \cdots + a_{p-2}(1-\zeta_p)^{p-2}$ $(*)$ with $a_i \in \mathbb{Z}$. We want to show that $p|a_i$ for all i. For $a \in \mathbb{Z}$ we have $p|a$ if and only if $(1-\zeta_p)|a$ in $\mathcal{O}_{\mathbb{Q}(\zeta_p)}$. One direction follows from the fact that $1-\zeta_p|p$. For the other implication, suppose $(1-\zeta_p)|a$, then $N(1-\zeta_p)|N(a) \Rightarrow p|a^{p-1}$, hence $p|a$. (Note for any number field and $a \in \mathbb{Q}$, we have $N(a) = a^{[K:\mathbb{Q}]}$). We have now the tools to do a prove by induction to show that a_n is divisible by p.

Let $n=0$ and consider $(*)$ module $1-\zeta_p$. We have $p\alpha \equiv 0 \mod (1-\zeta_p)$, also for $i \geq 1$ we have $a_i(1-\zeta_p) \equiv 0 \mod (1-\zeta_p)$. Hence we find that $a_0 \equiv 0 \mod (1-\zeta_p)$, so $(1-\zeta_p)|a_0$ and hence $p|a_0$

Now suppose that $p|a_0, a_1, \ldots, a_{n-1}$ and that $n \leq p-2$. We have that $p\alpha$ is divisible by $(1-\zeta_p)^{n+1}$, but so is a_0, $(1-\zeta_p)a_1, \ldots, (1-\zeta_p)^{n-1}a_{n-1}$ and $a_i(1-\zeta_p)^i$ for $i > n$. Hence we have $(1-\zeta_p)^n a_i \equiv 0 \mod (1-\zeta_p)^{n+1}$. Hence there exists $\beta \in \mathcal{O}_{\mathbb{Q}(\zeta_p)}$ with $\beta(1-\zeta_p)^{n+1} = (1-\zeta_p)^n a_n \Rightarrow \beta(1-\zeta_p) = a_n$, so we have $(1-\zeta_p)|a_n$.

Hence we have shown by induction that $p|a_i\, \forall i$. Hence $p\alpha \in p\mathbb{Z}[\zeta_p] \Rightarrow \alpha \in \mathbb{Z}[\zeta_p]$. So to recap, we have shown if $\mathbb{Z}[\zeta_p] \neq \mathcal{O}_{\mathbb{Q}(\zeta_p)}$, then we must have $\alpha \in \mathcal{O}_{\mathbb{Q}(\zeta_p)} \setminus \mathbb{Z}[\zeta_p]$ such that $p\alpha \in \mathbb{Z}[\zeta_p]$. But we also shown that if $\alpha \in \mathcal{O}_{\mathbb{Q}(\zeta_p)}$ with $p\alpha \in \mathbb{Z}[\zeta_p]$ then $\alpha \in \mathbb{Z}[\zeta_p]$, hence we have a contradiction. ☐

Example (Of the proof in action)**.** . What is $\mathcal{O}_{\mathbb{Q}(\sqrt[3]{2})}$? We know that $\mathbb{Z}[\sqrt[3]{2}] \subset \mathcal{O}_{\mathbb{Q}(\sqrt[3]{2})}$, we also know that $\Delta(\mathbb{Z}[\sqrt[3]{2}]) = -27(2^2) = -2^2\cdot 3^3 = (\mathcal{O}_{\mathbb{Q}(\sqrt[3]{2})} : \mathbb{Z}[\sqrt[3]{2}])^2 \cdot \Delta(\mathcal{O}_{\mathbb{Q}(\sqrt[3]{2})})$. Hence if $\mathbb{Z}[\sqrt[3]{2}] \neq \mathcal{O}_{\mathbb{Q}(\sqrt[3]{2})}$, then either 2 divides the index or 3 divides the index.

Suppose that 2 divides the index. Then there exists $\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt[3]{2})} \setminus \mathbb{Z}[\sqrt[3]{2}]$ with $2\alpha \in \mathbb{Z}[\sqrt[3]{2}]$. Note that in $\mathcal{O}_{\mathbb{Q}(\sqrt[3]{2})}$ we have $2 = \sqrt[3]{2}^3$. For $a \in \mathbb{Z}$ we have $2|a$ if and only if $\sqrt[3]{2}|a$ in $\mathcal{O}_{\mathbb{Q}(\sqrt[3]{2})}$. Let $2\alpha = a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{4}$. Consider this modulo $\sqrt[3]{2}$, we have $0 \equiv a_0 \mod \sqrt[3]{2}$. Hence $2|a_0$. Now considering this modulo $\sqrt[3]{4}$, we have $0 \equiv a_1\sqrt[3]{2} \mod \sqrt[3]{4}$, again implying that $\sqrt[3]{2}|a_1$, hence $2|a_1$. So finally considering this modulo 2, we see that $2|a_2$. Hence $2\alpha \in 2\mathbb{Z}[\sqrt[3]{2}]$, i.e., $\alpha \in \mathbb{Z}[\sqrt[3]{2}]$. So 2 does not divide the index

Now suppose that 3 divides the index. We claim that $3 = (1+\sqrt[3]{2})^3\cdot$unit. Now $(1+\sqrt[3]{2})^3 = 1+2\sqrt[3]{2}+3\sqrt[3]{4}+2 = 3(1+\sqrt[3]{2}+\sqrt[3]{4})$. Now $N(1+\sqrt[3]{2}) = 1^2 + 2\cdot 1^2 = 3$, so $N((1+\sqrt[3]{2})^3) = 3^3 = N(3)$ and hence $(1+\sqrt[3]{2}+\sqrt[3]{4})$ is a unit, proving our claim. Hence we have that for $\alpha \in \mathbb{Z}$, $3|\alpha$ if and only if $(1+\sqrt[3]{2})|\alpha$ in $\mathcal{O}_{\mathbb{Q}(\sqrt[3]{2})}$. So consider $\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt[3]{2})} \setminus \mathbb{Z}[\sqrt[3]{2}]$ such that $3\alpha \in \mathbb{Z}[\sqrt[3]{2}]$ and write $3\alpha = a_0 + a_1(1+\sqrt[3]{2}) + a_2(1+\sqrt[3]{2})^2$ (by changing the basis of

$\mathbb{Z}[\sqrt[3]{2}]$ to $\mathbb{Z}[1+\sqrt[3]{2}]$). Then if we consider the equation modulo successive powers of $(1+\sqrt[3]{2})$, we find that each a_i is divisible by $(1+\sqrt[3]{2})$ and thus by 3. Again this leads to a contradiction.

Hence we have that $\mathbb{Z}[\sqrt[3]{2}] = \mathcal{O}_{\mathbb{Q}(\sqrt[3]{2})}$

5 Dedekind Domains

5.1 Euclidean domains

Definition 5.1. Let R be a domain (that is $0 \neq 1$ and there are no non-trivial solutions to $ab = 0$). An *Euclidean function* on R is a function $\phi : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ such that for all $a, b \in R$ with $b \neq 0$, there exists $q, r \in R$ with $a = qb + r$ and either $r = 0$ or $\phi(r) < \phi(b)$

Example. $R = \mathbb{Z}$, and $\phi(n) = |n|$.
$R = k[x]$ where k is any field and $\phi(f(x)) = \deg(f)$
$R = \mathbb{Z}[i]$ and $\phi(\alpha) = N(\alpha)$

Definition 5.2. A domain on which there is an Euclidean function is called an *Euclidean domain.*

Theorem 5.3. *If R is an Euclidean domain then R is a principal ideal domain (PID), i.e., every ideal of R can be generated by one element*

Proof. Let $I \neq 0$ be a non-zero ideal of R. Take $0 \neq b \in I$ to be an element for which $\phi(b)$ is minimal. We claim that $I = (b)$

Let $a \in I \setminus \{0\}$ be another element. Then there exists $q \in R$ with $a - qb$ either 0 or $\phi(a - qb) < \phi(b)$. As b is an element with $\phi(b)$ minimal, we have that $a - qb$ is 0, hence $a = qb$, i.e., $a \in (b)$ □

Lemma 5.4. *If R is a PID and $\pi \in R$ an irreducible element, then for $a, b \in R$ we have $\pi | ab \Rightarrow \pi | a$ or $\pi | b$*

Proof. Suppose that $\pi \nmid a$, we want to show that $\pi | b$. Consider the ideal $I = (\pi, a)$. Let $\delta \in R$ be a generator for I, i.e., $(\pi, a) = (\delta)$. There exists $x, y \in R$ with $x\pi + ya = \delta$. Also $\pi \in (\delta)$ so $\delta | \pi$. This means that either $\delta \sim 1$ or $\delta \sim \pi$. But the case $\delta \sim \pi$ can not occur since $\pi \nmid a$ but $\delta | a$. So without loss of generality, assume that $\delta = 1$. Thus $x\pi + ya = 1$, hence $x\pi b + yab = b$, but since $\pi | ab$, we have $\pi | b$. □

Theorem 5.5. *A PID is a UFD*

Proof. Take $a \in R \setminus \{0\}$, such that a is not a unit. Assume that $a = \epsilon\pi_1 \dots \pi_n = \epsilon'\pi'_1 \dots \pi'_m$ are two distinct factorisation of a into irreducible. Without loss of generality we may assume that n is minimal amongst all elements a with non-unique factorisation. We have $\pi_1 | \pi'_1 \dots \pi'_m$ so by the lemma $\pi_1 | \pi'_i$ for some i. Without loss of generality we can assume that $i = 1$, so $\pi_1 | \pi'_1$ but both are irreducible, hence $\pi_1 \sim \pi'_1$. Without loss of generality we can assume that $\pi_1 = \pi'_1$. But then $\pi_2 \dots \pi_n = \epsilon\pi'_2 \dots \pi'_m$ and $\pi_2 \dots \pi_n$ has $n - 1$ irreducible factors, so by minimality of n, this factorisation into irreducible is unique. □

