Internship Report

Introduction to Algebraic Number Theory

Pierre Le Barbenchon

Supervisor : Konstantin Ardakov
Mathematical Institute, Oxford

June 4th 2018 — July 15th 2018

Contents

1 Foreword

1.1 Introduction

The title may be understood in two ways. The first one is the study of Number Theory in an algebraic point of view and the second is the study of algebraic numbers and all the linked theory. We will see both interpretations in this research document.

All the theory is presented along with exercises which are from the first edition of *Algebraic Number Theory* by Ian STEWART and David TALL. However the solutions are the result of an internship in Oxford with Konstantin Ardakov. We can consider this article as placing in context these exercises.

If a theorem or property is not demonstrated in this article, it is because the demonstration is already detailled in *Algebraic Number Theory*. Conversely, all the demonstrations in this article are not explicitly in *Algebraic Number Theory*.

1.2 Notations

- $\mathbb{Z}$ is the set of integers
- $\mathbb{Q}$ is the set of rationals
- L/K is the field extension L of K (K and L are fields)
- $K(\alpha_1, ...\alpha_n)$ is the least field that contains the field K and the elements $\alpha_1, ..., \alpha_n$
- $[L : K]$ is the degree of the extension L over K
- ∂P is the degree of the polynomial P
- $\mathfrak{O}_K$ is the ring of integers of the number field K
- $\lfloor x \rfloor$ is the integer part of x, we have $\lfloor x \rfloor \leqslant x < \lfloor x \rfloor + 1$.
- $a \equiv b\ [n]$ is equivalent to $a \equiv b \pmod{n}$, i.e. $n \mid (a - b)$.
- $\mathrm{Im}(\varphi)$ is the image of φ.
- $\mathrm{Ker}(\varphi)$ is the kernel of φ.
- $\varphi : A \hookrightarrow B$ implies that φ is injective.
- $\varphi : A \twoheadrightarrow B$ implies that φ is surjective.
- $[\![1, n]\!]$ is equivalent to $\{1, 2, ..., n\}$.
- $A \backslash B$ is the set of the elements that are in A but not in B.
- $\langle p \rangle$ in a ring A is the ideal generated by p in the ring A.

1.3 Theory Prerequisites

- Groups, rings, domains, fields, morphisms
- Background in fields extension
- Free Abelian Group
- Galois Theory
- Ideals of a ring
- Modules of a ring
- Noetherian notion and the equivalences of the definition

- Primes and irreducibles in a ring
- Chinese Remainder Theorem
- Correspondence Theorem for Ideals
- First Isomorphism Theorem

2 Field extensions and number field

Let K be a field, the motivation of extending the field K is to find a bigger field which contains zeros of polynomials on K. For example, $\mathbb{Q}(i)$, which is the least field that contains i and $\mathbb{Q}$, is an extension of $\mathbb{Q}$ that contains zeros of X^2+1 (they are not contained in $\mathbb{Q}$).

2.1 Definitions

Definition 2.1 (Algebraic number)**.** An element α is called *algebraic* over K if there exists a polynomial P over K such that $P(\alpha)=0$.

Definition 2.2 (Minimum polynomial)**.** Let α be an element of a field K, a polynomial P over K is called the *minimum polynomial* of α if $P(\alpha)=0$, the degree of P is as least as possible and the leading coefficient is 1.

Remark 2.3. The minimum polynomial is unique by definition.

Let us remind that a field extension L/K has a natural structure of vector space over K (with the addition in L and scalar multiplication of $\alpha \in K$ on $x \in L$ is just $\alpha x \in L$).

Definition 2.4 (Degree of extension)**.** The *degree of an extension* L over K is the dimension of the vector space L over K, written $[L:K]$.

Proposition 2.5. Let α be an algebraic element over $\mathbb{Q}$ and n be the degree of the minimum polynomial of α over $\mathbb{Q}$. Then $\{1, \alpha, ..., \alpha^{n-1}\}$ is a $\mathbb{Q}-$basis of $\mathbb{Q}(\alpha)$.

Proof. Let $P = \sum_{i=0}^{n} a_i \alpha^i$, where $a_n = 1$, the minimum polynomial of α over $\mathbb{Q}$ which is of degree n. We want to prove that $B = \{1, \alpha, ..., \alpha^{n-1}\}$ is a $\mathbb{Q}-$basis of $\mathbb{Q}(\alpha)$. The family $\{1, \alpha, ..., \alpha^{n-1}\}$ is $\mathbb{Q}-$independant because, if we cannot have $b_0 + b_1\alpha + ... + b_{n-1}\alpha^{n-1} = 0$ (unless all $b_i = 0$) because the minimum polynomial is of degree n. Then B generates $\mathbb{Q}(\alpha)$ because, $\mathbb{Q}$ is generated by 1, hence by B, α is generated by α, hence by B, all the linear combinations are generated by B by definition of space vector, all α^i is generated by B because we have $\alpha^n = -\sum_{i=0}^{n-1} a_i \alpha^i$, then for all α^p with $p \geqslant n$ we can rewrite it with elements of the form $\sum_{i=0}^{n-1} b_i \alpha^i$. We therefore can write all linear combinations

of power of α. Then we must prove that we can write the inverse of linear combination with the basis B. We know that there exists an inverse of $\sum_{i=0}^{n-1} b_i\alpha^i$ of the form $\sum_{i=0}^{n-1} c_i\alpha^i$ if and only if b_0 is a unit (it is just an easy exercise). So we only have to study the case $b_0 = 0$. There exists $k > 0$ such that $b_k \neq 0$ then we take the least $0 < k \leqslant n$ such that $b_k \neq 0$, now factorize by α^i, we have $\sum_{i=k}^{n-1} b_i\alpha^i = \alpha^k \sum_{i=k}^{n-1} b_i\alpha^i - k$ and now the coefficient of α^0 is not equal to zero. So we have an inverse for $\sum_{i=k}^{n-1} b_i\alpha^i - k$, and we have to find an inverse for α^k where $k > 0$. $\frac{1}{\alpha^k} = \frac{\alpha^{n-k}}{\alpha^k\alpha^{n-k}} = \frac{\alpha^{n-k}}{\alpha^n} = \frac{\alpha^{n-k}}{-\sum_{i=0}^{n-1} a_i\alpha^i}$ and it exists if and only if $a_0 \neq 0$, but $a_0 \neq 0$ because $\sum_{i=0}^{n} a_i\alpha^i$ is the minimum polynomial of α and if $a_0 = 0$ then we can factorize it by α and since $\alpha \neq 0$ we would have $\sum_{i=1}^{n} a_i\alpha^{i-1} = 0$ but it is a contradiction with P is the minimum polynomial of α. It follows that we have found an inverse. Then all elements of $\mathbb{Q}(\alpha)$ can be written with the basis B. It follows that B is well a basis of $\mathbb{Q}(\alpha)$ □

Proposition 2.6. Let α be an algebraic element over $\mathbb{Q}$. Then the degree of $\mathbb{Q}(\alpha)/\mathbb{Q}$ is equal to the degree of the minimum polynomial of α over $\mathbb{Q}$.

Proof. Let n be the degree of the minimum polynomial of α over $\mathbb{Q}$. Since Proposition 2.5, $B = \{1, \alpha, ..., \alpha^{n-1}\}$ is a $\mathbb{Q}-$basis of $\mathbb{Q}(\alpha)$. There are n elements in B then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$. □

If $[L : K]$ is finite, we say that L is a finite extension of K. Hence, we have a $K-$basis of L and the cardinal of this basis is $[L : K]$.

Now, unless otherwise specified, we will work with the extensions of the form $\mathbb{Q}(\alpha_1, ..., \alpha_n)$ where $\alpha_i \in \mathbb{C}$. Then all the extensions that we will see are subfields of $\mathbb{C}$.

Definition 2.7 (Number field)**.** A field K is a *number field* if $[K : \mathbb{Q}]$ is finite.

Remark 2.8. We could say that a number field is a finite extension over $\mathbb{Q}$.

Theorem 2.9. If K is a number field then $K = \mathbb{Q}(\theta)$ for some algebraic number θ.

Proof. You can find a proof in [1] (Theorem 2.2 of [1]). □

Exercise 2.2.
Express $\mathbb{Q}(\sqrt{3}, \sqrt[3]{5})$ in the form $\mathbb{Q}(\theta)$.

Solution 2.2.
Let θ be $\sqrt{3} + \sqrt[3]{5}$. We want to prove that $\mathbb{Q}(\sqrt{3}, \sqrt[3]{5}) = \mathbb{Q}(\theta)$. $\theta \in \mathbb{Q}(\sqrt{3}, \sqrt[3]{5})$ because it is a field that contains $\sqrt{3}$ and $\sqrt[3]{5}$. So $\mathbb{Q}(\theta) \subset \mathbb{Q}(\sqrt{3}, \sqrt[3]{5})$. For the other inclusion, we can see that $\sqrt{3} = \frac{1}{267}(8\theta^5 + 5\theta^4 - 80\theta^3 - 130\theta^2 + 335\theta - 455)$ and $\sqrt[3]{5} = \frac{1}{267}(-8\theta^5 - 5\theta^4 + 80\theta^3 + 130\theta^2 - 68\theta + 455)$ (it takes a while to obtain those polynomials) , so we have $\sqrt{3}$ and $\sqrt[3]{5} \in \mathbb{Q}(\theta)$. It follows that $\mathbb{Q}(\sqrt{3}, \sqrt[3]{5}) \subset \mathbb{Q}(\theta)$ and now $\mathbb{Q}(\sqrt{3}, \sqrt[3]{5}) = \mathbb{Q}(\theta)$.

2.2 Correspondence of Galois

We can use Galois theory to find the subfields of an extension field while using the Galois groups. There is a correspondence reverse inclusions between the subgroup of the Galois group and the subfield of the extension. You can find further details in the Chapter 12 and 13 in *Galois Theory* by Ian STEWART (Reference [2]).

Exercise 0.1.
Find all the subfields of $\mathbb{Q}(\zeta)$ where $\zeta = e^{2\pi i/5}$

Solution.
$1 + X + X^2 + X^3 + X^4$ is the minimum polynomial of $\mathbb{Q}(\zeta)$ (Lemma 3.4 of [1]), hence there are 4 monomorphisms (Theorem 2.3 of [1]): $\phi_1 : \zeta \mapsto \zeta$, $\phi_2 : \zeta \mapsto \zeta^2$, $\phi_3 : \zeta \mapsto \zeta^3$, $\phi_4 : \zeta \mapsto \zeta^4$. Then $2 \equiv 2$ [5], $2^2 \equiv 4$ [5], $2^3 \equiv 3$ [5], $2^4 \equiv 1$ [5]. Now let σ be $\zeta \mapsto \zeta^2$, we have $\phi_1 = \sigma^4$, $\phi_2 = \sigma$, $\phi_3 = \sigma^3$, $\phi_4 = \sigma^2$. It follows that the Galois group of $\mathbb{Q}(\zeta)$ is $\langle\sigma\rangle \simeq \mathbb{Z}/4\mathbb{Z}$.
The subgroup of $\mathbb{Z}/4\mathbb{Z}$ are $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$ and $\langle e\rangle$ where e is the neutral element. $\mathbb{Z}/2\mathbb{Z} \simeq \langle\sigma^2\rangle$, hence we want to find the subfield that corresponds to $\langle\sigma^2\rangle$. We have to calculate the fixed field of $\langle\sigma^2\rangle$. Let us take $\alpha = \zeta + \zeta^4$ and $\beta = \zeta^2 + \zeta^3$ we have $\sigma(\alpha) = \beta$ and $\sigma(\beta) = \alpha$, it follows that $\sigma^2(\alpha) = \alpha$ and $\sigma^2(\beta) = \beta$. So the fixed field is $\mathbb{Q}(\alpha, \beta)$ but we can write it with a better expression (we can just write it $\mathbb{Q}(\alpha)$, because $\beta = -1 - \alpha$, since $1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 = 0$ but we can still find better). $\alpha + \beta = -1$ and $\alpha\beta = -1$, it follows that α and β are solutions of $X^2 + X - 1$, but $\Delta = 1 + 4 = 5$, hence the solutions are $\frac{-1 \pm \sqrt{5}}{2}$. Then the subfield we are looking for is $\mathbb{Q}(\sqrt{5})$.

$$\begin{array}{cc} \mathbb{Q}(\zeta) & \langle e\rangle \\ \vdots & \vdots \\ \mathbb{Q}(\sqrt{5}) & \mathbb{Z}/2\mathbb{Z} \\ \vdots & \vdots \\ \mathbb{Q} & \mathbb{Z}/4\mathbb{Z} \end{array}$$

There are 3 subfields of $\mathbb{Q}(\zeta)$ which are $\mathbb{Q}$, $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\zeta)$.