We show that $\mathcal{O}_{\mathbb{Q}(\sqrt{-3})} = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ is Euclidean. We claim that the Euclidean function is the Norm. $N(a + b\frac{1+\sqrt{-3}}{2}) = (a + b\frac{1+\sqrt{-3}}{2})(a + b\frac{1-\sqrt{-3}}{2}) = a^2 + ab + b^2$ (Note that we had over $\mathbb{Q}(\sqrt{-3})$ $N(c + d\sqrt{-3}) = c^2 + 3d^2$) and this fits we the previous line as $N(a + b\frac{1+\sqrt{-3}}{2}) = N(a + \frac{b}{2} + \frac{b}{2}\sqrt{-3}) = (a + \frac{b}{2})^2 + 3\frac{b^2}{4} = a^2 + ab + b^2$). Suppose we are given $\alpha = a + b\frac{1+\sqrt{-3}}{2}$ and $\beta = c + d\frac{1+\sqrt{-3}}{2}$ with $\beta \neq 0$. Then

$$\frac{\alpha}{\beta} = \frac{a + b\frac{1+\sqrt{-3}}{2}}{c + d\frac{1+\sqrt{-3}}{2}} = \frac{(a + b\frac{1+\sqrt{-3}}{2})(c - d\frac{1+\sqrt{-3}}{2})}{N(\beta)} = e + f\frac{1+\sqrt{-3}}{2} \in \mathbb{Q}[\frac{1+\sqrt{-3}}{2}]$$

(so note $e, f \in \mathbb{Q}$). Then pick $g, h \in \mathbb{Z}$ such that $|g - e|, |h - f| \leq \frac{1}{2}$ and set

$$q = g + h\frac{1+\sqrt{-3}}{2}$$

$$r = \alpha - \beta q$$

Then we have $\alpha = \beta q + r$ and furthermore if $r \neq 0$.

$$\begin{aligned} N(r) &= N(\alpha - \beta(g + h\frac{1+\sqrt{-3}}{2})) \\ &= N(\beta(e + f\frac{1+\sqrt{-3}}{2} - g - h\frac{1+\sqrt{-3}}{2})) \\ &= N(\beta)N((e-g) + (f-h)\frac{1+\sqrt{-3}}{2}) \\ &= N(\beta)[(e-g)^2 + (e-g)(f-h) + (f-h)^2] \\ &\leq \frac{3}{4}N(\beta) \\ &< N(\beta) \end{aligned}$$

Similar arguments works for $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ with $d \in \{-1, -2, -3, -7, -11\}$ (you might need to change the bound)

Theorem 5.6. *If $d < -11$ then $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is not a Euclidean domain (but for $d \in \{-19, -43, -67, -163\}$ it is a PID)*

Proof. Assume that $\phi : R \to \mathbb{Z}_{\geq 0}$ is Euclidean, where $R = \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. Now $R^* = \{\pm 1\}$. Take an element $b \in R \backslash \{0, \pm 1\}$ with $\phi(b)$ as small as possible. For all $a \in R$ there exists $q, r \in R$ with $r = a - qb$ and $\phi(r) < \phi(b)$ or $r = 0$. Now since $\phi(b)$ is as small as possible, we have that $r \in \{0, 1, -1\}$, for all $a \in R$. We also have that $a \equiv r \mod b$, hence $R/(b)$ has at most 3 elements.

On the other hand the number of elements of $(R/(b)) = (R : (b))\Delta((b)) = (R : (b))^2\Delta(R)$ (by Theorem 3.19 since $(b) \subset R$). Let $R = \mathbb{Z} + \mathbb{Z}\theta$ where $\theta = \begin{cases} \sqrt{d} & d \not\equiv 1 \mod 4 \\ \frac{1+\sqrt{d}}{2} & d \equiv 1 \mod 4 \end{cases}$. Then we have $(b) = \mathbb{Z}b + \mathbb{Z}b\theta$. Now $\Delta((b)) = \det \begin{pmatrix} b & \theta b \\ \bar{b} & \bar{\theta}\bar{b} \end{pmatrix}^2 = (b\bar{b}\bar{\theta} - \bar{b}b\theta)^2 = (b\bar{b})^2(\bar{\theta} - \theta)^2 = N(b)^2\Delta(R)$. Hence we have $(R : (b))^2 = N(b)^2$, that is $(R : (b)) = N(b)$ (since the norm is positive). So if we show that $\forall b \in R \setminus \{0, \pm 1\}$ we have $N(b) > 3$ then $R/(b)$ has more than three elements, contradicting the first paragraph. Now we always have $N(a + b\sqrt{d}) = a^2 + |d|b^2$

Suppose $d \not\equiv 1 \mod 4$, then for $a + b\sqrt{d}$ to be in R we need $a, b \in \mathbb{Z}$. Suppose that $a^2 + |d|b^2 \leq 3$ then $|a| \leq 1$ and $|d| > 11$, so $b = 0$, but $a + b\sqrt{d} \in \{0, \pm 1\}$

If $d \equiv 1 \mod 4$ we can also have $a = \frac{a'}{2}, b = \frac{b'}{2}$ where $a', b' \in \mathbb{Z}$ and $a' \equiv b' \mod 2$. Then $N(a + b\sqrt{d}) = N\left(\frac{a' + b'\sqrt{d}}{2}\right) = \frac{1}{2}(a'^2 + |d|b'^2)$. Suppose $N(a + b\sqrt{d}) \leq 3$ then $a'^2 + |d|b'^2 \leq 12$. But $|d| \geq 13$, so again $b' = 0$ and $a'^2 \leq 12$ so $|a'| \leq 3$. Hence $a' \in \{-2, 0, 2\}$, implying $a + b\sqrt{d} \in \{0, \pm 1\}$. □

Conjecture. *Let K be a number field that is not $\mathbb{Q}(\sqrt{d})$ for some $d < 0$ then if $\mathcal{O}_K$ is a UFD, then it is Euclidean.*

Remark. In general $\phi = N$ does not work, then ϕ is very difficult to find.

5.2 Dedekind Domain

Definition 5.7. A prime ideal is an ideal $P \subset R$ satisfying $P \neq R$ and $\forall a, b \in R$ with $ab \in P$ then either $a \in P$ or $b \in P$.

Fact. *$P \subset R$ is prime if and only if R/I is a domain*

Definition 5.8. A maximal ideal is an ideal $M \subset R$ satisfying $M \neq R$ and there are no ideals $I \neq R$ with $M \subset I \subset R$.

Fact. *$M \subset R$ is a maximal ideal if and only if R/M is a field.*

Every proper ideal $I \subset R$ is contained in a maximal ideal. (See commutative Algebra Theorem 1.4 and its Corollaries)

Example. Let $R = \mathbb{Z}$. Then its prime ideals are (0) and (p) where p is prime. Its maximal ideals are (p) (as $\mathbb{Z}/(p) = \mathbb{F}_p$ is a field)

Definition 5.9. A ring R is *Noetherian* if one and thus both of the following equivalent conditions holds.

1. Every ideal of R is finitely generated

2. Every ascending chains of ideals $I_0 \subset I_1 \subset \dots$ is stationary, i.e., there exists $r > 0$ such that $I_i = I_j$ for all $i, j > r$.

Definition 5.10. Let R be a domain. Then R is a *Dedekind Domain* if:

1. R is Noetherian
2. R is integrally closed in its field of fractions
3. Every non-zero prime ideal is a maximal ideal

Example. Every field is a Dedekind domain (the only ideals are: (0), (1))

Lemma 5.11. *Every finite domain is a field.*

Proof. Let R be a finite domain. Take $0 \neq a \in R$, we need to show there exists $x \in R$ with $ax = 1$. Consider the map $R \xrightarrow{\cdot a} R$ defined by $x \mapsto ax$. We note that $\cdot a$ is injective, if $ab = ac$ then $a(b-c) = 0$, hence $b - c = 0$ since R is a domain. As R is finite, $\cdot a$ is also surjective. Hence there exists x with $ax = 1$. $\square$

Theorem 5.12. *If K is a number field, then $\mathcal{O}_K$ is a Dedekind domain.*

Proof. Let $I \subset \mathcal{O}_K$ be an ideal. If $I = (0)$ then it is finitely generated, so assume I is non-zero. Hence there exists $0 \neq a \in I$, so $a\mathcal{O}_K$ is a full rank lattice in $\mathcal{O}_K$. We have $a\mathcal{O}_K \subset I \subset \mathcal{O}_K$, so I is a full rank lattice as well. It has $[K : \mathbb{Q}] < \infty$ generators as a free abelian group and the same elements generates it as an ideal. So $\mathcal{O}_K$ is Noetherian.

We know that $\mathcal{O}_K = \overline{\mathbb{Z}} \cap K$. Furthermore the integral closure of a ring R in an extension S is in fact integrally closed in S. So $\mathcal{O}_K$ is integrally closed in K.

Let $P \in \mathcal{O}_K$ be a non-zero prime ideal. P is a full rank lattice so $(\mathcal{O}_K : P) < \infty$. Hence $\mathcal{O}_K/P$ is a finite domain. So by the above lemma, $\mathcal{O}_K/P$ is a field and hence P is maximal. $\square$

Definition 5.13. Let R be a domain. Then a *fractional ideal* I of R is a R-submodule of the fields of fractions of R, such that there exists $0 \neq a \in R$ with $aI \subset R$

Example. Let us work out the fractional ideals of $\mathbb{Z}$. The ideals of $\mathbb{Z}$ are (n) with $n \in \mathbb{Z}$. So fractional ideals are $I \subset \mathbb{Q}$ such that $\exists a \in \mathbb{Z}$ with $aI = (n)$ for some $n \in \mathbb{Z}$. That is $I = \frac{n}{a}\mathbb{Z} \in \mathbb{Q}$.

Note that $\mathbb{Q}$ is not a fractional ideal, as elements of $\mathbb{Q}$ have arbitrary large denominators.

If R is a ring, $I, J \subset R$ are ideals, then IJ is the ideal generated by $\{ij : i \in I, j \in J\}$.

If R is a domain, I, J fractional ideals of R and K the field of fraction of R, then IJ is a K-submodule generated by $\{ij : i \in I, j \in J\}$. It is a fractional ideal as $abIJ \subset R$ (where a, b are such that $aI, bJ \subset R$)

Example. Let $R = \mathbb{Z}$ and consider $I = (a), J = (b)$ with $a, b \in \mathbb{Q}$. Then $IJ = (ab)$

Definition 5.14. Let R be a domain, K its field of fraction, $I \subset K$ a fractional ideal. Then I is called *invertible* if there exists a fractional ideal $J \subset K$ such that $IJ = R = (1)$

Example. Every non-zero fractional ideal of $\mathbb{Z}$ is invertible.

Every principal non-zero fractional ideal (a) of R is invertible, consider $(a)(a^{-1}) = (1)$

Theorem 5.15. *The invertible ideals of a domain R forms a group with respect to fractional ideal multiplication, with unit element $R = (1)$ and inverse $I^{-1} = \{a \in K | aI \subset R\}$. ($K$ is the field of fractions of R)*

Proof. Let $I \subset K$ be invertible, then there exists J with $IJ = R$. We want to show: if $a \in J$ then $aI \subset R$ and if $aI \subset R$ then $a \in J$. The first one follows directly. Consider $aIJ = aR$ and $aIJ \subset J$, so $aR \subset J$ means $a \in J$. Hence $J = I^{-1}$.

If I_1, I_2, I_3 are fractional ideals then $I_1(I_2I_3) = (I_1I_2)I_3$

Finally we show that if I, J are invertible then so is IJ^{-1}. We claim $(IJ^{-1})^{-1} = JI^{-1}$. To see this consider $(IJ^{-1})(JI^{-1}) = IRI^{-1} = II^{-1} = R$. $\square$

Theorem 5.16. *Let R be a domain. Then the following conditions on R are equivalent*

1. *R is Dedekind*
2. *Every non-zero fractional ideals of R is invertible*

3. *Every non-zero ideals of R is the product of prime ideals.*

4. *Every non-zero ideal of R is the product of prime ideals uniquely.*

We will prove this after some examples.

Example. $\mathcal{O}_{\mathbb{Q}(\sqrt{-5})} = \mathbb{Z}[\sqrt{-5}]$ is not a UFD, we have $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$. But since $\mathbb{Z}[\sqrt{-5}]$ is Dedekind (by Theorem 5.12), we can write (6) as the product of prime ideal uniquely. In fact $(6) = (2) \cdot (3) = (1+\sqrt{-5})(1-\sqrt{-5}) = (2, 1+\sqrt{-5})(2, 1-\sqrt{-5})(3, 1+\sqrt{-5})(3, 1-\sqrt{-5})$. We check that $(2, 1+\sqrt{-5})$ is prime. Now $\mathbb{Z}[\sqrt{-5}]/(2, 1+\sqrt{-5}) \cong \mathbb{Z}[x]/(x^2+5, 2, 1+x)$. Now $(2, x+1, x^2+5) = (2, x+1, x^2+5-x(x+1) = (2, x+1, -x+5) = (2, x+1)$. Hence $\mathbb{Z}[\sqrt{-5}]/(2, 1+\sqrt{-5}) \cong \mathbb{Z}[x]/(2, x+1) \cong \mathbb{F}_2[x]/(x+1) \cong \mathbb{F}_2$, which is a field. Thus $(2, 1+\sqrt{-5})$ is maximal.

Definition 5.17. If R is a domain and K its field of fraction. Let I be a non-zero fractional ideal then $R : I = \{a \in K : aI \subset R\}$

Note that from Theorem 5.15, we see that I is invertible if and only if $(R : I) \cdot I = R$

Example 5.18. $R = \mathbb{Z}[\sqrt{-3}]$ is not Dedekind. (As it is not algebraically closed)

We show that the ideal $I = (2, 1+\sqrt{-3})$ is not invertible. $R : I = \{a + b\sqrt{-3} \in \mathbb{Q}(\sqrt{-3}) : 2(a+b\sqrt{-3}) \in \mathbb{Z}[\sqrt{-3}], (1+\sqrt{-3})(a+b\sqrt{-3}) \in \mathbb{Z}[\sqrt{-3}]\}$. From the first condition, we can rewrite $a = \frac{a'}{2}, b = \frac{b'}{2}$ with $a', b' \in \mathbb{Z}$. So consider the second condition

$$(1+\sqrt{-3})(\frac{a'}{2} + \frac{b'}{2}\sqrt{-3}) = \frac{a'}{2} + \frac{a'+b'}{2}\sqrt{-3} - 3\frac{b'}{2}$$

So $a' \equiv b' \mod 2$, i.e.,

$$\mathbb{Z}[\sqrt{-3}] : (2, 1+\sqrt{-3}) = \left\{\frac{a'+b'\sqrt{-3}}{2} : a', b' \in \mathbb{Z}, a' \equiv b' \mod 2\right\} = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$$

Now

$$\begin{aligned}
\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right] \cdot (2, 1+\sqrt{-3}) &= \left(1, \frac{1+\sqrt{-3}}{2}\right)(2, 1+\sqrt{-3}) \\
&= \left(2, 1+\sqrt{-3}, \frac{1+\sqrt{-3}}{2}(1+\sqrt{-3})\right) \\
&= (2, 1+\sqrt{-3}, \sqrt{-3}-1) \\
&= (2, 1+\sqrt{-3}) \\
&= I \\
&\neq R
\end{aligned}$$

Hence I is not invertible.

We now show that $I = (2)$ can not be written as the product of prime ideals. Suppose $I = P_1 P_2 \ldots P_n$, then $I \subset P_i$ for all i. Now $\{$ideals of R containing $I\} \leftrightarrow \{$ideals of $R/I\}$. The bijection is defined by $J \mapsto J/I \subset R/I$ and $\{x : \overline{x} \in J\} \longleftarrow\!\dashv \overline{J}$

In our case

$$\begin{aligned}
{}^{R}\!/_{I} &= {}^{\mathbb{Z}[\sqrt{-3}]}\!/_{(2)} \\
&\cong {}^{\mathbb{Z}[x]}\!/_{(x^2+3, 2)} \\
&\cong {}^{\mathbb{F}_2[x]}\!/_{(x^2+1)} \\
&\cong {}^{\mathbb{F}_2}\!/_{(x+1)^2} \\
&\cong {}^{\mathbb{F}_2[x]}\!/_{(x)^2} \\
&= \{a + b\epsilon : a.b \in \mathbb{F}_2, \epsilon^2 = 0\}
\end{aligned}$$

The ideals in R/I are $(0), (1) = (1+\epsilon)$ and (ϵ). Which of these ideal is prime? (1) is never prime, and (0) is not prime as it is not a domain. So (ϵ) is the only maximal ideal and hence must be the only prime R/I has. Clearly $(2) \subset (2, 1+\sqrt{-3})$, which we saw maximal and so must be the only prime ideal which contains (2).

So all P_i are equal to $(2, 1+\sqrt{-3})$. Thus $(2) = (2, 1+\sqrt{-3})^m$ for some m. Now $(2) \neq (1)$, hence $m \neq 0$ and $(2) \neq (2, 1+\sqrt{-3})$ as the first is invertible but not the second so $m \neq 1$.

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

So if $(2)(2, 1+\sqrt{-3}) = (2)$, then $(2, 1+\sqrt{-3}) = (2^{-1})(2) = (1)$ which is a contradiction. And for all $m \geq 2$ we have $(2, 1+\sqrt{-3})^m \subset (2, 1+\sqrt{-3})^2 \subset (2)$. Hence there is no m with $(2, 1+\sqrt{-3})^m = (2)$.

The proof of Theorem 5.16 requires proofs by Noetherian induction. Here is a quick layout of how such a proof works. To prove a statement about ideals in a Noetherian ring R:

- First prove it for all maximal ideals.
- Then induction step: assume it holds for all $I \supsetneq J$. Prove it hold for J

Why does this proves the statement for all ideal? Suppose the statement is false for a certain set $S \neq \emptyset$ of ideals: Pick any $I_0 \in S$. By induction step, there exists $I_1 \supsetneq I_0$, for which the statement is false. Repeat and we get an infinite ascending chain, which is impossible in a Noetherian ring.

Proof of Theorem 5.16. [NB: This proof is rather long and was spread over several lectures. The lecturer got a big confuse at some point and so it also incomplete, it only proves some implications, including the most important for this course, Dedekind implies everything else. I have tried to reorganise this proof so that it makes more sense. I do know that he managed to prove it in one lecture successfully the following year (2011-2012) but I did not get a copy of it]

Note: If R is a field, the only ideals are (0) and (1) so there is nothing to prove. Hence assume that R is not a field.

2. $\Rightarrow$ 3. Assume 2. We want to show that every ideal is the product of prime ideals. We first show that every invertible ideal is finitely generated. Let I be a fractional ideal of R, then there exists J with $IJ = (1)$, hence $1 \in IJ$. Now elements of IJ are sums of the form $r_1x_1y_1 + \cdots + r_nx_ny_n$ with $r_i \in R, x_i \in I$ and $y_i \in J$. Hence $1 = \sum r_ix_iy_i$ for some r_i, x_i, y_i. We claim that $I = (x_1, \ldots, x_n)$, to prove our claim we just need to show that $(x_1, \ldots, x_n)J = (1)$ (since inverses in groups are unique). It is obvious that $(1) \subset (x_1, \ldots, x_n)J$. On the other hand $(x_1, \ldots, x_n) \subset I$ so $(x_1, \ldots, x_n)J \subset IJ \subset (1)$.

Hence R is Noetherian, since every invertible ideal is finitely generated.

Lemma 5.19. *Assuming 2., we have for non-zero ideals I, J: $I \subset J$ if and only if $J|I$ (that is there is a J' with $JJ' = 1$)*

Proof. $\Leftarrow$) Obvious

$\Rightarrow$) Put $J' = IJ^{-1}$, this is a fractional ideal. We need to show that $IJ^{-1} \subset R$ (i.e., that it is an ideal and not just a fractional ideal). We have $I \subset J$, so $IJ^{-1} \subset JJ^{-1} = R$ □

We now proceed by a proof by Noetherian induction.

If I is a maximal ideal, then I is itself a factorisation into prime ideals. Now let an ideal I not prime be given and assume that for all $J \supsetneq I$, J has a factorization into primes. There exists is a prime $P \supsetneq I$, so $P|I$ and hence $I = PJ$ for some $J \subset R$. We want to show that $J \supsetneq I$. We know that $I = PJ \subset J$. Suppose that $I = J$, then $PJ = J$, so multiply by J^{-1}, then $P = R$ which is a contradiction.

Hence we have just shown by Noetherian induction that every fractional ideal is a product of primes.

1., 2.&3. $\Rightarrow$ 4. Assume there is an ideal I that has two distinct factorisation into primes. That is $I = P_1 \ldots P_m = Q_1 \ldots Q_n$ and without loss of generality suppose that m is minimal. We have that no Q_i is equal to some P_j as otherwise if $Q_i = P_j$ then $P_1 \ldots P_{j-1}P_{j+1} \ldots P_m = IP_j^{-1} = Q_1 \ldots Q_{i-1}Q_{i+1} \ldots Q_n$ contradicting minimality of m.