2.3 Norm and Trace

Now, unless otherwise specified, we will work with number fields, hence we can write it $\mathbb{Q}(\theta)$ due to the Theorem 2.9.

Definition 2.10 (Monomorphism)**.** Let K be a number field, a *monomorphism* is an injective homomorphism $\sigma : K \to \mathbb{C}$ such that $\sigma_{|\mathbb{Q}} = \mathrm{Id}_{|\mathbb{Q}}$.

Proposition 2.11. Let $K = \mathbb{Q}(\theta)$ be a number field of degree n over $\mathbb{Q}$. Then there are exactly n distinct monomorphisms $\sigma_i : K \to \mathbb{C}$ for i in $\{1, ...n\}$. The elements $\sigma_i(\theta) = \theta_i$ are the distinct zeros in $\mathbb{C}$ of the minimum polynomial of θ over $\mathbb{Q}$.

Proof. You can find a proof in [1] (Theorem 2.3 of [1]). □

Definition 2.12 (Conjugates)**.** Let $K = \mathbb{Q}(\theta)$ of degree n, $\alpha \in K$, σ_i all the monomorphisms. Then we call $\sigma_i(\alpha)$ for $i = 1, ..., n$ the $K-$*conjugates* of α.

Remark 2.13. All the conjugates of an element θ are not necessarily in the field K, for example, in $\mathbb{Q}(\sqrt[3]{2})$, all the elements are real, but the conjugates of $\sqrt[3]{2}$ are $\sqrt[3]{2}$, $j\sqrt[3]{2}$ and $j^2\sqrt[3]{2}$, where $j = e^{2\pi i/3} \in \mathbb{C}$.

Exercise 2.3.
Find all monomorphisms $\mathbb{Q}(\sqrt[3]{7}) \to \mathbb{C}$.

Solution.
We use the Proposition 2.11, then there are 3 monomorphisms $\sigma : \mathbb{Q}(\sqrt[3]{7}) \to \mathbb{C}$, because $X^3 - 7$ is the minimum polynomial over $\mathbb{Q}$ of $\sqrt[3]{7}$.

$$\begin{array}{ll} \sqrt[3]{7} \mapsto \sqrt[3]{7} & \text{(Identity function)} \\ \sqrt[3]{7} \mapsto j\sqrt[3]{7} & \\ \sqrt[3]{7} \mapsto j^2\sqrt[3]{7} & \end{array}$$

where $j = e^{2\pi i/3}$. They are the conjugates of $\sqrt[3]{7}$ (complex roots of $X^3 - 7$). (We remind that $\sigma_{|\mathbb{Q}} = I_{d|\mathbb{Q}}$)

Definition 2.14 (Discriminant)**.** Let $K = \mathbb{Q}(\theta)$ of degree n, let $\{\alpha_1, ..., \alpha_n\}$ be a basis of K. The *discriminant* is defined to be

$$\Delta[\alpha_1, ..., \alpha_n] = \big(\det(\sigma_i(\alpha_j))\big)^2$$

Proposition 2.15. The discriminant of any basis for $K = \mathbb{Q}(\theta)$ is rational and non-zero.

Proof. You can find a proof in [1] (Theorem 2.6 of [1]). □

Definition 2.16 (Norm)**.** Let $K = \mathbb{Q}(\theta)$ be a number field of degree n. Let $\alpha \in K$. We define the *norm* as

$$N_K(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha).$$

In other words, the norm is the product of all the conjugates of α.

Definition 2.17 (Trace)**.** Let $K = \mathbb{Q}(\theta)$ be a number field of degree n. Let $\alpha \in K$. We define the *trace* as

$$T_K(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha).$$

In other words, the trace is the sum of all the conjugates of α.

Proposition 2.18. The norm is multiplicative and the trace is $\mathbb{Q}-$linear, i.e. for $\alpha, \beta \in K$ and $p, q \in \mathbb{Q}$ we have $N_K(\alpha\beta) = N(\alpha)N(\beta)$ and $T_K(p\alpha + q\beta) = pT_K(\alpha) + qT_K(\beta)$.

Proof. It follows from the definition of norm and trace and the properties of the monomorphisms. $N_K(\alpha\beta) = \prod \sigma_i(\alpha\beta) = \prod \sigma_i(\alpha)\sigma_i(\beta) = N_K(\alpha)N_K(\beta)$. $T_K(p\alpha + q\beta) = \sum \sigma_i(p\alpha + q\beta) = \sum(\sigma_i(p)\sigma_i(\alpha) + \sigma_i(q)\sigma_i(\beta)) = \sum(p\sigma_i(\alpha) + q\sigma_i(\beta)) = pT_K(\alpha) + qT_K(\beta)$. □

Remark 2.19. The norm and trace depend on K, we will write $N(\alpha)$ and $T(\alpha)$ if the number field K is obvious in the context.

Exercise 2.12.
Give examples to show that for fixed α, $N_K(\alpha)$ and $T_K(\alpha)$ depend on K. (This is to emphasize that the norm and trace must always be defined in the context of a specific field K; there is no such thing as the norm or trace of α without a specified field.)

Solution.
Let us consider the field $K_1 = \mathbb{Q}(\sqrt{2})$ and the element $\alpha = 1 + \sqrt{2} \in K_1$. The monomorphisms of K_1 are $\sigma_1 : \sqrt{2} \mapsto \sqrt{2}$ and $\sigma_2 : \sqrt{2} \mapsto -\sqrt{2}$, so $N_{K_1}(1+\sqrt{2}) = \sigma_1(1+\sqrt{2})\sigma_2(1+\sqrt{2}) = (1+\sqrt{2})(1-\sqrt{2}) = 1 - 2 = -1$ and $T_{K_1}(1+\sqrt{2}) = \sigma_1(1+\sqrt{2}) + \sigma_2(1+\sqrt{2}) = (1+\sqrt{2}) + (1-\sqrt{2}) = 2$.
Then, let consider the field $K_2 = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and still the element $\alpha = 1 + \sqrt{2} \in K_2$. The monomorphisms of K_2 are

$$\begin{array}{ll} \sigma_1 : \sqrt{2} \mapsto \sqrt{2} & \sigma_1 : \sqrt{3} \mapsto \sqrt{3} \\ \sigma_2 : \sqrt{2} \mapsto -\sqrt{2} & \sigma_2 : \sqrt{3} \mapsto \sqrt{3} \\ \sigma_3 : \sqrt{2} \mapsto \sqrt{2} & \sigma_3 : \sqrt{3} \mapsto -\sqrt{3} \\ \sigma_4 : \sqrt{2} \mapsto -\sqrt{2} & \sigma_4 : \sqrt{3} \mapsto -\sqrt{3} \end{array}$$

so $N_{K_2}(1+\sqrt{2}) = \sigma_1(1+\sqrt{2})\sigma_2(1+\sqrt{2})\sigma_3(1+\sqrt{2})\sigma_4(1+\sqrt{2}) = (1+\sqrt{2})(1-\sqrt{2})(1+\sqrt{2})(1-\sqrt{2}) = (-1)^2 = 1$ and $T_{K_2}(1+\sqrt{2}) = \sigma_1(1+\sqrt{2}) + \sigma_2(1+\sqrt{2}) + \sigma_3(1+\sqrt{2}) + \sigma_4(1+\sqrt{2}) = (1+\sqrt{2}) + (1-\sqrt{2}) + (1+\sqrt{2}) + (1-\sqrt{2}) = 4$.
We see that $N_{K_1}(\alpha) = -1$, $N_{K_2}(\alpha) = 1$ and $T_{K_1}(\alpha) = 2$, $T_{K_2}(\alpha) = 4$ □

Remark 2.20. We consider monomorphisms σ such that $\sigma_{|\mathbb{Q}} = \mathrm{Id}_{|\mathbb{Q}}$ because we work with number field (finite extension over $\mathbb{Q}$) but we may be generalized the norm and trace on other extension field K/L. We explain that generalization in Exercise 2.13 and use it in Exercise 4.14.

Exercise 2.13.
The norm and trace may be generalized by condiering number field $K \supseteq L$. Suppose $K = L(\theta)$ and $[K : L] = n$. Consider monomorphisms $\sigma : K \to \mathbb{C}$ such that $\sigma(x) = x$ for all $x \in L$. Show that there are precisely n such monomorphisms $\sigma_1, ..., \sigma_n$ and describe them. For $\alpha \in K$, define

$$N_{K/L}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha),$$
$$T_{K/L}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha).$$

(Compared with our earlier notation, we have $N_K = N_{K/\mathbb{Q}}, T_K = T_{K/\mathbb{Q}}$.) Prove that

$$N_{K/L}(\alpha_1\alpha_2) = N_{K/L}(\alpha_1)N_{K/L}(\alpha_2),$$
$$T_{K/L}(\alpha_1 + \alpha_2) = T_{K/L}(\alpha_1)T_{K/L}(\alpha_2).$$

Let $K = \mathbb{Q}(\sqrt[4]{3}), L = \mathbb{Q}(\sqrt{3})$. Calculate $N_{K/L}(\alpha), T_{K/L}(\alpha)$ for $\alpha = \sqrt[4]{3}$ and $\alpha = \sqrt[4]{3} + \sqrt{3}$.

Solution.
We just have to use the proof of the Proposition 2.11 (Theorem 2.3 of [1]) while replacing $\mathbb{Q}$ by L and so we have our n monomorphisms σ_i such that $\sigma_i(\theta) = \theta_i$ where θ_i are the $L-$conjugates of θ (the other zeros in L of the minimum ploynomial of θ in $L[X]$).

$$N_{K/L}(\alpha_1\alpha_2) = \prod_{i=1}^{n} \sigma_i(\alpha_1\alpha_2) = \prod_{i=1}^{n} \sigma_i(\alpha_1)\sigma_i(\alpha_2) = \prod_{i=1}^{n} \sigma_i(\alpha_1) \prod_{i=1}^{n} \sigma_i(\alpha_2) = N_{K/L}(\alpha_1)N_{K/L}(\alpha_2)$$

$$T_{K/L}(\alpha_1 + \alpha_2) = \sum_{i=1}^{n} \sigma_i(\alpha_1 + \alpha_2) = \sum_{i=1}^{n} \sigma_i(\alpha_1) + \sigma_i(\alpha_2) = T_{K/L}(\alpha_1) + T_{K/L}(\alpha_2)$$

$X^2 - \sqrt{3}$ is the minimum polynomial of $\sqrt[4]{3}$ in $L[X]$. Then $[K : L] = 2$ and there are 2 monomorphisms that are $\sigma_1 : \sqrt[4]{3} \mapsto \sqrt[4]{3}$ and $\sigma_2 : \sqrt[4]{3} \mapsto -\sqrt[4]{3}$. Calculate $N_{K/L}(\sqrt[4]{3})$ and $T_{K/L}(\sqrt[4]{3})$. $N_{K/L}(\sqrt[4]{3}) = \sigma_1(\sqrt[4]{3})\sigma_2(\sqrt[4]{3}) = -\sqrt{3}$ and $T_{K/L}(\sqrt[4]{3}) = \sigma_1(\sqrt[4]{3}) + \sigma_2(\sqrt[4]{3}) = 0$. Calculate $N_{K/L}(\sqrt[4]{3} + \sqrt{3})$ and $T_{K/L}(\sqrt[4]{3} + \sqrt{3})$. $N_{K/L}(\sqrt[4]{3} + \sqrt{3}) = \sigma_1(\sqrt[4]{3} + \sqrt{3})\sigma_2(\sqrt[4]{3} + \sqrt{3}) = (\sqrt{3} + \sqrt[4]{3})(\sqrt{3} - \sqrt[4]{3}) = 3 - \sqrt{3}$ and $T_{K/L}(\sqrt[4]{3} + \sqrt{3}) = \sigma_1(\sqrt[4]{3} + \sqrt{3}) + \sigma_2(\sqrt[4]{3} + \sqrt{3}) = 2\sqrt{3}$.