We have $Q_1 \dots Q_n = P_1 \dots P_m \subset P_1$, so $P_1 | Q_1 \dots Q_m$. Let $I' = IP_1^{-1} = P_2 \dots P_m = Q_1 \dots Q_n P_1^{-1}$. Now I' is an ideal of R but it has a factorisation into $n-1$ factors, so this factorisation is unique. We want to show that there exists i with $Q_i | I'$, equivalently there exists i with $I' \subset Q_i$. Assume that there is no such i, then $\forall i\, I' \not\subseteq Q_i$. Consider P_1 and Q_1 which are distinct. We have $P_1, Q_1 \subset P_1 + Q_1$. We claim that $P_1 + Q_1 = R$. Since P_1 and Q_1 are maximal (assuming 1.) we have $P_1 \subset P_1 + Q_1 \Rightarrow P_1 + Q_1 = P_1$ or R, similarly, we concluder $P_1 + Q_1 = Q_1$ or R. Hence $P_1 + Q_1 = R$.

So there exists $p \in P_1, q \in Q_1$ with $p + q = 1$. So $I = (p+q)I = pI + qI \subset pQ_1 + qP_1 \subset P_1 Q_1$. So $P_1 Q_1 | I \Rightarrow Q_1 | IP_1^{-1} = I'$. Hence we get a contradiction.

1. $\Rightarrow$ 2. We use Noetherian induction.

Let P be a maximal ideal, then we want to show that P is invertible. Pick $0 \neq a \in P$. Then the ideal (a) is invertible ($(a)(a^{-1}) = (a)$) and $(a) \subset P$.

Lemma 5.20. *Let R be a Dedekind domain and let $I \neq 0$ be an ideal. There exists $P_1, \dots, P_n$ maximal ideals with $P_1 \dots P_n \subset I$*

Proof. We'll use Noetherian induction. If I is maximal then $I \subset I$. Assume for all $J \supsetneq I$, we have prime ideals Q_i with $Q_1 \dots Q_n \subseteq I$. We have to show that there exists P_i prime ideals with $P_1 \dots P_n \subset I$. I itself is not prime because all non-zero primes are maximal.

This means there exists $a, b \in R$ such that $a, b \notin I$ but $ab \in I$. Consider the ideals $I + (a)$ and $I + (b)$. By induction hypothesis there exists P_i such that $P_1, \dots, P_n \subset I + (a)$ and $P_{n+1} \dots P_m \subset 1 + (b)$. Hence $P_1 \dots P_m \subset (I + (a))(I + (b)) \subset I$. $\square$

Hence by the lemma, there exists $P_1, \dots, P_n$ with $P_1 \dots P_n \subset (a)$ and without loss of generality we have n is minimal.

We will use the following lemma later in the proof.

Lemma 5.21. *Let R be a Dedekind domain and let $I \subset R$ be a finitely generated ideal. Let $\phi : I \to I$ be a map such that $\phi(I) \subset I$, then there exists $a_0, \dots, a_{n-1} \in J$ such that $\phi^n + a_{n-1}\phi^{n-1} + \dots + a_0 = 0$*

A special case: Let $\alpha \in K$, the field of fraction of R, be such that $\alpha I \subset I$. Then there exists a relation $\alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_0 = 0$ with $a_i \in R$

Proof. Choose a matrix that $A = (a_{ij})_{ij}$, that describes ϕ in terms of x_i, the generators of I, and that satisfies $a_{ij} \in I$. By Cayley-Hamilton, if P_A is the characteristic polynomial of A, then $P_A(A) = 0$. Now $P_A = \det(XI_n - A) := X^n + a_{n-1}X^{n-1} + \dots + a_0$ for some a_i which clearly are in R. $\square$

Corollary 5.22. *If R is Dedekind and K its field of fraction. Let $I \subset R$ be an ideal and $\alpha \in K$ with $\alpha I \subset I$, then $\alpha \in R$.*

As a recap, we have $P \neq 0$ is prime (and hence maximal). Take $0 \neq a \in P$, then there exists $P_1, \dots, P_n$with $P_1 \dots P_n \subset (a) \subset P$. We claim that one of the P_i is P. In general for prime ideals we have $IJ \subset P \Rightarrow I \subset P$ or $J \subset P$. (Otherwise, assume $I \not\subseteq P, J \not\subseteq P$, then there exists $a \in I, b \in J$ with $a \notin P, b \notin P$, but then $ab \notin P$). So without loss of generality assume $P_1 \subset P$, but P_1 is maximal so $P_1 = P$

Let $J = P_2 \dots P_n$, i.e., $PJ \subset (a) \subset P$. Since we assumed n was minimal, we have $J \not\subseteq (a)$. So $PJ \subset (a)$, hence $PJ(a)^{-1} \subset R$, but $a^{-1}J \not\subseteq R$.

Consider $R : P = \{\alpha \in K | \alpha P \subset R\}$, we need to show that $(R : P)P = R$. Now $\forall \alpha \in R : P$, we have $\alpha P \subset P$, so by the corollary $R : P \subset R$. We have $P \subset (R : P)P \subset P$, but P is maximal, so if $(R : P)P \neq R$ then $(R : P)P = P$. Hence if P is not invertible then $R : P = R$. Take $\alpha \in a^{-1}J \setminus R$. Then $\alpha P \subset R$, so $\alpha \in R : P$ but $\alpha \notin R$. Contradicting $R : P = R$, hence P is invertible.

So we have proven that every non-zero prime ideals (i.e., every maximal ideal) is invertible. We finish off the Noetherian induction.

Assume for all $J \supsetneq I$ we have that J is invertible. We will show I is invertible. Choose a prime $P \supset I$. We know that P is invertible. Consider $I \subset P^{-1}I \subset R$. (Since $P^{-1}I \subset PP^{-1} = R$) If $P^{-1}I \neq I$ then $P^{-1}I \supsetneq I$, so $P^{-1}I$ is invertible. Then $I = RI = P(P^{-1}P)$ is invertible as well. So assume $P^{-1}I = I$. For all $\alpha \in P^{-1}$ we have $\alpha I \subset I$, thus $\alpha \in R$. Hence $P^{-1} \subset R \Rightarrow PP^{-1} = R \subset RP = P$ which is a contradiction.

$\square$

Definition 5.23. Let K be a number field. Then the *ideal group* of K is the group I_K consisting of all fractional ideals of $\mathcal{O}_K$

The *principal ideal group* of K, P_K, is the group of all principal ideals.

We have $P_K \lhd I_K$. The quotient $\mathrm{Cl}_K = I_K/P_K$ is called the *calls group* of K.

An *ideal class* is a set $\{\alpha I : \alpha \in K^*\}$ of ideals.

Theorem 5.24. *For all number field K, the class group is finite. The class number of K is $h_K := |Cl_K|$*

We will prove this later in the course.

Remark. If $\mathcal{O}_K$ is a PID, then $h_K = 1$ (in fact this is a if and only if statement.)

P_K is the trivial ideal class. Define a map $K^* \to P_K$ by $\alpha \mapsto (\alpha)$. Then $P_K \cong K^*/\mathcal{O}_K^*$, so the kernel is $\mathcal{O}_K$

Lemma 5.25. *If R is a UFD then for an irreducible elements, π, the ideal (π) is prime.*

Proof. Take $a, b \in R$ with $ab \in (\pi)$. This means $\pi | ab$ hence $\pi | a$ or $\pi | b$. So $a \in (\pi)$ or $b \in (\pi)$ $\square$

Theorem 5.26. *Let R be a Dedekind domain. Then R is a UFD if and only if R is a PID.*

Proof. $\Leftarrow$) Every PID is a UFD

$\Rightarrow$) Let $I \neq 0$ be any ideal that is not principal. We can write $I = P_1 P_2 \dots P_n$, without loss of generality say P_1 is not principal. Now take any $0 \neq a \in P_1$ and write $a = \epsilon \pi_1 \dots \pi_m$ with π_i irreducible. Then $(a) = (\pi_1)(\pi_2)\dots(\pi_m)$. But $P_1 | (a)$, so we get P_1 is not principal while (a) is, hence contradiction. $\square$

So $\mathcal{O}_K$ is a UFD if and only if $h_K = 1$. We can say "h_K measures the non-uniqueness of factorisation on $\mathcal{O}_K$"

Example. Find all integer solutions to $x^2 + 20 = y^3$

We can factorise this over $\mathbb{Z}[\sqrt{-5}] = \mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$ into $(x + 2\sqrt{-5})(x - 2\sqrt{-5}) = y^3$. Fact: $h_{\mathbb{Q}(\sqrt{-5})} = 2$.

As ideals we have $(x + 2\sqrt{-5}) \cdot (x - 2\sqrt{-5}) = (y)^3$. As usual, let us find the common factors of $(x + 2\sqrt{-5})$ and $(x - 2\sqrt{-5})$

Suppose P is a prime ideal such that $P | (x + 2\sqrt{-5})$ and $P | (x - 2\sqrt{-5})$, then $(x + 2\sqrt{-5}, x - 2\sqrt{-5}) \subseteq P$. Now we have $(4\sqrt{-5}) \subset (x + 2\sqrt{-5}, x - 2\sqrt{-5})$. Note that $(2, 1 + \sqrt{-5})(2, 1 - \sqrt{-5}) = (4, 2 + 2\sqrt{-5}, 2 - 2\sqrt{-5}, 6) = (2)$, hence $(2) = (2, 1 + \sqrt{-5})^2$ (and we know from a previous exercise that $(2, 1 + \sqrt{-5})$ is prime). Furthermore $(\sqrt{-5})$ is prime:

$$\begin{aligned} \mathbb{Z}[\sqrt{-5}]/(\sqrt{-5}) &\cong \mathbb{Z}[x]/(x^2+5, x) \\ &\cong \mathbb{Z}[x]/(5, x) \\ &\cong \mathbb{F}_5 \end{aligned}$$

So $(4\sqrt{-5}) = (2, 1 + \sqrt{-5})^4(\sqrt{-5}) \Rightarrow P = (2, 1 + \sqrt{-5})$ or $P = (\sqrt{-5})$.

Write $(x + 2\sqrt{-5}) = (2, 1 + \sqrt{-5})^{e_1}(\sqrt{-5})^{e_2} \prod P_i^{e_i}$. Apply the automorphism $\alpha \mapsto \overline{\alpha}$, to get $(x - 2\sqrt{-5}) = (2, 1 + \sqrt{-5})^{e_1}(\sqrt{-5})^{e_2} \prod \overline{P_i}^{e_i}$ (since $(\sqrt{-5}) = (-\sqrt{-5})$ and as noted before $(2, 1 + \sqrt{-5}) = (2, 1 - \sqrt{-5})$). Note that the products P_i must be distinct. So we get $(x + 2\sqrt{-5})(x - 2\sqrt{-5}) = (2, 1 + \sqrt{-5})^{2e_1}(\sqrt{-5})^{2e_2} \prod P_i^{e_i} \prod \overline{P_i}^{e_i} = (y)^3$. Since factorization into prime ideal is unique, we have $3 | e_i$ for all i. Hence $(x + 2\sqrt{-5}) = I^3$ for some ideal I.