3 Algebraic Integers

3.1 Definition

Definition 3.1 (Algebraic integer)**.** An *algebraic integer* is an algebraic element that is solution of a monic polynomial with integer coefficients, i.e. α is an algebraic integer if there exists $n \in \mathbb{N}$ and $a_0, ..., a_{n-1} \in \mathbb{Z}$ such that $\alpha^n + a_{n-1}\alpha^{n-1} + ... + a_0 = 0$.

Remark 3.2. We will use the expression "rational integer" for the elements of $\mathbb{Z}$ to avoid confusion with algebraic integers.

Theorem 3.3. The algebraic integers form a subring of the field of algebraic numbers.

Proof. You can find a proof in [1] (Theorem 2.8 of [1]). □

Definition 3.4 (Ring of integers)**.** Let K be a number field. The *ring of integers* of K is the set of all the algebraic integers in K. It is a ring because K is a ring and the algebraic integers form a ring. We will write $\mathfrak{O}_K$ for the ring of integers of K.

Proposition 3.5. An algebraic integer is a rational number if and only if it is a rational integer, i.e. $\mathfrak{O}_{\mathbb{Q}} = \mathbb{Z}$.

Proof. You can find a proof in [1] (Lemma 2.13 of [1]). □

Proposition 3.6. Let K be a number field and let α be an algebraic integer of K. Then $T(\alpha)$ and $N(\alpha)$ are in $\mathbb{Z}$.

Proof. Let P_α an integer monic polynomial of α then for all monomorphism σ, $0 = \sigma(0) = \sigma(P_\alpha(\alpha)) = P_\alpha(\sigma(\alpha)) = 0$, hence $\sigma(\alpha)$ is an algebraic integer, then $N(\alpha)$ and $T(\alpha)$ are also algebraic integers because they are the product or the sum of $\sigma(\alpha)$ for all monomorphism σ and the algebraic integers form a ring. But the norm and the trace are always in $\mathbb{Q}$, because $N(\alpha) = (-1)^n f_\alpha(0)$ and $T(\alpha)$ is the coefficient of t^{n-1} of f_α which is a polynomial in $\mathbb{Q}$ (Theorem 2.4 of [1]) (f_α is the field polynomial introduce in [1] p.42). Then use Proposition 3.5 to see that $N(\alpha) \in \mathbb{Z}$. □

Remark 3.7. Let θ be an algebraic integer. The ring of integers of $K = \mathbb{Q}(\theta)$ is sometimes $\mathfrak{O}_K = \mathbb{Z}[\theta]$ but it is not always the case (We shall see examples in subsection *Quadratic fields*). However, we always have $\mathbb{Z}[\theta] \subset \mathfrak{O}_K$.

3.2 Integral Basis

Let K be a number field with $[K : \mathbb{Q}] = n$. There exists a $\mathbb{Q}-$basis of K. Let $\mathfrak{O}_K$ the ring of integers of K, we want to find a basis of $\mathfrak{O}_K$ such that all element of $\mathfrak{O}_K$ can be expressed in this basis and all element that could be generated by this basis is in $\mathfrak{O}_K$. This is possible because $\mathfrak{O}_K$ is a free abelian group under addition of rank n.

Definition 3.8 (Integral basis)**.** Let K be a number field of degree n. An *integral basis* of the ring of integers of K is a $\mathbb{Z}-$basis for $(\mathfrak{O}_K, +)$.

Theorem 3.9. Every number field $K$of degree n possesses an integral basis, and the additive group of $\mathfrak{O}_K$ is free abelian of rank n.

Proof. You can find a proof in [1] (Theorem 2.15 of [1]). □

Remark 3.10. The discriminant of an integral basis is an integer, since Proposition 2.15 and Proposition 3.5.

Definition 3.11 (Squarefree)**.** Let n be in $\mathbb{Z}$, n is said *squarefree*, if n is not divisible by the square of a prime number.

Theorem 3.12. Suppose $\alpha_1, ..., \alpha_n \in \mathfrak{O}$ form a $\mathbb{Q}-$basis for K. If $\Delta[\alpha_1, ..., \alpha_n]$ is squarefree then $\{\alpha_1, ...\alpha_n\}$ is an integral basis.

Proof. You can find a proof in [1] (Theorem 2.16 of [1]). □

Remark 3.13. Warning, we can find integral basis that have a discriminant which is not squarefree. We shall have examples in the subsection *Quadratic fields*.

Theorem 3.14. Let $B = \{b_1, b_2, ..., b_n\}$ be a $\mathbb{Q}-$basis of K a number field such that B is not an integral basis but $b_i \in \mathfrak{O}_K$ for all i in $[\![1, n]\!]$. Then there is an element $\alpha \in \mathfrak{O}_K$ that can be written in the following form:

$$\alpha = \frac{1}{p}(\lambda_1 b_1 + ... + \lambda_n b_n) \tag{1}$$

where p is a prime such that $p^2 \mid \Delta[b_1, ..., b_n]$, $\lambda_i \in [\![0; p-1]\!]$ and there exists λ_j such that $\lambda_j = 1$.

Proof. Take $\beta \in \mathfrak{O}_K \backslash (b_1\mathbb{Z} + ... + b_n\mathbb{Z})$ (this is possible because B is not an integral basis). We can write $\beta = \dfrac{1}{N}\displaystyle\sum_{i=1}^{n} c_i b_i$ with $c_i \in \mathbb{Z}, N \in \mathbb{Z}$, $N \notin \{\pm 1\}$ and $\text{hcf}(N, c_1, c_2, ..., c_n) = 1$. Let p a prime such that $p \mid N$ and it exists j such that $p \nmid c_j$. Take $\beta' = \dfrac{N}{p}\beta = \dfrac{1}{p}\displaystyle\sum_{i=1}^{n} c_i b_i \in \mathfrak{O}_K$ (because $p \mid N$). But $\text{hcf}(c_j, p) = 1$, then it exists $k, l \in \mathbb{Z}$ such that $c_j k + pl = 1$. Take $\beta'' = k\beta' + l b_j \in \mathfrak{O}_K$, $\beta'' = \dfrac{1}{p}\displaystyle\sum_{i=1}^{n} s_i b_i$ with $s_j = 1$. Use Euclidean division on s_i by p, then it exists m_i and λ_i such that $s_i = m_i p + \lambda_i$ with $\lambda_i \in [\![0, p-1]\!]$ and $\lambda_j = 1$ (because $s_j = 1$ and $m_j = 0$). Then take $\alpha = \beta'' - \sum m_i b_i = \dfrac{1}{p}\displaystyle\sum_{i=1}^{n} \lambda_i b_i$.

We finally have to prove that $p^2 \mid \Delta[b_1, ..., b_n]$. Take $B' = (B \backslash b_j) \cup \alpha$. The change of basis matrix is $C = \begin{bmatrix} 1 & 0 & & \lambda_1/p & & 0 \\ 0 & 1 & & \vdots & & 0 \\ \vdots & & \ddots & \vdots & & \vdots \\ 0 & & & \lambda_j/p & & \vdots \\ & \ddots & & \vdots & \ddots & 0 \\ 0 & & 0 & \lambda_n/p & & 1 \end{bmatrix}$, with $\det C = \pm\frac{1}{p}$.

Then $\Delta(B') = (\det C)^2 \Delta[b_1, ..., b_n] = \frac{1}{p^2}\Delta[b_1, ..., b_n]$, but $\Delta(B') \in \mathbb{Z}$ (Lemma 2.14), it follows that $p^2 \mid \Delta[b_1, ..., b_n]$. □

Proposition 3.15. Let K be a number field. All the integral basis of K have the same discriminant.

Proof. Let us take two integral basis $\mathcal{A} = \{\alpha_1, ..., \alpha_n\}$ and $\mathcal{B} = \{\beta_1, ..., \beta_n\}$ (They have the same cardinal because $\mathfrak{O}_K$ is free abelian group of rank n (Theorem 3.9)). We can write all α_j in the basis $\mathcal{B}$, $\alpha_j = \sum_{k=1}^{n} c_{j,k}\beta_k$ where $c_{j,k} \in \mathbb{Z}$. For all monomorphism σ_i, we have $\sigma_i(\alpha_j) = \sum_{k=1}^{n} c_{j,k}\sigma_i(\beta_k)$, because $\sigma_i(c_{j,k}) = c_{j,k}$ since $c_{j,k} \in \mathbb{Z} \subset \mathbb{Q}$, by the formula of determinants, we have $\Delta[\alpha_1, ..., \alpha_n] = [\det(c_{j,k})]^2 \Delta[\beta_1, ..., \beta_n]$. But $\mathcal{A}$ is also an integral basis then the matrix of $\{c_{j,k}\}$ is inversible. Since $c_{j,k} \in \mathbb{Z}$, we have $\det(c_{j,k}) = \pm 1$. It follows that $\Delta[\alpha_1, ..., \alpha_n] = \Delta[\beta_1, ..., \beta_n]$. □

Remark 3.16. This is why we can say *the discriminant* of K (or of $\mathfrak{O}_K$).

3.3 Computing an integral basis

Let K be a number field, we want to compute an integral basis of $\mathfrak{O}_K$.

Step 1. Take a candidate B to be an integral basis (in practice a $\mathbb{Q}-$basis consisting of algebraic integers)

Step 2. Calculate the discriminant $\Delta(B)$ of B. If $\Delta(B)$ is squarefree, we use the Theorem 3.12 and B is an integral basis. Otherwise go to step 3.

Step 3. Find one p prime such that $p^2 \mid \Delta(B)$.

Step 4. Let α be of the form of Theorem 3.14.

Step 5. Calculate the trace, it must be in $\mathbb{Z}$ (Proposition 3.6). With the trace's information that depends of λ_i, we can find some conditions on λ_i to satisfy $T_K(\alpha) \in \mathbb{Z}$. Then we could simplify α.

Step 6. Calculate the norm, it must be in $\mathbb{Z}$ (Proposition 3.6). With the norm's information that depends of λ_i, we can find some conditions on λ_i to satisfy $N_K(\alpha) \in \mathbb{Z}$. Then we could simplify α. (We begin by calculating the trace because it is often simpler to calculate).

Step 7. After all those calculations, find an α that satisfies the condition of Theorem 3.14 even if you have to consider all the possible configuration. If there is no possible α, go to Step 8. If you find an α, go to Step 9.

Step 8. If there is no possible α, return to step 3 and try with another p prime such that $p^2 \mid \Delta(B)$. If there is no possible α and there is no more p to work with, then use the Theorem 3.14 to say that B was already an integral basis, because there is no possible α.

Step 9. You have an α that you can add to your basis B, then make all the simplifications in $B \cup \{\alpha\}$ because there is at least an element b_i of B that you can write just with $B \cup \{\alpha\} \backslash \{b_i\}$ (with coefficient in $\mathbb{Z}$). You have now a new basis B'.

Step 10. Start the process over again with the basis B' from Step 2.

3.4 Example of computing an integral basis

Exercise 2.8.
Compute an integral bases of $\mathbb{Q}(\sqrt{2}, i)$.

Solution.

Step 1.
We choose $B = \{1, \sqrt{2}, i, i\sqrt{2}\}$ which is a $\mathbb{Q}-$basis of K. Indeed $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2.2 = 4$.

Step 2.
Let us calculate the discriminant $\Delta(B)$ of the basis B. Then we can see that the 4 monomorphisms are :

$$\begin{array}{ll} \sigma_1 : \sqrt{2} \mapsto \sqrt{2} & \sigma_1 : i \mapsto i \\ \sigma_2 : \sqrt{2} \mapsto -\sqrt{2} & \sigma_2 : i \mapsto i \\ \sigma_3 : \sqrt{2} \mapsto \sqrt{2} & \sigma_3 : i \mapsto -i \\ \sigma_4 : \sqrt{2} \mapsto -\sqrt{2} & \sigma_4 : i \mapsto -i \end{array}$$

It follows that $\Delta(B) = \begin{vmatrix} 1 & \sqrt{2} & i & i\sqrt{2} \\ 1 & -\sqrt{2} & i & -i\sqrt{2} \\ 1 & \sqrt{2} & -i & -i\sqrt{2} \\ 1 & -\sqrt{2} & -i & i\sqrt{2} \end{vmatrix}^2 = 4 \begin{vmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{vmatrix}^2 = 4 \begin{vmatrix} 1 & 1 & 1 & 1 \\ 0 & -2 & 0 & -2 \\ 0 & 0 & -2 & -2 \\ 0 & -2 & -2 & 0 \end{vmatrix}^2 =$

$4 \begin{vmatrix} 1 & 1 & 1 & 1 \\ 0 & -2 & 0 & -2 \\ 0 & 0 & -2 & -2 \\ 0 & 0 & -2 & 2 \end{vmatrix}^2 = 4 \begin{vmatrix} 1 & 1 & 1 & 1 \\ 0 & -2 & 0 & -2 \\ 0 & 0 & -2 & -2 \\ 0 & 0 & 0 & 4 \end{vmatrix}^2 = 4.16^2 = 2^{10}.$

Step 3.
The only prime p such that $p^2 \mid \Delta(B)$ is 2.

Step 4.
As mentioned in Theorem 3.14, let us consider α of the form $\frac{1}{2}(a + b\sqrt{2} + ci + di\sqrt{2})$ where $a, b, c, d \in \{0, 1\}$ and $(a, b, c, d) \neq (0, 0, 0, 0)$.

Step 5.
$T(\alpha) = \dfrac{4a}{2}$. Then $T(\alpha) \in \mathbb{Z}$. The trace does not give any information on the coefficients.

Step 6.
$N(\alpha) = \frac{1}{2^4}(a+b\sqrt{2}+ci+di\sqrt{2})(a-b\sqrt{2}+ci-di\sqrt{2})(a+b\sqrt{2}-ci-di\sqrt{2})(a-b\sqrt{2}-ci+di\sqrt{2}) = \frac{1}{2^4}((a^2-2b^2+c^2-2d^2)^2+8(ad-bc)^2)$ (To compute the norm in an simpler manner, start by multiply $(a + b\sqrt{2} + ci + di\sqrt{2})$ with $(a-b\sqrt{2}-ci+di\sqrt{2})$ then multiply $(a-b\sqrt{2}+ci-di\sqrt{2})$ with $(a+b\sqrt{2}-ci-di\sqrt{2})$ and then multiply both results)
We study all 16 cases since $a, b, c, d \in \{0, 1\}$.

a, b, c, d	$2^4.N(\alpha)$	$N(\alpha) \in \mathbb{Z}$?
$0, 0, 0, 1$	4	NO
$0, 0, 1, 0$	1	NO
$0, 0, 1, 1$	1	NO
$0, 1, 0, 0$	4	NO
$0, 1, 0, 1$	16	YES
$0, 1, 1, 0$	9	NO
$0, 1, 1, 1$	17	NO
$1, 0, 0, 0$	1	NO
$1, 0, 0, 1$	9	NO
$1, 0, 1, 0$	4	NO
$1, 0, 1, 1$	8	NO
$1, 1, 0, 0$	1	NO
$1, 1, 0, 1$	17	NO
$1, 1, 1, 0$	8	NO
$1, 1, 1, 1$	4	NO

Step 7.
We find $\alpha = \frac{\sqrt{2}+i\sqrt{2}}{2} = \sqrt{2}\frac{1+i}{2}$ which is an algebraic integer (minimum polynomial is $X^4 + 1$). We find an α so we go to Step 9.

Step 9.
We have $\{1, \sqrt{2}, i, i\sqrt{2}, \sqrt{2}\frac{1+i}{2}\}$ then we can remove $i\sqrt{2}$ because $i\sqrt{2} = 2\alpha - \sqrt{2}$.

Step 10.
We start the process again with the basis $B' = \{1, \sqrt{2}, i, \sqrt{2}\frac{1+i}{2}\}$.

Step 2.

Calculate the discriminant $\Delta(B') = \begin{vmatrix} 1 & \sqrt{2} & i & \sqrt{2}\frac{1+i}{2} \\ 1 & -\sqrt{2} & i & -\sqrt{2}\frac{1+i}{2} \\ 1 & \sqrt{2} & -i & \sqrt{2}\frac{1-i}{2} \\ 1 & -\sqrt{2} & -i & -\sqrt{2}\frac{1-i}{2} \end{vmatrix}^2 = -\begin{vmatrix} 1 & 1 & 1 & 1+i \\ 1 & -1 & 1 & -1-i \\ 1 & 1 & -1 & 1-i \\ 1 & -1 & -1 & -1+i \end{vmatrix}^2 =$

$-\begin{vmatrix} 1 & 1 & 1 & 1+i \\ 0 & -2 & 0 & -2-2i \\ 0 & 0 & -2 & -2i \\ 0 & -2 & -2 & -2 \end{vmatrix}^2 = -\begin{vmatrix} 1 & 1 & 1 & 1+i \\ 0 & -2 & 0 & -2-2i \\ 0 & 0 & -2 & -2i \\ 0 & 0 & -2 & 2i \end{vmatrix}^2 = -\begin{vmatrix} 1 & 1 & 1 & 1+i \\ 0 & -2 & 0 & -2-2i \\ 0 & 0 & -2 & -2i \\ 0 & 0 & 0 & 4i \end{vmatrix}^2 =$

$16^2 = 2^8$

Step 3.

The only prime p such that $p^2 \mid \Delta(B')$ is 2.

Step 4.

As mentioned in Theorem 3.14, let us consider α of the form $\frac{1}{2}(a + b\sqrt{2} + ci + d\sqrt{2}\frac{1+i}{2})$ where $a, b, c, d \in \{0, 1\}$ and $(a, b, c, d) \neq (0, 0, 0, 0)$.

Step 5.

$T(\alpha) = \dfrac{4a}{2}$. Then $T(\alpha) \in \mathbb{Z}$. The trace does not give any information on the coefficients.

Step 6.

$N(\alpha) = \frac{1}{2^4}(a + b\sqrt{2} + ci + d\sqrt{2}\frac{1+i}{2})(a - b\sqrt{2} + ci - d\sqrt{2}\frac{1+i}{2})(a + b\sqrt{2} - ci + d\sqrt{2}\frac{1-i}{2})(a - b\sqrt{2} - ci - d\sqrt{2}\frac{1-i}{2}) = \frac{1}{2^4}((a^2 - 2b^2 + c^2 - d^2 - 2bd)^2 + 2(ad - 2bc - cd)^2)$.
We study all 16 cases since $a, b, c, d \in \{0, 1\}$.

a, b, c, d	$2^4.N(\beta)$	$N(\beta) \in \mathbb{Z}$?
$0, 0, 0, 1$	1	NO
$0, 0, 1, 0$	1	NO
$0, 0, 1, 1$	2	NO
$0, 1, 0, 0$	4	NO
$0, 1, 0, 1$	25	NO
$0, 1, 1, 0$	9	NO
$0, 1, 1, 1$	34	NO
$1, 0, 0, 0$	1	NO
$1, 0, 0, 1$	2	NO
$1, 0, 1, 0$	4	NO
$1, 0, 1, 1$	1	NO
$1, 1, 0, 0$	1	NO
$1, 1, 0, 1$	18	NO
$1, 1, 1, 0$	8	NO
$1, 1, 1, 1$	17	NO

Step 7.
We cannot find an α of the form of Theorem 3.14. So go to Step 8.

Step 8.
We find no α and there is no prime $p \neq 2$ such that $p^2 \mid \Delta(B')$. Then $B' = \{1, i, \sqrt{2}, \sqrt{2}\frac{1+i}{2}\}$ is an integral basis for $\mathbb{Q}(\sqrt{2}, i)$.

Exercise 2.6.
Find a $\mathbb{Z}-$basis for the integers of $\mathbb{Q}(\sqrt[3]{5})$.

Solution.

Step 1.
We choose $B = \{1, \sqrt[3]{5}, (\sqrt[3]{5})^2\}$ which is a $\mathbb{Q}-$basis of K. Indeed $[\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}] = 3$ because $X^3 - 5$ is the minimum polynomial of $\sqrt[3]{5}$ over $\mathbb{Q}$ (Theorem 2.6).

Step 2.
Let us calculate the discriminant $\Delta(B)$ of the basis B. The 3 monomorphisms are $\sigma_1 : \sqrt[3]{5} \mapsto \sqrt[3]{5}; \sigma_2 : \sqrt[3]{5} \mapsto j\sqrt[3]{5}$ and $\sigma_3 : \sqrt[3]{5} \mapsto j^2\sqrt[3]{5}$ with $j = e^{2\pi i/3}$ ($j^2 + j + 1 = 0$ and $j^3 = 1$). Then $\sigma_1((\sqrt[3]{5})^2) = (\sqrt[3]{5})^2; \sigma_2((\sqrt[3]{5})^2) = j^2(\sqrt[3]{5})^2$ and $\sigma_3((\sqrt[3]{5})^2) = j(\sqrt[3]{5})^2$. Calculate $\Delta[1, \sqrt[3]{5}, (\sqrt[3]{5})^2] = \begin{vmatrix} 1 & \sqrt[3]{5} & (\sqrt[3]{5})^2 \\ 1 & j\sqrt[3]{5} & j^2(\sqrt[3]{5})^2 \\ 1 & j^2\sqrt[3]{5} & j(\sqrt[3]{5})^2 \end{vmatrix}^2 = (5j^2 + 5j^2 + 5j^2 - 5j - 5j - 5j)^2 = 15^2(j^2 - j)^2 = 15^2(j^4 - 2j^3 + j^2) = 15^2(j + 1 + j^2 - 3) = -3^3.5^2$.

Step 3.
Let us take 3 as prime such that $3^2 \mid \Delta(B)$.

Step 4.
As mentioned in Theorem 3.14, let us consider α of the form $\alpha = \dfrac{a + b\sqrt[3]{5} + c(\sqrt[3]{5})^2}{3}$ where $a, b, c \in \{0, 1, 2\}$ and $(a, b, c) \neq (0, 0, 0)$.

Step 5.
Let us calculate the trace $T_K(\alpha) = \dfrac{a + b\sqrt[3]{5} + c(\sqrt[3]{5})^2}{3} + \dfrac{a + bj\sqrt[3]{5} + cj^2(\sqrt[3]{5})^2}{3} + \dfrac{a + bj^2\sqrt[3]{5} + cj(\sqrt[3]{5})^2}{3} = \dfrac{3a}{3}$ because $1 + j + j^2 = 0$ and $\dfrac{3a}{3} \in \mathbb{Z}$. Then the trace does not give any informations on the coefficients.