Let $\widetilde{I}$ be the class of I. Then in $\mathrm{Cl}_{\mathcal{O}_{\mathbb{Q}(\sqrt{-5})}}$, we have $\widetilde{I}^3 = 1$ (since $(x + 2\sqrt{-5})$ is principal). Now the class group has order 2, hence $\widetilde{I} = 1$ since $\gcd(2, 3) = 1$. Hence I is principal, so write $I = (a + b\sqrt{-5})$. So $(x + 2\sqrt{-5}) = ((a + b\sqrt{-5})^3) \Rightarrow x + 2\sqrt{-5} = \text{unit} \cdot (a + b\sqrt{-5})^3$. Now units in $\mathbb{Z}[\sqrt{-5}]$ are ± 1, which are both cubes, so without loss of generality, $x + 2\sqrt{-5} = (x + b\sqrt{-5})$.

Hence $x + 2\sqrt{05} = a^3 + 3a^2 b\sqrt{-5} - 15ab^2 - 5b^3\sqrt{-5} = (a^3 - 15ab^2) + \sqrt{-5}(3a^2 b - 5b^3)$. So we need to solve $2 = b(3a^2 - 5b^2)$, but 2 is prime, so $b = \pm 1, \pm 2$.

If $b = \pm 1$, then $3a^2 - 5 = \pm 2$, either $3a^2 = 7$ which is impossible, or $3a^2 = 3 \Rightarrow a = \pm 1$. In that case we have $x = a^3 - 15ab^2 = \pm(1 - 15) = \pm 14$. Then $14^2 + 20 = 196 + 20 = 216 = 6^3 \Rightarrow (\pm 14, 16)$ are solutions.

If $b = \pm 2$, then $3a^2 - 20 = \pm 1$, so $3a^2 = 21$ or 19, but both cases are impossible.

Hence $(\pm 14, 16)$ are the only integer solutions to $x^2 + 20 = y^3$.

5.3 Kummer-Dedekind Theorem

Let K be a number field, and $I \subset \mathcal{O}_K$ a non-zero ideal. Note that I contains $a\mathcal{O}_K$ for any $a \in I$, hence we have that $(\mathcal{O}_K : I)$ is finite. This leads us to the following definition:

Definition 5.27. The norm of an ideal $I \subset \mathcal{O}_K$ is defined as $N(I) = \begin{cases} (\mathcal{O}_K : I) & I \neq 0 \\ 0 & I = 0 \end{cases}$

Theorem 5.28. *For any principal ideal $(a) \subset \mathcal{O}_K$, we have $N((a)) = |N(a)|$*

Proof. If $\omega_1, \ldots, \omega_n$ is a basis for $\mathcal{O}_K$, then $a\omega_1, \ldots, a\omega_n$ is a basis for (a). Now multiplication by a can be seen as a matrix A in terms of $\omega_1, \ldots, \omega_n$. So $(\mathcal{O}_K : a\mathcal{O}_K) = |\det A| = |N(a)|$ □

Theorem 5.29. *The norm of ideals in $\mathcal{O}_K$ is multiplicative. That is $N(IJ) = N(I)N(J)$*

Proof. First note $N(\mathcal{O}_K) = 1$.

We can write every non-zero ideal as a product of prime ideals (as $\mathcal{O}_K$ is Dedekind and using Theorem 5.16) So it suffices to prove that $N(IP) = N(I)N(P)$ where P is a non-zero prime. We have $N(IP) = (\mathcal{O}_K : IP)$ and $IP \subset I \subset \mathcal{O}_K$, hence $N(IP) = (I : IP)(\mathcal{O}_K : I) = (I : IP)N(I)$.

We must show that $(I : IP) = N(P) = (\mathcal{O}_K : P)$. Now P is maximal, so $\mathcal{O}_K/P$ is a field. We have I/IP is a vector space over $\mathcal{O}_K/P$. We want to show that $d = \dim_{\mathcal{O}_K/P} I/IP = 1$.

$IP \neq I$ as $\mathcal{O}_K$ is Dedekind, so $I/IP \neq 0$, hence $d \geq 1$

Suppose that $d \geq 2$, then there exists $\overline{a}, \overline{b} \in I/IP$ that are linearly independent over $\mathcal{O}_K/P$. Take lifts $a, b \in I$. For all $x, y \in \mathcal{O}_K$ with $ax+by \in P$, we have $x \in P$ and $y \in P$. Write $I = P^e I'$, then $(a) \subset I$, so $P^e|I|(a)$, also $a \notin IP$, so $IP \nmid (a)$. Hence $P^{e+1} \nmid (a)$. Similarly we find $P^{e+1} \nmid (b)$. So we can rewrite this as $(a) = P^e I' J_1, (b) = P^e I' J_2$ with $P \nmid I'J_1, P \nmid I'J_2$. We have $(a)J_2 = (b)J_1$. Since $J_2 \nsubseteq P$, there exists $c \in J_2 \setminus P$. So $av \in (b)J_1 \Rightarrow ac = be$ for some $e \in J_1$. Now $ac - be = 0 \in P \Rightarrow c \in P$. This is a contradiction. Hence the dimension is 1 as required. □

Corollary 5.30. *If $N(I)$ is prime, then I is prime*

Proof. If I is not prime, then $I = PI'$ with P a non-zero prime and $I' \neq (1)$. Then $N(I) = N(P)N(I')$ cannot be prime. □

Theorem 5.31. *If $I \subset \mathcal{O}_K$ is a non-zero prime, then $N(I) = p^f$ for some prime p and $f \in \mathbb{Z}_{>0}$*

Proof. $\mathcal{O}_K/I$ is a field (I is maximal) of $N(I)$ elements. Any finite field has p^f elements for some prime p and $f \in \mathbb{Z}_{>0}$ □

Theorem 5.32. *If I is a non-zero ideal, we have $N(I) \in I$*

Proof. $N(I) = |\mathcal{O}_K/I|$ by definition. Then Lagrange theorem implies $N(I) \cdot \mathcal{O}_K/I = \mathcal{O}_K$, so $N(I)\mathcal{O}_K \subset I$. □

Theorem 5.33. *If P is a non-zero prime with $N(P) = p^f$ then $p \in P$*

Proof. By the previous theorem we have $p^f \in P$. But since P is prime, $p \in P$. □

Kummer - Dedekind Theorem. *Let $f \in \mathbb{Z}[x]$ be monic and irreducible. Let $\alpha \in \overline{\mathbb{Q}}$ be such that $f(\alpha) = 0$. Let $p \in \mathbb{Z}$ be prime. Choose $g_i(x) \in \mathbb{Z}[x]$ monic and $e_i \in \mathbb{Z}_{>0}$ such that $f \equiv \prod g_i(x)^{e_i} \mod p$ is the factorization of $\overline{f} \in \mathbb{F}_p[x]$ into irreducible (with $\overline{g_i} \neq \overline{g_j}$ for $i \neq j$). Then:*

1. *The prime ideals of $\mathbb{Z}[\alpha]$ containing p are precisely the ideals $(p, g_i(\alpha)) =: P_i$*
2. *$\prod P_i^{e_i} \subset (p)$*
3. *If all P_i are invertible then $\prod P_i^{e_i} = (p)$. Furthermore $N(P_i) = p^{f_i}$ where $f_i = \deg g_i$*
4. *For each i, let $r_i \in \mathbb{Z}[x]$ be the remainder of f upon division by g_i. Then P_i is not invertible if and only if $e_i > 1$ and $p^2 | r_i$*

Proof.

1. We have $\mathbb{Z}[\alpha] \cong \mathbb{Z}[x]/(f)$ (Galois Theory). Primes of $\mathbb{Z}[\alpha]$ containing p have a one to one correspondence to primes of $\mathbb{Z}[\alpha]/(p) \cong \mathbb{Z}[x]/(p)(f)$. But $\mathbb{Z}[x]/(p, f) \cong \mathbb{F}_p[x]/(\overline{f})$, so primes of $\mathbb{F}_p[x]/(\overline{f})$ have a one to one correspondence to primes of $\mathbb{F}_p[x]$ containing $\overline{f}$. We know $\mathbb{F}_p[x]$ is a PID. So theses primes corresponds to irreducible $\overline{g} \in \mathbb{F}_p[x]$ such that $\overline{g}|\overline{f} \iff \overline{f} \in (\overline{g})$.

   Working backward from this set of correspondence we get what we want

2. Let $I = \prod(p, g_i(\alpha))^{e_i}$.We want to show that $I \subset (p)$, i.e., all elements of I are divisible by p. Now I is generated by expression of the form $p^d \prod_{i=1}^s g_i(\alpha)^{m_i}, m_i \le e_i$. So the only non-trivial case is when $d = 0$, i.e., $\prod g_i(\alpha)^{e_i}$. We have $\prod g_i(x)^{e_i} \equiv f \mod p$. Substituting α we get $\prod g_i(\alpha)^{e_i} \equiv f(\alpha) \equiv 0 \mod p$

3. Assume $\mathbb{Z}[\alpha] = \mathcal{O}_{\mathbb{Q}(\alpha)}$. We have $\prod P_i^{e_i} \subset (p) \Rightarrow (p) | \prod P_i^{e_i}$. Now $N((p)) = |N(p)| = p^n$ where $n = \deg f$. So $N(\prod P_i^{e_i}) = \prod N(P_i^{e_i}) = p^{\sum e_i \cdot \deg(g_i)} = p^n$

4. Left out as it requires too much commutative algebra.

$\square$

Example. Consider $\mathbb{Q}(\sqrt{-5})$, then $\mathcal{O}_{\mathbb{Q}(\sqrt{-5})} = \mathbb{Z}[\sqrt{-5}]$. So take $f = x^2 + 5$.

- $p = 2$, then $\overline{f} = x^2 + 1 = (x+1)^2 \in \mathbb{F}_2[x]$. So $g_1 = x + 1$ and $e_1 = 2$. Now $(2) = P_1^2 = (2, 1 + \sqrt{-5})^2$ and $N(P_1) = 2$. If P_1 principle? If $P_1 = (\alpha)$ then $N(P_1) = |N(\alpha)|$. Now $N(a + b\sqrt{-5}) = a^2 + 5b^2$ which is never 2. Hence P_1 is not principal.

- $p = 3$, then $\overline{f} = x^2 - 1 = (x+1)(x-1) \in \mathbb{F}_3[x]$. So we have $(3) = P_1P_2$ where $P_1 = (3, -1 + \sqrt{-5})$ and $P_2 = (3, 1 + \sqrt{-5})$. Again we have $N(P_1) = N(P_2) = 3$, so neither are principal as $3 \ne a^2 + 5b^2$.

- $p = 5$, then $\overline{f} = x^2 \in \mathbb{F}_5[x]$. So we get $(5) = (5, \sqrt{-5})^2 = (\sqrt{-5})^2$ (since $5 = -\sqrt{-5}\sqrt{-5}$).

Consider $\mathbb{Q}(\sqrt[3]{2})$, then $\mathcal{O}_{\mathbb{Q}(\sqrt[3]{2})} = \mathbb{Z}[\sqrt[3]{2}]$. So take $f = x^3 - 2$.

- $p = 2$, then $\overline{f} = x^3 \in \mathbb{F}_2[x]$. So $(2) = (2, \sqrt[3]{2})^3 = (\sqrt[3]{2})^3$ (since $2 = \sqrt[3]{2}\sqrt[3]{2}\sqrt[3]{2}$)

- $p = 3$, then $\overline{f} = x^3 - 2$ is a cubic. Cubic polynomials are reducible if and only if they have a root. If this case, i.e., in $\mathbb{F}_3$, we have 2 is a root. So $x^3 - 2 = (x-2)(x^2 + 2x + 1) = (x-2)(x+1)^2 = (x+1)^3$. Hence $(3) = (3, 1 + \sqrt[3]{2})^3$ and $N(3, 1 + \sqrt[3]{2}) = 3$. Now $(3, 1 + \sqrt[3]{2})$ is principal if there exist $\alpha \in (3, 1 + \sqrt[3]{2})$ with $|N(\alpha)| = 3$. Notice that $N(1 + \sqrt[3]{2}) = 1^3 + 2 \cdot 1^3 = 3$, so $(3, 1 + \sqrt[3]{2}) = (1 + \sqrt[3]{2})$

6 The Geometry of Numbers

6.1 Minkowski's Theorem

Let K be a number field of degree n. Let $\sigma_1, \ldots, \sigma_n : K \hookrightarrow \mathbb{C}$ be its complex embedding. We see that if $\sigma : K \hookrightarrow \mathbb{C}$ is an embedding then $\overline{\sigma} : K \hookrightarrow \mathbb{C}$ defined by $\alpha \mapsto \overline{\sigma(\alpha)}$ is also an embedding. We have $\overline{\overline{\sigma}} = \sigma$ so $^-$ is an involution on $\{\sigma_1, \ldots, \sigma_n\}$, with fixed points being those σ with $\sigma(k) \subseteq \mathbb{R}$ for all $k \in K$.

Definition 6.1. Let K be a number field of degree n and $\sigma_1, \ldots, \sigma_n : K \hookrightarrow \mathbb{C}$ be its complex embeddings. Say there are r real embeddings ($\sigma(k) \subset \mathbb{R}$) and s pairs of complex embedding. So we have $r + 2s = n$. Then (r, s) is called the *signature* of K

We can use $\sigma_1, \ldots, \sigma_n$ to embed K into $\mathbb{C}^n$ by $\alpha \mapsto (\sigma_1, (\alpha), \ldots, \sigma_n(\alpha))$. We view $\mathbb{C}^n$ as $\mathbb{R}^{2n}$ with the usual inner product, that is $||z_1, \ldots, z_n||^2 = |z_1|^2 + \cdots + |z_n|^2$.

Let $v_1, \ldots, v_m \in \mathbb{R}^{2n}$ be given, denote $P_{v_1,\ldots,v_m} := \{\lambda_1 v_1 + \cdots + \lambda_m v_m : \lambda_i \in [0,1]\}$. We have (see Algebra I)

$$\mathrm{Vol}(P_{v_1,\ldots,v_m}) = \left(\det \begin{pmatrix} \langle v_1, v_1 \rangle & \cdots & \langle v_1, v_m \rangle \\ \vdots & \ddots & \vdots \\ \langle v_m, v_1 \rangle & \cdots & \langle v_m, v_m \rangle \end{pmatrix} \right)^{1/2}$$

Theorem 6.2. $(\sigma_1, \ldots, \sigma_n)$ *embeds* K *as a subset of* $K_{\mathbb{R}} := \{z_1, \ldots, z_n \in \mathbb{C}^n : z_i = \overline{z_j} \text{ when } \sigma_i = \overline{\sigma_j}\}$

Proof. For each $\alpha \in K$ we have $(\sigma_1(\alpha), \ldots, \sigma_n(\alpha)) = (z_1, \ldots, z_n)$ satisfied for i, j with $\sigma_i = \overline{\sigma_j}$. So $z_i = \sigma_i(\alpha) = \overline{\sigma_j(\alpha)} = \overline{z_j}$ □

Theorem 6.3. $K_{\mathbb{R}}$ *has dimension* n.

Proof. Without loss of generality let $\sigma_1, \ldots, \sigma_r$ be the real embedding of $K \hookrightarrow \mathbb{R}$ and let $\sigma_{r+i} = \overline{\sigma_{r+s+i}}$ for $i \in \{1, \ldots, s\}$. Identifying $\mathbb{C}^n \cong \mathbb{R}^{2n}$, we have $(x_1, y_1, x_2, y_2, \ldots, x_n, y_n)$ is in $K_{\mathbb{R}}$ if an only if:

- $y_i = 0$ for $i \in \{1, \ldots, r\}$
- $x_{r+i} = x_{r+i+s}$ for $i \in \{1, \ldots, s\}$
- $y_{r+i} = -y_{r+i+s}$ for $i \in \{1, \ldots, s\}$

The number of independent linear equation is $r + 2s = n$. Hence the dimension of $K_{\mathbb{R}} = 2n - n = n$. □

Definition 6.4. Let V be a finite dimensional vector space over $\mathbb{R}$, with inner product $\langle\, , \rangle$ (that is a positive definite symmetric bilinear form). Then V is called a *Euclidean space.*

Example. $V = \mathbb{R}^n$ with $\langle (x_1, \ldots, x_n), (y_1, \ldots, y_n) \rangle = x_1 y_1 + \cdots + x_n y_n$. Or V a subspace of $\mathbb{R}^n$ (with the same inner product)

Fact. *Any Euclidean space has an orthonormal basis.*

Definition 6.5. Let V be an Euclidean space. A *lattice* Λ in V is a subgroup generated by $\mathbb{R}$-linearly independent vectors, $v_1, \ldots, v_m$.

The *rank* of the lattice is m.

The *covolume* of Λ is $\mathrm{Vol}(P_{v_1,\ldots,v_m})$

Theorem 6.6. $\mathcal{O}_K$ *embeds as a full rank lattice in* $K_{\mathbb{R}}$ *of covolume* $\sqrt{|\Delta(\mathcal{O}_K)|}$

Proof. Let $\omega_1, \ldots, \omega_n$ be a basis for $\mathcal{O}_K$. Put $\sigma(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_n(\alpha)) \in K_{\mathbb{R}} \subset \mathbb{C}^n$ for all $\alpha \in K$. We have the vectors $\sigma(\omega_1), \ldots, \sigma(\omega_n) \in K_{\mathbb{R}}$.

So we need to show that $\text{Vol}(P_{\sigma(\omega_1),\ldots,\sigma(\omega_n)}) = \sqrt{\Delta(\mathcal{O}_K)} \neq 0$. We have

$$\begin{aligned}
\text{Vol}(P_{\sigma(\omega_1),\ldots,\sigma(\omega_n)})^2 &= \det\Big((\langle\sigma(\omega_i),\sigma(\omega_j)\rangle)_{ij}\Big) \\
&= \det\left(\left(\sum_{k=1}^{n}\sigma_k(\omega_i)\sigma_k(\omega_j)\right)_{ij}\right) \\
&= \det\left(\left(\sum_{k=1}^{n}\sigma_k(\omega_i\omega_j\right)_{ij}\right) \\
&= \det\Big((\text{Tr}(\omega_i\omega_j)_{ij}\Big) \\
&= \Delta(\mathcal{O}_K)
\end{aligned}$$

□

Corollary 6.7. *For any non-zero ideal $I \subset \mathcal{O}_K$, we have $\sigma(I) \subset K_{\mathbb{R}}$ is a full rank lattice of covolume $\sqrt{|\Delta(\mathcal{O}_K)|} \cdot N(I)$*

Proof. Obvious □

Minkowski's Theorem. *Let Λ be a full rank lattice in a Euclidean space V of dimension n. Let $X \subset V$ be a bounded convex symmetric subset, satisfying Vol$(X) > 2^n \cdot$ covolume(Λ). Then X contains a non-zero point of Λ.*

Proof. See Topics in Number Theory course □

A small refinement to the theorem can be made: If X is closed then $\text{Vol}(X) \geq 2^n \cdot \text{covolume}(\Lambda)$ suffices.

6.2 Class Number

Theorem 6.8. *Let K be a number field of signature (r,s). Then every non-zero ideal I of $\mathcal{O}_K$ contains a non-zero element α with*

$$|N(\alpha)| \leq \left(\frac{2}{\pi}\right)^s N(I)\sqrt{|\Delta(\mathcal{O}_K)|}$$

Proof. Let $n = r + 2s = [K : \mathbb{Q}]$. Consider for $t \in \mathbb{R}_{>0}$, the closed set $X_t = \{(z_1,\ldots,z_n) \in K_{\mathbb{R}} : |z_i| \leq t\}$. We claim that $\text{Vol}(X_t) = 2^{r+s}\pi^s t^n$

In terms of the orthogonal basis, X_t is isomorphic to $[-t,t]^r \times B(0,\sqrt{2}t)^s$ (where $B(a,r)$ is the standard notation for a ball of radius r centred at a, there is some bit of work need to see that the radius is indeed $\sqrt{2}t$). So

$$\begin{aligned}
\text{Vol}(X_t) &= (2t)^2((\pi(\sqrt{2}t)^2)^s \\
&= 2^r t^r \pi^s 2^s t^{2s} \\
&= 2^{r+s}\pi^s t^{r+2s}
\end{aligned}$$

Now choose t such that $\text{Vol}(X_t) = 2^n\text{covolume}(I \text{ in } K_{\mathbb{R}}) = 2^n N(I)\sqrt{|\Delta(\mathcal{O}_K)|}$. Then by Minkwoski's there is an $0 \neq \alpha \in I$ with $\sigma(\alpha) \in X_t$. So $|N(\alpha)| = \prod|\sigma_i(\alpha)| \leq t^n$, but since $s^{r+s}\pi^s t^n = 2^n N(I)\sqrt{|\Delta(\mathcal{O}_K)|}$, we have $|N(\alpha)| \leq t^n = \frac{2^s}{\pi^s}N(I)\sqrt{|\Delta(\mathcal{O}_K)|}$ □

A better set for the above proof is $X'_t = \{(z_1,\ldots,z_n) \in K_{\mathbb{R}} : |z_1| + \cdots + |z_n| \leq t\}$. In that case we have $\text{Vol}(X'_t) = \frac{2^r\pi^s t^n}{n!}$. This can be proven using integral calculus.