Step 6.
Let us calculate the norm $N_K(\alpha) = \dfrac{1}{3^3}(a + b\sqrt[3]{5} + c(\sqrt[3]{5})^2)(a + bj\sqrt[3]{5} + cj^2(\sqrt[3]{5})^2)(a + bj^2\sqrt[3]{5} + cj(\sqrt[3]{5})^2) = \dfrac{1}{27}(a^3 + 5b^3 + 25c^3 - 15abc)$ (this results in a long and somewhat exhausting calculation). So we need that $3^3 \mid (a^3 + 5b^3 + 25c^3 - 15abc)$. We study all the possible cases, listed below:

a, b, c	$\sigma = (a^3 + 5b^3 + 5^2c^3 - 3.5abc)$	$3^3 \mid \sigma$?
$0, 0, 1$	5^2	NO
$0, 0, 2$	$2^3.5^2$	NO
$0, 1, 0$	5	NO
$0, 1, 1$	$2.3.5$	NO
$0, 1, 2$	5.41	NO
$0, 2, 0$	$2^3.5$	NO
$0, 2, 1$	5.13	NO
$0, 2, 2$	$2^4.3.5$	NO
$1, 0, 0$	1	NO
$1, 0, 1$	2.13	NO
$1, 0, 2$	3.67	NO
$1, 1, 0$	2.3	NO
$1, 1, 1$	2^4	NO
$1, 1, 2$	$2^4.11$	NO
$1, 2, 0$	41	NO
$1, 2, 1$	$2^2.3^2$	NO
$1, 2, 2$	181	NO
$2, 0, 0$	2^3	NO
$2, 0, 1$	3.11	NO
$2, 0, 2$	$2^4.13$	NO
$2, 1, 0$	13	NO
$2, 1, 1$	2^3	NO
$2, 1, 2$	$3^2.17$	NO
$2, 2, 0$	$2^4.3$	NO
$2, 2, 1$	13	NO
$2, 2, 2$	2^7	NO

Step 7.
We cannot find an α of the form $\frac{1}{3}(a + b\sqrt[3]{5} + c(\sqrt[3]{5})^2)$. So go to Step 8.

Step 8.
We return to Step 3 because we still have a p prime such that $p^2 \mid \Delta(B)$.

Step 3.
Let us take $p = 5$ which is such that $p^2 \mid \Delta(B)$

Step 4.
Let us take α of the form $\alpha = \frac{a + b\sqrt[3]{5} + c(\sqrt[3]{5})^2}{5}$ with $a, b, c \in \{0, 1, 2, 3, 4\}$ and $(a, b, c) \neq (0, 0, 0)$.

Step 5.

Let us calculate the trace $T_K(\alpha) = \frac{a + b\sqrt[3]{5} + c(\sqrt[3]{5})^2}{5} + \frac{a + bj\sqrt[3]{5} + cj^2(\sqrt[3]{5})^2}{5} + \frac{a + bj^2\sqrt[3]{5} + cj(\sqrt[3]{5})^2}{5} = \frac{3a}{5}$ that must be in $\mathbb{Z}$ then $a \in 5\mathbb{Z} \cap \{0, 1, 2, 3, 4\}$, hence $a = 0$. Then we can write $\alpha = \frac{b\sqrt[3]{5} + c(\sqrt[3]{5})^2}{5}$.

Step 6.

Let us calculate the norm $N_K(\alpha) = \frac{1}{5^3}(5b^3 + 25c^3) = \frac{b^3 + 5c^3}{25}$ that must be in $\mathbb{Z}$ so we want $b^3 + 5c^3 = 25m$ with $m \in \mathbb{Z}$. If we are looking in $\mathbb{Z}/5\mathbb{Z}$ we have $b^3 \equiv 0$ [5], but $1^3 \equiv 1$ [5], $2^3 \equiv 3$ [5], $3^3 \equiv 2$ [5] and $4^3 \equiv 4$ [5]. Hence $b = 0$ because $b \in 5\mathbb{Z} \cap \{0, 1, 2, 3, 4\}$. Now we can write $\alpha = \frac{c(\sqrt[3]{5})^2}{5}$. The norm is $N_K(\alpha) = \frac{1}{5^3}(25c^3) = \frac{c^3}{5}$ that must still be in $\mathbb{Z}$, but for the same raison as case b, we have $c = 0$.

Step 7.

So we cannot find an α of the form $\frac{a + b\sqrt[3]{5} + c(\sqrt[3]{5})^2}{5}$ with $a, b, c \in \{0, 1, 2, 3, 4\}$ and $(a, b, c) \neq (0, 0, 0)$. Then go to Step 8.

Step 8.

We have no α and no more p prime such that $p^2 \mid \Delta(B)$. It follows that our basis B was already an integral basis. $\{1, \sqrt[3]{5}, (\sqrt[3]{5})^2\}$ is an integral basis of $\mathbb{Q}(\sqrt[3]{5})$.

4 Examples

4.1 Quadratic Fields

Definition 4.1 (Quadratic field)**.** A *quadratic field* is an extension of degree 2.

Since we work with number fields, we will focus on quadratic fields over $\mathbb{Q}$ (Definition 2.9).

Proposition 4.2. All quadratic field can be written $\mathbb{Q}(\sqrt{d})$ where d is a square-free rational integer (d can be negative).

Proof. Let $K = \mathbb{Q}(\theta)$ be a quadratic field. By definition $[K : \mathbb{Q}] = 2$ then the minimum polynomial of θ over $\mathbb{Q}$ is 2 (Proposition 2.6), let us call it $X^2 + aX + b$, then $\Delta = a^2 - 4b$ and $\theta = \frac{-a \pm \sqrt{\Delta}}{2}$. Then $\mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{\Delta})$ because $\sqrt{\Delta} = \pm(2\theta + a)$ then $\mathbb{Q}(\sqrt{\Delta}) \subset \mathbb{Q}(\theta)$ and conversely $\theta = \frac{-a \pm \sqrt{\Delta}}{2}$, hence

$\mathbb{Q}(\theta) \subset \mathbb{Q}(\sqrt{\Delta})$. Then if Δ is squarefree, we have finished. If not, we can write $\Delta = \alpha^2 d$ where d is squarefree and $\alpha \in \mathbb{Z}$ then $\sqrt{\Delta} = \alpha\sqrt{d}$. It follows that $\mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{d})$ because $\sqrt{\Delta} = \alpha\sqrt{d}$ then $\mathbb{Q}(\sqrt{\Delta}) \subset \mathbb{Q}(\sqrt{d})$ and conversely $\sqrt{d} = \sqrt{\Delta}/\alpha$ then $\mathbb{Q}(\sqrt{d}) \subset \mathbb{Q}(\sqrt{\Delta})$. □

Theorem 4.3. Let d be a squarefree rational integer. Then the ring of integers of $\mathbb{Q}(\sqrt{d})$ is :

(a) $\mathbb{Z}[\sqrt{d}]$ if $d \not\equiv 1$ [4],

(b) $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ if $d \equiv 1$ [4].

Proof. You can find a proof in [1] (Theorem 3.2 of [1]). But we would like to add a detail. We want to prove why a and b must be odd. We are in the case where $c = 2$. Since no prime divides all of a, b, c; a or b must be odd. If b is even, then a is odd. Since $a^2 - b^2 d \equiv 0$ [4] and $b = 2k$ where $k \in \mathbb{Z}$, we have $0 \equiv a^2 - (2k)^2 d \equiv a^2 - 4k^2 d \equiv a^2$ [4]. But a is odd, so $a = 2k' + 1$ and $a^2 = 4k'^2 + 4k' + 1 \equiv 1$ [4], there is a contradiction, therefore b is odd. If a was even then $a = 2k$ and $a^2 = 4k^2 \equiv 0$ [4], hence $b^2 d \equiv 0$ [4] but b is odd then $b^2 \equiv 1$ [4] then $0 \equiv b^2 d \equiv d$ [4], so we can write $d = 4q$ where $q \in \mathbb{Z}$ but d is squarefree, hence a contradiction. It follows that a and b must both be odd. □

Remark 4.4. This theorem proves the Remark 3.7

Theorem 4.5. An integral basis $\mathcal{B}$ of the ring of integers of $\mathbb{Q}(\sqrt{d})$ and the discriminant Δ are :

(a) If $d \not\equiv 1$ [4] then $\mathcal{B} = \{1, \sqrt{d}\}$ and $\Delta = 4d$.

(b) If $d \equiv 1$ [4] then $\mathcal{B} = \{1, \frac{1+\sqrt{d}}{2}\}$ and $\Delta = d$.

Proof. $\mathcal{B}$ comes from the Theorem 4.3. Then compute the discriminants:

$$\begin{vmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{vmatrix}^2 = (-2\sqrt{d})^2 = 4d$$

and

$$\begin{vmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & \frac{1-\sqrt{d}}{2} \end{vmatrix}^2 = (-\sqrt{d})^2 = d$$

. □

Remark 4.6. The (a) of this theorem proves the Remark 3.13.

Proposition 4.7 (Norm and Trace)**.** Let $K = \mathbb{Q}(\sqrt{d})$ a quadratic field (where d is a squarefree rational integer). Let $\alpha = a + b\sqrt{d} \in K$ where $a, b \in \mathbb{Q}$. Then $N(\alpha) = a^2 - db^2$ and $T(\alpha) = 2a$.

Proof. The minimum polynomial of $\sqrt{d}$ over $\mathbb{Q}$ is $X^2 - d = (X - \sqrt{d})(X + \sqrt{d})$. Then by Proposition 2.11, the monomorphisms of $\mathbb{Q}(\sqrt{d})$ are $\sigma_1 : \sqrt{d} \mapsto \sqrt{d}$ and $\sigma_2 : \sqrt{d} \mapsto -\sqrt{d}$. Now, by definition of the norm, $N(a + b\sqrt{d}) = \sigma_1(a + b\sqrt{d})\sigma_2(a + b\sqrt{d}) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2$. And, by definition of the trace, $T(a+b\sqrt{d}) = \sigma_1(a+b\sqrt{d})+\sigma_2(a+b\sqrt{d}) = (a+b\sqrt{d})+(a-b\sqrt{d}) = 2a$. □

Exercise 3.1.
Find integral bases and discriminants for :

(a) $\mathbb{Q}(\sqrt{3})$

(b) $\mathbb{Q}(\sqrt{-7})$

(c) $\mathbb{Q}(\sqrt{11})$

(d) $\mathbb{Q}(\sqrt{-11})$

(e) $\mathbb{Q}(\sqrt{6})$

(f) $\mathbb{Q}(\sqrt{-6})$

Solution.
We use Theorem 4.5.

(a) Here $d = 3 \not\equiv 1 \pmod 4$, so $\mathbb{Q}(\sqrt{3})$ has an integral basis of the form $\{1, \sqrt{3}\}$ and the discriminant is $4d = 4 \times 3 = 12$.

(b) Here $d = -7 \equiv 1 \pmod 4$, so $\mathbb{Q}(\sqrt{-7})$ has an integral basis of the form $\{1, \frac{1+\sqrt{-7}}{2}\}$ and the discriminant is $d = -7$.

(c) Here $d = 11 \not\equiv 1 \pmod 4$, so $\mathbb{Q}(\sqrt{11})$ has an integral basis of the form $\{1, \sqrt{11}\}$ and the discriminant is $4d = 4 \times 11 = 44$.

(d) Here $d = -11 \equiv 1 \pmod 4$, so $\mathbb{Q}(\sqrt{-11})$ has an integral basis of the form $\{1, \frac{1+\sqrt{-11}}{2}\}$ and the discriminant is $d = -11$.

(e) Here $d = 6 \not\equiv 1 \pmod 4$, so $\mathbb{Q}(\sqrt{6})$ has an integral basis of the form $\{1, \sqrt{6}\}$ and the discriminant is $4d = 4 \times 6 = 24$.

(f) Here $d = -6 \not\equiv 1 \pmod 4$, so $\mathbb{Q}(\sqrt{-6})$ has an integral basis of the form $\{1, \sqrt{-6}\}$ and the discriminant is $4d = 4 \times -6 = -24$.

4.2 Cyclotomic Fields

Definition 4.8 (Cyclotomic field)**.** A *cyclotomic field* is a field $\mathbb{Q}(\zeta_p)$ where $\zeta_p = e^{2\pi i/p}$ is a pth root of unity with p an odd prime number.

Remark 4.9. We consider only odd prime numbers because the only even prime number is 2 and $\zeta_2 = -1$, but $\mathbb{Q}(-1) = \mathbb{Q}$, hence we ignore this case.

Proposition 4.10. The minimum polynomial of $\zeta_p = e^{2\pi i/p}$ over $\mathbb{Q}$ is $X^{p-1} + X^{p-2} + ... + X + 1$.

Proof. You can find a proof in [1] (Lemma 3.4 of [1]). □

Corollary 4.11. The degree of $\mathbb{Q}(\zeta_p)$ is $p - 1$.

Proof. Use the Proposition 4.10 and the Proposition 2.6. Then the degree of the minimum polynomial of ζ_p is $p - 1$, hence $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$. □

Theorem 4.12. The ring of integers of $\mathbb{Q}(\zeta_p)$ is $\mathbb{Z}[\zeta_p]$, i.e. $\mathfrak{O}_{\mathbb{Q}(\zeta_p)} = \mathbb{Z}[\zeta_p]$.

Proof. You can find a proof in [1] (Theorem 3.5 of [1]). □

Exercise 3.3.
Let $K = \mathbb{Q}(\zeta)$ where $\zeta = e^{2\pi i/p}$ for a rational prime p. In the ring of integers $\mathbb{Z}[\zeta]$, show that $\alpha \in \mathbb{Z}[\zeta]$ is a unit if and only if $N_K(\alpha) = \pm 1$.

Solution.
Suppose that α is a unit of $\mathbb{Z}[\zeta]$, then there exists α^{-1} such that $\alpha\alpha^{-1} = 1$. While using the norm, we have $N_K(\alpha)N_K(\alpha^{-1}) = N_K(1) = 1$ and $N_K(\alpha)$ and $N_K(\alpha^{-1})$ are integers (Proposition 3.6), so $N_K(\alpha) = \pm 1$. Conversely, we consider that $N_K(\alpha) = \pm 1$, and we can write α as $a_0 + a_1\zeta + ... + a_{p-2}\zeta^{p-2}$ (because $1+X+...+X^{p-1}$ is the minimal polynomial of ζ then K is a $\mathbb{Q}-$vector space of dimension $p-1$ so we need $p-1$ a_i). Then $N_K(\alpha) = \prod_i \sigma_i(a_0 + a_1\zeta + ... + a_{p-2}\zeta^{p-2}) = \prod_i (\sigma_i(a_0) + \sigma_i(a_1)\zeta^i + ... + \sigma_i(a_{p-2})\zeta^{i(p-2)}) = \prod_i (a_0 + a_1\zeta^i + ... + a_{p-2}\zeta^{i(p-2)}) = \pm 1$ and for $i = 1$, we find α, so we have a product of factors including α which is equal to ± 1, then α has an inverse and it follows that it is a unit.

Exercise 3.4.
If $\zeta = e^{2\pi i/3}$, $K = \mathbb{Q}(\zeta)$, prove that the norm of $\alpha \in \mathbb{Z}[\zeta]$ is of the form $\frac{1}{4}(a^2 + 3b^2)$ where a, b are rational integers which are either both even or both odd. Using the result of question 3.3, deduce that there are precisely six units in $\mathbb{Z}[\zeta]$ and find them all.

Solution.
Let $a+b\zeta \in K$. $N(a+b\zeta) = (a+b\zeta)(a+b\zeta^2) = a^2+b^2-ab = b^2(\frac{a^2}{b^2}+1-\frac{a}{b}) = b^2((\frac{a}{b}-\frac{1}{2})^2+\frac{3}{4}) = \frac{1}{4}((2a-b)^2+3b^2)$. Then if b is odd, $2a-b$ is also odd and if b is even, $2a-b$ is also even (because $2a$ is always even).
We are looking for a and b in $\mathbb{Z}$ such that $\frac{1}{4}(a^2+3b^2) = \pm 1$ (Exercise 3.3). That is equivalent to $a^2+3b^2 = 4$ because a^2+3b^2 is positive. It implies $|a| \leqslant 2$ and $|b| \leqslant 2$. Among the few possibilities, only the couples $(1,1)$, $(1,-1)$, $(-1,1)$, $(-1,-1)$, $(2,0)$ and $(-2,0)$ work. So there are precisely 6 units in $\mathbb{Z}[\zeta]$.

5 Properties of the ring of integers

Let K be a number field. We want to study the unique factorization into irreducibles in $\mathfrak{O}_K$. We will see that the factorization is always possible while it is not always unique.

5.1 Existence of factorization into irreducibles

Definition 5.1 (Unit)**.** An element u in a ring A is called a *unit* if there exists $v \in A$ such that $uv = 1$.

Definition 5.2 (Associate)**.** In a ring A, two elements x and y are called *associates* if there exists a unit u of A such that $x = uy$.

Definition 5.3 (Irreducible)**.** Let D be an integral domain. $x \in D$ is said *irreducible* if:

- x is not a unit
- if $x = yz$ with $y, z \in D$ then either y or z is a unit

Definition 5.4 (Factorization into irreducibles)**.** The *factorization into irreducibles* of x is $x = x_1x_2x_3...x_n$ where x_i for $i \in \{1,..,n\}$ are irreducible.

Proposition 5.5. Let K be a number field. The ring of integers $\mathfrak{O}_K$ is noetherian.

Proof. You can find a proof in [1] (Theorem 4.7 of [1]). □

Theorem 5.6. If a domain D is noetherian, then factorization into irreducibles is possible in D.

Proof. You can find a proof in [1] (Theorem 4.6 of [1]). □

Corollary 5.7. Let K be a number field. Then factorization into irreducibles is possible in $\mathfrak{O}_K$.

Proof. Factorization is possible in a noetherian domain (Theorem 5.6) and $\mathfrak{O}_K$ is noetherian (Proposition 5.5) then factorization into irreducibles is possible in $\mathfrak{O}_K$. □

Proposition 5.8. Let K be a number field. Let x and y in $\mathfrak{O}_K$. Then

(a) x is a unit if and only if $N(x) = \pm 1$,

(b) If x and y are associates, then $N(x) = \pm N(y)$,

(c) If $N(x)$ is a rational prime, then x is irreducible in $\mathfrak{O}_K$.

Proof. You can find a proof in [1] (Proposition 4.9 of [1]). □

Exercise 4.1.
Which of the following elements of $\mathbb{Z}[i]$ are irreducible ($i = \sqrt{-1}$): $1+i,\ 3-7i,\ 5,\ 7,\ 12i,\ -4+5i$?

Solution.
For $a+bi$ in $\mathbb{Z}[i]$, $N(a+bi) = a^2+b^2$.

- $N(1+i) = 2$, if we have $\alpha\beta = 1+i$ with α, β not unit ($N(\alpha) \neq \pm 1$ and $N(\beta) \neq \pm 1$), then $N(\alpha)N(\beta) = N(1+i) = 2$, it is impossible because 2 is irreducible in $\mathbb{Z}$. It follows that $1+i$ is irreducible.
- $N(3-7i) = 9+49 = 58 = 2.29 = (1^2+1^2)(5^2+2^2)$, while looking at this expression, we find $3-7i = (1-i)(5-2i)$, hence $3-7i$ is not irreducible.
- $5 = (2+i)(2-i)$, hence 5 is not irreducible.
- 7 is irreducible because $N(7) = 49 = 7.7$, so we looking for $a+bi$ such that $N(a+bi) = 7$. But $a^2+b^2 = 7$ has no integer solution (Try all the possibilities with $|a| \leqslant 3$ and $|b| \leqslant 3$.)
- $12i = 4.3i$, hence $12i$ is not irreducible.
- For the same raison than the case $1+i$, $N(-4+5i) = 4^2+5^2 = 41$ which is irreducible (because prime in $\mathbb{Z}$), hence $-4+5i$ is irreducible.

5.2 Unique factorization into irreducibles

Definition 5.9 (Unique factorization)**.** We say that the factorization into irreducibles of $x = x_1x_2...x_n$ is *unique* if for an other factorization into irreducibles of $x = y_1y_2...y_m$, then we have $m = n$ and there exists a permutation π of $\{1, 2, ..., n\}$ such that x_i is associate to $y_{\pi(i)}$ for all i in $\{1, .., n\}$.

Definition 5.10 (Euclidean)**.** A domain D is said *Euclidean* if there exists a function $\phi : D\backslash\{0\} \to \mathbb{N}$ such that:

(a) If $a, b \in D\backslash\{0\}$ and $a \mid b$ then $\phi(a) \leqslant \phi(b)$,

(b) If $a, b \in D\backslash\{0\}$ then there exist $q, r \in D$ such that $a = bq+r$ where either $r = 0$ or $\phi(r) < \phi(b)$.

Remark 5.11. $\mathbb{Z}$ is Euclidean with $\phi(n) = |n|$ and $K[X]$ is Euclidean with $\phi(P) = \partial P$ where K is a field.

Proposition 5.12. An Euclidean domain is a principal ideal domain which is a unique factorization domain, i.e.

$$\text{Euclidean} \implies \text{principal} \implies \text{unique factorization}$$

Proof. You can find a proof in [1] (Theorem 4.14 and 4.15 of [1]). □

Example 5.13. In $\mathbb{Q}(\sqrt{-6})$, $6 = 2.3 = -\sqrt{-6}.\sqrt{-6}$. We want to prove that $2, 3, \sqrt{-6}$ are irreducible. The norm in $\mathbb{Q}(\sqrt{-6})$ is $N(a+b\sqrt{-6}) = a^2+6b^2$. The norm of $2, 3, \sqrt{-6}$ are respectively $4, 9, 6$. If $2 = \alpha\beta$, then $N(2) = 4 = N(\alpha)N(\beta)$ with $N(\alpha)$ and $N(\beta)$ proper factors of 4 and we can also do that for 3 and $\sqrt{-6}$. The proper factors of $4, 9, 6$ are 2 and 3. But $a^2 + 6b^2 = 2$ or 3 have no solutions, because that implies that $b = 0$ and 2 and 3 are not square. It follows that $2, 3, \sqrt{-6}$ are irreducible. And $2, 3, \sqrt{-6}$ are not associate due to Proposition 5.8. Then the factorization is not unique. It follows that $\mathbb{Q}(\sqrt{-6})$ cannot be Euclidean.

5.3 Examples

Theorem 5.14. The ring of integers $\mathfrak{O}_{\mathbb{Q}(\sqrt{d})}$ is Euclidean for $d = -1,\ -2,\ -3,\ -7,\ -11,\ 2,\ 3,\ 4,\ 6,\ 7,\ 13,\ 17,\ 21,\ 29$ with the function $\phi(\alpha) = |N(\alpha)|$

Proof. You can find a proof in [1] (Theorem 4.17, 4.19, 4.20 of [1]). □

Theorem 5.15. The ring of integers $\mathfrak{O}_{\mathbb{Q}(\sqrt{d})}$ is not Euclidean for $d = -5,\ -6,\ -10,\ 10,\ 15,\ 26,\ 30$ and $d < -11$ for the function $\phi(\alpha) = |N(\alpha)|$

Proof. You can find a proof in [1] (Theorem 4.10, 4.11, 4.18 of [1]). □

Remark 5.16. We already proved that $\mathbb{Q}(\sqrt{-6})$ is not Euclidean in the example 5.13.

Exercise 4.14.
Prove that the ring of integers of $K = \mathbb{Q}(e^{2\pi i/5})$ is Euclidean.