Theorem 6.9. *Every ideal $I \subset \mathcal{O}_K$ has an element $\alpha \neq 0$ with $|N(\alpha)| \leq \mu_K N(I)$ with*

$$\mu_K = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\sqrt{|\Delta(\mathcal{O}_K)|}$$

Proof. Choose t with $\mathrm{Vol}(X_t') = 2^n N(I)\sqrt{|\Delta(\mathcal{O}_K)|}$, that is $\frac{2^r \pi^s t^n}{n!} = 2^n N(I)\sqrt{|\Delta(\mathcal{O}_K)|}$. Then there exists $0 \neq \alpha \in I$ with $\sigma(\alpha) \in X_t'$. Hence

$$\begin{aligned}
|N(\alpha)| &= \prod |\sigma_i(\alpha)| \\
&\leq \left(\frac{\sum |\sigma_i(\alpha)|}{n}\right)^n \\
&\leq \left(\frac{t}{n}\right)^n \\
&= \frac{1}{n^n} n! 2^{n-r} \pi^{-s} N(I)\sqrt{|\Delta(\mathcal{O}_K)|} \\
&= \frac{4^s}{\pi^s}\frac{n!}{n^n} N(I)\sqrt{|\Delta(\mathcal{O}_K)|}
\end{aligned}$$

where the first inequality follows form the well know theorem that Geometric Mean $\leq$ Arithmetic Mean. (If $x_1, \dots, x_n \in \mathbb{R}_{>0}$, then the Geometric mean is $(x_1, \dots, x_n)^{1/n}$, while the arithmetic mean is $\frac{1}{n}(x_1 + \cdots + x_n)$) $\square$

Remark. The number μ_K is sometimes called *Minkowski's constant.*

Theorem 6.10. *For any number field K we have*

$$|\Delta(\mathcal{O}_K)| \leq \left(\frac{\pi}{4}\right)^{2s}\left(\frac{n^n}{n!}\right)^2$$

Proof. Apply the above with $I = \mathcal{O}_K$. Then there exists $\alpha \in \mathcal{O}_K$ with $|N(\alpha)| \leq \mu_K$. Also $N(\alpha) \in \mathbb{Z}$ and non-zero if $\alpha \neq 0$. So $|N(\alpha)| \geq 1$. Hence

$$\mu_K = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\sqrt{|\Delta(\mathcal{O}_K)|} \geq 1 \Rightarrow |\Delta(\mathcal{O}_K)| \leq \left(\frac{\pi}{4}\right)^{2s}\left(\frac{n^n}{n!}\right)^2$$

$\square$

Corollary 6.11. *If $K \neq \mathbb{Q}$, then $|\Delta(\mathcal{O}_K)| \neq 1$*

Proof. We have $n \geq 2$. We need to show that $\left(\frac{\pi}{4}\right)^{2s}\left(\frac{n^n}{n!}\right)^2 > 1$. Now $\left(\frac{\pi}{4}\right)^{2s} \geq \left(\frac{\pi}{4}\right)^n$, so we need to show $\left(\frac{\pi}{4}\right)^n\left(\frac{n^n}{n!}\right)^2 > 1$. This can easily be done by induction. $\square$

Corollary 6.12. *Let K be a number field and let C be an ideal class of K. Then there exists $I \in C$ with $N(I) \leq \mu_K$*

Proof. Apply Theorem 6.9 to an ideal $J \in C^{-1}$. (Note: if $J \in C^{-1}$ is any fractional ideal there is an $a \in \mathcal{O}_K$ with $aJ \subset \mathcal{O}_K$, since $aJ \in C^{-1}$ we may suppose without lose of generality that J is an ideal).

So there exists $\alpha \in J$ with $|N(\alpha)| \leq \mu_k N(J)$. Consider $(\alpha)J^{-1}$, we have $J|(\alpha)$ so $I := (\alpha)J^{-1}$ is an ideal of $\mathcal{O}_K$. Furthermore $N(I) = N((\alpha))N(J^{-1}) \leq \mu_k N(J)N(J^{-1}) = \mu_k$ $\square$

Corollary 6.13. *The class group of any number field is finite.*

Proof. Every class is represented by an ideal of bounded norm and norms are in $\mathbb{Z}_{>0}$. So it suffices to show that for any $n \in \mathbb{Z}_{>0}$ we have$\#\{I \subset \mathcal{O}_K : N(I) = n\} < \infty$

Let $n \in \mathbb{Z}_{>0}$ be given and $I \subset \mathcal{O}_K$ be an ideal with $N(I) = n$. Factor n into primes, $n = p_1^{e_1}p_2^{e_2}\dots p_r^{e_r}$, and factor I into prime ideals $I = P_1^{f_1}P_2^{f_2}\dots P_s^{f_s}$. Then we have $N(I) = N(P_1)^{f_1}N(P_2)^{f_2}\dots N(P_s)^{f_s} = p_1^{e_1}\dots p_r^{e_r}$. By Kummer - Dedekind, for any p there exists finitely many prime ideals whose norms is a power of p. So there are finitely many prime ideals P whose norm is a power of one of the p_i. Furthermore if $N(P_i) = p_j^{e_j}$, then $f_i \leq e_j$, so there are finitely many possibilities. $\square$

Example.

- Let $K = \mathbb{Q}(\sqrt{-5})$, note that it has signature $(0, 1)$. Then we have

$$\mu_K = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\sqrt{|\Delta(\mathcal{O}_K)|} = \frac{4}{\pi}\frac{2}{4}\sqrt{4\cdot 5} = \frac{1}{\pi}\sqrt{80} < \frac{1}{3}\sqrt{81} = 3$$

  So every ideal class is represented by an ideal of norm at most 2. Let us work out the ideals of norm 2. By Kummer - Dedekind, we know $(2) = (2, 1+\sqrt{-5})^2$, and $N((2, 1+\sqrt{-5})) = 2$.

  We have seen before that $(2, 1+\sqrt{-5})$ is not principal. So there are two ideal class in $\mathcal{O}_K$. They are $[(1)], [(2, 1+\sqrt{-5})]$, so $h_k = 2 \Rightarrow \mathrm{Cl}_K \cong \mathbb{Z}/2\mathbb{Z}$

- Let $K = \mathbb{Q}(\sqrt{-19})$, note that is has signature $(0,1)$. Then we have

$$\mu_K = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\sqrt{|\Delta(\mathcal{O}_K)|} = \frac{4}{\pi}\frac{2}{4}\sqrt{19} = \frac{1}{\pi}\sqrt{76} < \frac{1}{3}\sqrt{81} = 3$$

  Also here, every ideal class is represented by an ideal of norm 1 or 2. Apply Kummer - Dedekind to factor (2). $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$, hence $f_\alpha = \left(x - \frac{1+\sqrt{-19}}{2}\right)\left(x - \frac{1-\sqrt{-19}}{2}\right) = x^2 - x + 5$. So $f \equiv x^2 + x + 1 \in \mathbb{F}_2[x]$, but this is an irreducible polynomial. So $(2) = (2, 0) = (2)$ is a prime ideal, of norm 4. Hence there are no ideals of norm 2.

  So $h_K = 1$, hence $\mathcal{O}_K$ is a PID.

- Let $K = \mathbb{Q}(\sqrt{-14})$, this has signature $(0,1)$. Then we have

$$\mu_K = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\sqrt{|\Delta(\mathcal{O}_K)|} = \frac{4}{\pi}\frac{2}{4}\sqrt{4\cdot 14} = \frac{1}{\pi}\sqrt{16\cdot 14} \leq \frac{1}{3}\sqrt{15^2} = 5$$

  So only ideals of norms at most 4 are of concern. Every ideal can be factored into prime ideals. So the class group is generated by classes represented by prime ideals of norm $\leq \mu_K$. Prime ideals of norm ≤ 4 are prime ideals dividing (2) or (3). Hence we apply Kummer - Dedekind. We have $f = x^2 + 14$

  - $p = 2$: $x^2 + 14 \equiv x^2 \mod 2$. So $(2) = (2, \sqrt{-14})^2 := P^2$. Note that $N(P) = 2$
  - $p = 3$: $x^2 + 14 \equiv x^2 - 1 \equiv (x-1)(x+1) \mod 3$. So $(3) = (3, \sqrt{-14} - 1)(3, \sqrt{-14} + 1) := QR$. Note that $N(Q) = N(R) = 3$

  So ideals of norms less than 4 are $(1), P, Q, R, P^2$. Note that P^2 is principal as it is (2), so $[P^2] = [(1)]$. Since $N(a + b\sqrt{-14}) = a^2 + 14b^2$ but 2 and 3 are not of this form, we have that P, Q, R are not principal. Also note that $QR = (3)$ so $[Q][R] = 1$

  We claim that $[(1)], [P], [Q], [R]$ are four distinct elements of the class group.

  Suppose that $[P] = [Q]$. Then $[Q][Q] = [P]^2 = 1 = [Q][R] \Rightarrow [Q] = [R]$. Furthermore, since $N(Q) = N(R) = 3$, if $[Q] = [R]$ then $[QR] = 1 = [QQ]$. Hence Q^2 is principal, $N(Q^2) = N(Q)^2 = 9$, so we need to solve $a^2 + 14b^2 = 9 \Rightarrow a = 3, b = 0$. Hence $Q^2 = (3) = QR \Rightarrow Q = R$. Which is a contradiction.

  This argument also showed $[Q] \neq [R]$. A similar argument shows that $[P] \neq [R]$.

  Hence we have that $h_K = 4$. (With not too much work we can show that $\mathrm{Cl}_K \cong \mathbb{Z}/4\mathbb{Z}$)

6.3 Dirichlet's Unit Theorem

Dirichlet's Unit Theorem. *Let K be a number field of signature (r,s). Let W be the group of roots of unity in K. Then W is finite, and $\mathcal{O}_K^* \cong W \times \mathbb{Z}^{r+s-1}$. That is, there exists $\eta_1, \dots, \eta_{r+s-1} \in \mathcal{O}_K^*$ such that every units in $\mathcal{O}_K$ can be uniquely written as $\omega \cdot \eta_1^{k_1} \cdot \dots \cdot \eta_{r+s-1}^{k_{r+s-1}}$ with $\omega \in W$ and $k_i \in \mathbb{Z}$.*

Example. Let $K = \mathbb{Q}(\sqrt{d})$ with $d > 0$ and square free. Then it has signature $(2,0)$, so $r + s - 1 = 1$. Also $W = \{\pm 1\}$. Hence $\mathcal{O}_K^* \cong W \times \mathbb{Z} = \{\pm 1\} \times \mathbb{Z} = \pm\epsilon_d^n$ (where ϵ_d is as in section 1)

If $K = \mathbb{Q}(\sqrt{d})$ with $d < 0$ square free, then it has signature $(0,1)$, so $\mathcal{O}_K^* = W$, which is finite (see next lemma)

Fact. *A subgroup $\Lambda \subset \mathbb{R}^n$ is a lattice if and only if for any $M \in \mathbb{R}_{>0}$ we have $[-M, M]^n \cap \Lambda$ is finite.*

Lemma 6.14. *The group W is finite.*

Proof. If $\omega \in W$, then for all $\sigma_i : K \hookrightarrow \mathbb{C}$ we have $\sigma_i(\omega)$ is a root of unity (if $\omega^n = 1$ then $\sigma_i(\omega)^n = 1$). So $\sigma(\omega) = (\sigma_1(\omega), \dots, \sigma_n(\omega)) \in \{(z_1, \dots, z_n) \in K_\mathbb{R} : |z_i| = 1\,\forall i\}$. This is a bounded subset of $K_\mathbb{R}$. Also $\omega \in \mathcal{O}_K$ as it satisfies some monic polynomial $x^n - 1 \in \mathbb{Z}[x]$. Hence $\sigma(W) \subset \sigma(\mathcal{O}_K) \cap$ bounded set, but $\sigma(\mathcal{O}_K)$ is a lattice, hence by the fact, $\sigma(W)$ is finite. $\square$

Proof of Dirichlet's Unit Theorem. Let $K_\mathbb{R}^* = \{(z_1, \dots, z_n) \in K_\mathbb{R} : z_i \neq 0\,\forall i\}$. We have $\mathcal{O}_K^* \hookrightarrow K^* \hookrightarrow K_\mathbb{R}^*$. We will use logarithms: define $\log : K_\mathbb{R}^* \to \mathbb{R}^n$ by $(z_1, \dots, z_n) \mapsto (\log|z_1|, \dots, \log|z_n|)$. This is a group homomorphism. Also define $L : \mathcal{O}_K^* \to \mathbb{R}^n$ by $\alpha \mapsto \log(\sigma(\alpha)) = (\log|\sigma_1(\alpha)|, \dots, \log|\sigma_n(\alpha)|)$, this is also a group homomorphism.

Lemma 6.15. $\ker(L) = W$

Proof. $\supset$: For all $\omega \in W$ and σ_i we have $|\sigma_i(\omega)| = 1$, so $\log|\sigma_i(\omega)| = 0$

$\subset$: Take $\alpha \in \ker(L)$. Then $\log|\sigma_i(\alpha)| = 0\,\forall i \Rightarrow |\sigma_i(\alpha)| = 1$ for all i. So α is in some finite set. For every n, we have $\alpha^n \in \ker(L)$ which is a finite set, so there are some $n > m$, with $\alpha^n = \alpha^m$ and $n \neq m$. Then $\alpha^{n-m} = 1$. □

Lemma 6.16. $\mathrm{im}(L)$ *is a lattice in* $\mathbb{R}^n$.

Proof. We must show that $[-M, M]^n \cap \mathrm{im}(L)$ is finite. Take $L(\alpha) = (x_1, \ldots, x_n) \in [-M, M]^n \cap \mathrm{im}(L)$ (where $\alpha \in \mathcal{O}_K^* \subset \mathcal{O}_K$) . We have for all i, $|\log|\sigma_i(\alpha)|| \leq M$, so $|\sigma_i(\alpha)| \leq e^M$, hence $\sigma(\alpha) \in$bounded set $\cap \sigma(\mathcal{O}_K) =$finite. So there are finitely many possibilities for α □

Put $\Lambda = L(\mathcal{O}_K^*) \subset \mathbb{R}^n$. Eventually, we have to show that $\mathrm{rk}(\Lambda) = r + s - 1$.

Lemma 6.17. *We have that* $\mathrm{rk}(\Lambda) \leq r + s - 1$

Proof. Order σ_i such that $\sigma_1, \ldots \sigma_r$ are real and $\sigma_{r+i} = \overline{\sigma_{r+s+i}}$for $i \in \{1, \ldots, s\}$. Take $\alpha \in \mathcal{O}_K^*$. Then for $i \in \{1, \ldots, s\}$ we have $\sigma_{r+i}(\alpha) = \overline{\sigma_{r+s+i}(\alpha)}$. Hence $\log|\sigma_{r+i}(\alpha)| = \log|\overline{\sigma_{r+s+i}(\alpha)}| = \log|\sigma_{r+s+i}(\alpha)|$. So for $(x_1, \ldots, x_n) \in \Lambda$, we have $x_{r+i} = x_{r+s+i}$ for $i \in \{1, \ldots, s\}$. Hence we have found s relations. So $\Lambda \subset$subspace of dimension $n - r = r + 2s - s = r + s$

So we need to find one extra relation. Now α is a unit, so $|N(\alpha)| = 1$. So $|N(\alpha)| = |\sigma_1(\alpha) \ldots \sigma_n(\alpha)| = |\sigma_1(\alpha)| \ldots |\sigma_n(\alpha)| = 1 \Rightarrow \log|\sigma_1(\alpha)| + \cdots + \log|\sigma_n(\alpha)| = 0$. So we have also the relation $x_1 + \cdots + x_n = 0$. this shows $\Lambda \subset V \subset \mathbb{R}^n$, where V is a subspace of dimension $r + s - 1$ defined by these relations. □

So we are left to prove that $\mathrm{rk}(\Lambda) \geq r + s - 1$ or Λ is a full rank lattice in V.

Note that for $\alpha \in \mathcal{O}_K^*$, we have $\sigma_1(\alpha) \ldots \sigma_n(\alpha) = \pm 1$. So $\sigma(\mathcal{O}_K^*) \subset \{(z_1, \ldots, z_n) \in K_{\mathbb{R}}^* : z_1 \ldots z_n = \pm 1\} =: E$. We have to construct lots of units:

The idea: if $(\alpha) = (\beta)$ then β/α is a unit. So we will construct lots of $\alpha \in \mathcal{O}_K$ by generating finitely many ideals. Consider $X_t = \{(z_1, \ldots, z_n) \in K_{\mathbb{R}} : |z_i| \leq t\}$. Choose t such that $\mathrm{Vol}(X_t) = 2^n\sqrt{|\Delta(\mathcal{O}_K)|}$. Then by Minkowski's theorem, there exists a non-zero element in $\sigma(\mathcal{O}_K) \cap X_t$.

For any $e \in E$, consider $eX_t = \{(z_1, \ldots, z_n) \in K_{\mathbb{R}} : |z_i| < |e_i|t\}$. Then $\mathrm{Vol}(eX_t) = |e_1 \ldots e_n|\mathrm{Vol}(X_t) = \mathrm{Vol}(X_t)$. So by Minkowski's there exists a non-zero element in $\sigma(\mathcal{O}_K) \cap eX_t$. Covering E with boxes eX_t means we get lots of elements $a_e \in \sigma(\mathcal{O}_K) \cap eX_t\,\forall e \in E$. We have $|N(a_e)| = \prod|\sigma_i(a_e)| \leq \prod|e_i|t \leq t^n$. So the norms of a_e are bounded, hence $N((a_e)) = |N(a_e)|$ is bounded.

So the set of ideals $\{(a_e) : e \in E\}$ is finite. Let $b_1, \ldots, b_m$ be such that $\{(a_e) : e \in E\} = \{(b_1), \ldots, (b_m)\}$. For all $e \in E$ there is some $i \in \{1, \ldots, m\}$ such that $(a_e) = (b_i)$. So $U_e = a_e/b_i$ is a unit of $\mathcal{O}_K$.

Claim: $S = \{U_e : e \in E\}$ generates a full rank lattice in V, after applying L. If $\langle L(S)\rangle$ is not of full rank, then $L(S)$ spans a subspace $Z \not\subseteq V$. Consider $Y := \cup(b_i^{-1} \cdot X_t) \subset K_{\mathbb{R}}$, it is bounded and without loss of generality we can choose it, such that $\sigma(1) \in Y$. Consider $\cup_{e \in E} U_e^{-1} \cdot Y$ (all of these are bounded) We want to show that $e^{-1} \in U_e^{-1}Y = \frac{b_i}{a_e} \cdot Y$. By construction, $b_i \cdot Y \supset X_t$, so $\frac{b_i}{a_e} \cdot Y \supset \frac{1}{a_e} \cdot X_t$. We have $a_e \in eX_t$, so $\frac{1}{e} \in \frac{1}{a_e}X_t$. Hence $\cup_{e \in E} U_e^{-1}$ contains E. So $V = \cup_{s \in S}\log(s) + \log(Y)$. We are assuming $\log(s) \in Z$ and $\log(Y)$ is bounded. If $Z \neq V$ then V is at some bounded distance from Z. This proves that $\langle L(S)\rangle$ is of full rank.

So $L(\mathcal{O}_K^*)$ is a full rank lattice in V. Hence it has rank $r + s - 1$, i.e., $L(\mathcal{O}_K^*) \cong \mathbb{Z}^{r+s-1}$

Lemma 6.18. *Let A be an abelian group, let $A' \subset A$ be a subgroup and put $A'' = A/A'$. If A'' is free (i.e., $\cong \mathbb{Z}^n$ for some n), then $A \cong A' \times A''$*

Proof. Omitted, but can be found in any algebra course. □

In our case, we have $A = \mathcal{O}_K^*$ and $A' = W$. Then by the first isomorphism theorem $A'' \cong L(\mathcal{O}_K^*)$ (as $W = \ker(L)$). So using the lemma, we have $A \cong W \times L(\mathcal{O}_K^*) \cong L \times \mathbb{Z}^{r+s-1}$ as required.

□