Solution.
We want to prove that $\mathbb{Q}(e^{2\pi i/5})$ is Euclidean with Euclidean function $\phi(\alpha) = |N(\alpha)|$. We use the same approach than the proof of Theorem 4.17 of [1]. We have (a) with the same methods. We want to prove (c), because (c) is equivalent to (b) where for all $\alpha,\ \beta \in \mathfrak{O}_K\backslash\{0\}$, (a) is "If $\alpha \mid \beta$ then $|N(\alpha)| \leqslant |N(\beta)|$", (b) is "There exist $\gamma, \delta \in \mathfrak{O}_K$ such that $\alpha = \beta\gamma + \delta$ where either $\delta = 0$ or $|N(\delta)| < |N(\beta)|$" and (c) is "For any $\epsilon \in \mathbb{Q}(e^{2\pi i/5})$ there exists $\kappa \in \mathfrak{O}_K$ such that $|N(\epsilon - \kappa)| < 1$".
We will use the Exercise 0.1 to see that $\mathbb{Q}(\sqrt{5})$ is a subfield of $\mathbb{Q}(\zeta)$ where $\zeta = e^{2\pi i/5}$ and we have $[\mathbb{Q}(\zeta) : \mathbb{Q}(\sqrt{5})] = 2$. Let α be in $\mathbb{Q}(\zeta)$, then we can write

$\alpha = \alpha_1 + \alpha_2\zeta$ where $\alpha_1, \alpha_2 \in \mathbb{Q}(\sqrt{5})$. As in the Exercise 2.13, $N_{\mathbb{Q}(\zeta)/\mathbb{Q}(\sqrt{5})}(\alpha) = (\alpha_1 + \alpha_2\zeta)(\alpha_1 + \alpha_2\zeta^4) = \alpha_1^2 + \alpha_2^2 + (\sqrt{5}-1)\alpha_1\alpha_2$.
We want to prove that for all $\alpha \in \mathbb{Q}(\zeta)$ there exists $\kappa \in \mathfrak{O}_{\mathbb{Q}(\zeta)}$ such that $|N(\alpha - \kappa)| < 1$. We assume that it is true for $\kappa = \kappa_1 + \kappa_2\zeta$ where $\kappa_1, \kappa_2 \in \mathbb{Z}[\sqrt{5}]$ and use $\mathbb{Z}[\sqrt{5}] \subset \mathfrak{O}_{\mathbb{Q}(\sqrt{5})}$, hence $\kappa \in \mathfrak{O}_{\mathbb{Q}(\zeta)}$ because ζ is an algebraic integer in $\mathbb{Q}(\zeta)$. We write $\alpha = \alpha_1 + \alpha_2\zeta$ where $\alpha_1, \alpha_2 \in \mathbb{Q}(\sqrt{5})$ and $\kappa = \kappa_1 + \kappa_2\zeta$ where $\kappa_1, \kappa_2 \in \mathbb{Z}[\sqrt{5}]$. Then $N(\alpha - \kappa) = (\alpha_1 - \kappa_1)^2 + (\alpha_2 - \kappa_2)^2 + (\sqrt{5}-1)(\alpha_1 - \kappa_1)(\alpha_2 - \kappa_2)$. Let us write $\sigma = \alpha - \kappa$, $\sigma_1 = \alpha_1 - \kappa_1$ and $\sigma_2 = \alpha_2 - \kappa_2$.
Claim: For all $r \in \mathbb{R}$, for all $\epsilon > 0$, there exists $s \in \mathbb{Z}[\sqrt{5}]$ such that $|r - s| \leqslant \epsilon$.
Proof of the claim: Let r be in $\mathbb{R}$ and $\epsilon > 0$. $|\sqrt{5} - 2| < 1$, hence $(\sqrt{5}-2)^n \to 0$ when $n \to \infty$. Then there exists n_0 such that $(\sqrt{5}-2)^{n_0} < \epsilon$. Let u be $\sqrt{5}-2$. u is in $\mathbb{Z}[\sqrt{5}]$ then $u^n \in \mathbb{Z}[\sqrt{5}]$ for all $n \in \mathbb{N}$ because $\mathbb{Z}[\sqrt{5}]$ is a group for multiplication (because it is a ring).

$$\begin{array}{rcccl} \frac{r}{u^{n_0}} - 1 & \leqslant & \lfloor \frac{r}{u^{n_0}} \rfloor & \leqslant & \frac{r}{u^{n_0}} \\ \frac{r}{u^{n_0}} & \leqslant & 1 + \lfloor \frac{r}{u^{n_0}} \rfloor & \leqslant & 1 + \frac{r}{u^{n_0}} \\ r & \leqslant & (1 + \lfloor \frac{r}{u^{n_0}} \rfloor)u^{n_0} & \leqslant & u^{n_0} + r \\ 0 & \leqslant & (1 + \lfloor \frac{r}{u^{n_0}} \rfloor)u^{n_0} - r & \leqslant & u^{n_0} \leqslant \epsilon \end{array}$$

It follows that we have $|r - (1 + \lfloor \frac{r}{u^{n_0}} \rfloor)u^{n_0}| \leqslant \epsilon$ and $(1 + \lfloor \frac{r}{u^{n_0}} \rfloor) \in \mathbb{Z}$, hence $(1 + \lfloor \frac{r}{u^{n_0}} \rfloor)u^{n_0} \in \mathbb{Z}[\sqrt{5}]$. So $\mathbb{Z}[\sqrt{5}]$ is dense in $\mathbb{R}$. □
We use the claim with $r = \alpha_i$ where $i = 1,\ 2$ and $\epsilon = 1/2$, then there exist κ_1 and κ_2 such that $|\alpha_i - \kappa_i| \leqslant 1/2$, it follows that $\sigma_1^2 \leqslant 1/4$, $\sigma_2^2 \leqslant 1/4$ and $|\sigma_1\sigma_2| \leqslant 1/4$ then $N(\alpha - \kappa) \leqslant \frac{1}{4} + \frac{1}{4} + \frac{\sqrt{5}-1}{4} < \frac{1+1+2}{4} = 1$. We have proved (c), hence the ring of integers of $\mathbb{Q}(\zeta)$ is Euclidean with the norm as Euclidean function.

6 Ideals

6.1 Definition

We will denote ideals by small bold Gothic letters, for example '$\mathfrak{a}$'.

Definition 6.1. Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals. Then we define the *product of ideals* $\mathfrak{ab}$ as the set of finite sums $\sum x_i y_i$ where $x_i \in \mathfrak{a}$ and $y_i \in \mathfrak{b}$.

Definition 6.2 (Prime ideal)**.** Let $\mathfrak{a}$ an ideal of a ring R. $\mathfrak{a}$ is said *prime* if:

- $\mathfrak{a} \neq R$
- if $\mathfrak{bc} \subset \mathfrak{a}$ where $\mathfrak{b},\ \mathfrak{c}$ ideals of R then either $\mathfrak{b} \subset \mathfrak{a}$ or $\mathfrak{c} \subset \mathfrak{a}$.

Exercise 5.1.
In an integral domain D, show that a principal ideal $\langle p \rangle$ is prime if and only if p is a prime or zero.

Solution.
The definition of '$\langle p\rangle$ is prime' is: $\mathfrak{ab} \subset \langle p\rangle$ implies $\mathfrak{a} \subset \langle p\rangle$ or $\mathfrak{b} \subset \langle p\rangle$. The definition of 'p is a prime' is: $p \mid ab$ implies $p \mid a$ or $p \mid b$.
Suppose $p = 0$, then $\langle p\rangle = \{0\}$. If $\mathfrak{ab} \subset \{0\}$, then $\mathfrak{a} = \{0\}$ or $\mathfrak{b} = \{0\}$ (because if $a \in \mathfrak{a}\backslash\{0\}$ and $b \in \mathfrak{b}\backslash\{0\}$, then $ab \in \mathfrak{ab} \subset \{0\}$, so $ab = 0$ but it is impossible because D is a domain, $a \neq 0$ and $b \neq 0$), hence $\mathfrak{a} \subset \{0\}$ or $\mathfrak{b} \subset \{0\}$. It follows that $\langle p\rangle$ is prime.
Suppose p is a prime and $\mathfrak{ab} \subset \langle p\rangle$. If $\mathfrak{a} \not\subset \langle p\rangle$, then it exists a in $\mathfrak{a}\backslash\langle p\rangle$. For all b in $\mathfrak{b}$, $ab \in \mathfrak{ab} \subset \langle p\rangle$, then $ab = pk$ for $k \in D$. So $p \mid ab$ but p is a prime, then $p \mid a$ or $p \mid b$ but $a \notin \langle p\rangle$ hence $p \mid b$, so $\mathfrak{b} \subset \langle p\rangle$ and it follows that $\langle p\rangle$ is prime.
Conversely, $\langle p\rangle$ is prime. Let $p \mid ab$, then $ab \in \langle p\rangle$ and it follows that $\langle a\rangle\langle b\rangle \subset \langle p\rangle$. $\langle p\rangle$ is prime so $\langle a\rangle \subset \langle p\rangle$ or $\langle b\rangle \subset \langle p\rangle$. Then $a \in \langle p\rangle$ or $b \in \langle p\rangle$, hence $p \mid a$ or $p \mid b$.

Definition 6.3 (Maximal ideal)**.** Let $\mathfrak{a}$ an ideal of a ring R. $\mathfrak{a}$ is said *maximal* if there is no ideal strictly between $\mathfrak{a}$ and R

Proposition 6.4. Let $\mathfrak{a}$ an ideal of a ring R. Then

(a) $\mathfrak{a}$ is maximal if and only if $R/\mathfrak{a}$ is a field.

(b) $\mathfrak{a}$ is prime if and only if $R/\mathfrak{a}$ is a domain.

Proof. You can find a proof in [1] (Lemma 5.1 of [1]). □

Corollary 6.5. Every maximal ideal is prime.

Proof. We use the Proposition 6.4 because a field is always a domain, hence a maximal ideal is prime. □

Theorem 6.6. The ring of integers $\mathfrak{O}_K$ of a number field K has the following properties :

(a) It is a domain with the field of fractions K,

(b) It is noetherian,

(c) If $\alpha \in K$ satisfies a monic polynomial equation with coefficients in $\mathfrak{O}_K$ then $\alpha \in \mathfrak{O}_K$,

(d) Every non-zero prime ideal of $\mathfrak{O}_K$ is maximal.

Proof. You can find a proof in [1] (Theorem 5.3 of [1]). □

Exercise 5.8.
Suppose $\mathfrak{p}$, $\mathfrak{q}$ are distinct prime ideals in $\mathfrak{O}$. Show $\mathfrak{p} + \mathfrak{q} = \mathfrak{O}$ and $\mathfrak{p} \cap \mathfrak{p} = \mathfrak{pq}$.

Solution.
$\mathfrak{p}$, $\mathfrak{q}$ are distinct, hence, without loss of generality, there exists an element α in $\mathfrak{q}$ which is not in $\mathfrak{p}$. We know that $\mathfrak{p}+\mathfrak{q}$ is an ideal of $\mathfrak{O}$ and $\mathfrak{p} \subset \mathfrak{p}+\mathfrak{q}$. But while using Theorem 6.6, $\mathfrak{p}$ is a maximal ideal, and $\mathfrak{p}+\mathfrak{q} \neq \mathfrak{p}$ because $\alpha \in \mathfrak{p}+\mathfrak{q}$ but $\alpha \notin \mathfrak{p}$, hence $\mathfrak{p} \subsetneq \mathfrak{p}+\mathfrak{q}$, then by definition of a maximal ideal, $\mathfrak{p}+\mathfrak{q}=\mathfrak{O}$.
$\mathfrak{pq} \subset \mathfrak{p} \cap \mathfrak{q}$ because by definition of an ideal, for all $\alpha \in \mathfrak{pq}$, α is in $\mathfrak{p}$ and α is in $\mathfrak{q}$, then α is in $\mathfrak{p} \cap \mathfrak{q}$. Conversely, let $z \in \mathfrak{p} \cap \mathfrak{q}$, we can find $x \in \mathfrak{p}$ and $y \in \mathfrak{q}$ such that $x+y=1$ because $1 \in \mathfrak{O} = \mathfrak{p}+\mathfrak{q}$. Then $z = xz + zy \in \mathfrak{pq}$ because $xz \in \mathfrak{pq}$ and $zy \in \mathfrak{pq}$. It follows that $\mathfrak{p} \cap \mathfrak{q} \subset \mathfrak{pq}$.

Definition 6.7 (fractional ideal)**.** Let K be a number field. Let $\mathfrak{a}$ be an $\mathfrak{O}_K-$submodule of K. $\mathfrak{a}$ is a *fractional ideal* of $\mathfrak{O}_K$ if there exists a non-zero $c \in \mathfrak{O}_K$ such that $c\mathfrak{a}$ is an ideal of $\mathfrak{O}_K$. In other words, the fractional ideals of $\mathfrak{O}_K$ are subsets of K of the form $c^{-1}\mathfrak{b}$ where $\mathfrak{b}$ is an ideal of $\mathfrak{O}_K$ and c a non-zero element of $\mathfrak{O}_K$.

Exercise 5.10.
Find all fractional ideals of $\mathbb{Z}$ and of $\mathbb{Z}[\sqrt{-1}]$.

Solution.
$\mathbb{Z}$ and $\mathbb{Z}[\sqrt{-1}]$ are Euclidean (Theorem 5.14) then they are principal ideal domain (Proposition 5.12). So the ideals of $\mathbb{Z}$ are $n\mathbb{Z}$ where $n \in \mathbb{Z}$ and the ideals of $\mathbb{Z}[\sqrt{-1}]$ are $\alpha\mathbb{Z}[\sqrt{-1}]$ where $\alpha \in \mathbb{Z}[\sqrt{-1}]$. By definition of fractional ideals (Definition 6.7), fractional ideals can be written as $c^{-1}\mathfrak{a}$ where $\mathfrak{a}$ is an ideal of the ring of integers we work with and c a non-zero element of the ring of integers. Then the fractional ideals of $\mathbb{Z}$ are $\frac{a}{b}\mathbb{Z}$ where $a, b \in \mathbb{Z}$ and $b \neq 0$ (equivalent to $r\mathbb{Z}$ where $r \in \mathbb{Q}$ (Example page 112 of [1])). The fractional ideals of $\mathbb{Z}[\sqrt{-1}]$ are $\frac{\alpha}{\beta}\mathbb{Z}[\sqrt{-1}]$ where $\alpha, \beta \in \mathbb{Z}[\sqrt{-1}]$ and $\beta \neq 0$.

Theorem 6.8. The non-zero fractional ideals of $\mathfrak{O}_K$ form an abelian group under multiplication.

Proof. You can find a proof in [1] (Theorem 5.4 of [1]). □

Theorem 6.9. Every non-zero ideal of $\mathfrak{O}_K$ can be written as a product of prime ideals, uniquely up to the order of the factors.

Proof. You can find a proof in [1] (Theorem 5.5 of [1]). □

Theorem 6.10. Let K be a number field of degree n with the ring of integers $\mathfrak{O}_K = \mathbb{Z}[\theta]$ generated by $\theta \in \mathfrak{O}_K$. Given a rational prime p, suppose the

minimum polynomial f of θ over $\mathbb{Q}$ gives rise to the factorization into irreducibles over $\mathbb{Z}/p\mathbb{Z}$:

$$\overline{f} = \overline{f}_1^{e_1} ... \overline{f}_r^{e_r}$$

where the bar denotes the natural map $\mathbb{Z}[X] \to (\mathbb{Z}/p\mathbb{Z})[X]$. Then if $f_i \in \mathbb{Z}[X]$ is any polynomial mapping onto $\overline{f}_i$, the ideal

$$\mathfrak{p}_i = \langle p \rangle + \langle f_i(\theta) \rangle$$

is prime and the prime factorization of $\langle p \rangle$ in $\mathfrak{O}_K$ is

$$\langle p \rangle = \mathfrak{p}_1^{e_1} ... \mathfrak{p}_r^{e_r}$$

Proof. You can find a proof in [1] (Theorem 10.1 of [1]). □

Exercise 5.2.
In $\mathbb{Z}[\sqrt{-5}]$, define the ideals $\mathfrak{p} = \langle 2, 1+\sqrt{-5} \rangle$, $\mathfrak{q} = \langle 3, 1+\sqrt{-5} \rangle$ and $\mathfrak{r} = \langle 3, 1-\sqrt{-5} \rangle$. Prove that these are maximal ideals, hence prime. Show that

(i) $\mathfrak{p}^2 = \langle 2 \rangle$

(ii) $\mathfrak{q}\mathfrak{r} = \langle 3 \rangle$

(iii) $\mathfrak{p}\mathfrak{q} = \langle 1+\sqrt{-5} \rangle$

(iv) $\mathfrak{p}\mathfrak{r} = \langle 1-\sqrt{-5} \rangle$

Show that the factorizations of 6 given in the proof of Theorem 4.10 of [1] come from two different groupings of the factorization into prime ideals $\langle 6 \rangle = \mathfrak{p}^2\mathfrak{q}\mathfrak{r}$.

Solution.
Proof of $\mathfrak{p}$ *is maximal.* Let I be an ideal of $\mathbb{Z}[\sqrt{-5}]$ such that $\mathfrak{p} \subsetneq I$. we want to prove that $I = \mathbb{Z}[\sqrt{-5}]$. Let α be in I but not in $\mathfrak{p}$. $\alpha = a + b\sqrt{-5}$ where $a, b \in \mathbb{Z}$, then $\alpha - b(1+\sqrt{-5}) = a - b$ is in I because $\mathfrak{p} \subset I$ but not in $\mathfrak{p}$ because if it was then α will be also in $\mathfrak{p}$ ($\alpha = \alpha - b(1+\sqrt{-5}) + b(1+\sqrt{-5}) \in \mathfrak{p}$). Now $a - b \in \mathbb{Z}$, do the Euclidean division by 2, then $a - b = 2q + r$ with $r \in \{0, 1\}$, but 0 is not possible because if we have $a - b = 2q$, then $a - b$ would be in $\mathfrak{p}$ but we have just told that it was not possible. It follows that $a - b = 2q + 1$ then $1 = a - b - 2q \in I$ because $2 \in \mathfrak{p} \subset I$. Hence $1 \in I$, so $I = \mathbb{Z}[\sqrt{-5}]$. It follows that $\mathfrak{p}$ is maximal, hence prime (Corollary 6.5).
Proof of $\mathfrak{q}$ *is maximal.* We proceed with the same approach. The difference is that the rest of Euclidean division $a - b = 3q + r$ is $r = 1$ or $r = 2$, then if $r = 1$ we have $1 = a - b - 3q \in I$, and if $r = 2$, we have $1 = 3(q+1) - a + b \in I$. Then we conclude in the same way than before.
Proof of $\mathfrak{r}$ *is maximal.* We proceed with the same approach. The difference is that we consider $\alpha + b(1-\sqrt{-5}) = a + b$ instead of $\alpha - b(1+\sqrt{-5}) = a - b$. The rest is in the same way than before.
Proof of $\mathfrak{p}^2 = \langle 2 \rangle$. $\mathfrak{p}^2 = \langle 4, 2(1+\sqrt{-5}), (1+\sqrt{-5})^2 \rangle$ and $(1+\sqrt{-5})^2 = -4 + 2\sqrt{-5}$ then we see that $\mathfrak{p}^2 \subset \langle 2 \rangle$. For the other inclusion, we do assume

that 2 is in $\mathfrak{p}^2$ (Indeed $2 = 2(1+\sqrt{-5}) - (-4+2\sqrt{-5}) - 4$), it follows that $\langle 2\rangle \subset \mathfrak{p}^2$, hence $\langle 2\rangle = \mathfrak{p}^2$.
Proof of $\mathfrak{q}\mathfrak{r} = \langle 3\rangle$. $\mathfrak{q}\mathfrak{r} = \langle 9, 3(1+\sqrt{-5}), 3(1-\sqrt{-5}), (1+\sqrt{-5})(1-\sqrt{-5})\rangle = \langle 9, 3+3\sqrt{-5}), 3-3\sqrt{-5}), 6\rangle$ then we see that $\mathfrak{q}\mathfrak{r} \subset \langle 3\rangle$. For the other inclusion, we assume that 3 is in $\mathfrak{q}\mathfrak{r}$ (Indeed $3 = 9-6$), it follows that $\langle 3\rangle \subset \mathfrak{q}\mathfrak{r}$, hence $\langle 3\rangle = \mathfrak{q}\mathfrak{r}$.
Proof of $\mathfrak{p}\mathfrak{q} = \langle 1+\sqrt{-5}\rangle$. $\mathfrak{p}\mathfrak{q} = \langle 6, 3(1+\sqrt{-5}), 2(1+\sqrt{-5}), (1+\sqrt{-5})\rangle = \langle (1+\sqrt{-5})(1-\sqrt{-5}), 3(1+\sqrt{-5}), 2(1+\sqrt{-5}), (1+\sqrt{-5})^2\rangle$ then we see that $\mathfrak{p}\mathfrak{q} \subset \langle 1+\sqrt{-5}\rangle$. For the other inclusion, we assume that $1+\sqrt{-5}$ is in $\mathfrak{p}\mathfrak{q}$ (Indeed $1+\sqrt{-5} = 3(1+\sqrt{-5}) - 2(1+\sqrt{-5})$), it follows that $\langle 1+\sqrt{-5}\rangle \subset \mathfrak{p}\mathfrak{q}$, hence $\langle 1+\sqrt{-5}\rangle = \mathfrak{p}\mathfrak{q}$.
Proof of $\mathfrak{p}\mathfrak{r} = \langle 1-\sqrt{-5}\rangle$. $\mathfrak{p}\mathfrak{r} = \langle 6, 3(1+\sqrt{-5}), 2(1-\sqrt{-5}), (1+\sqrt{-5})(1-\sqrt{-5})\rangle = \langle (1+\sqrt{-5})(1-\sqrt{-5}), (-2+\sqrt{-5})(1-\sqrt{-5}), 2(1-\sqrt{-5})\rangle$ then we see that $\mathfrak{p}\mathfrak{r} \subset \langle 1-\sqrt{-5}\rangle$. For the other inclusion, we assume that $1-\sqrt{-5}$ is in $\mathfrak{p}\mathfrak{r}$ (Indeed $1-\sqrt{-5} = (1+\sqrt{-5})(1-\sqrt{-5}) - (-2+\sqrt{-5})(1-\sqrt{-5}) - 2(1-\sqrt{-5})$), it follows that $\langle 1-\sqrt{-5}\rangle \subset \mathfrak{p}\mathfrak{r}$, hence $\langle 1-\sqrt{-5}\rangle = \mathfrak{p}\mathfrak{r}$.
Then we have $\langle 6\rangle = \mathfrak{p}^2\mathfrak{q}\mathfrak{r}$ and if we consider $\langle 6\rangle = \mathfrak{p}^2.\mathfrak{q}\mathfrak{r} = \langle 2\rangle\langle 3\rangle$, we find $6 = 2.3$, and if we consider $\langle 6\rangle = \mathfrak{p}\mathfrak{q}.\mathfrak{p}\mathfrak{r} = \langle 1+\sqrt{-5}\rangle\langle 1-\sqrt{-5}\rangle$, we find $6 = (1+\sqrt{-5})(1-\sqrt{-5})$. So we understand the factorizations of 6 in the proof of Theorem 4.10 of [1].

6.2 Norm

Definition 6.11 (Norm)**.** Let K be a number field. Let $\mathfrak{a}$ be an ideal of the ring of integers $\mathfrak{O}_K$. We define the *norm* of $\mathfrak{a}$ to be $N(\mathfrak{a}) = |\mathfrak{O}_K/\mathfrak{a}|$.

Proposition 6.12. If $\mathfrak{a}$ and $\mathfrak{b}$ are non-zero ideals of $\mathfrak{O}_K$, then $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$.

Proof. You can find a proof in [1] (Theorem 5.10 of [1]). There is an easy case: if $\mathfrak{a}$ and $\mathfrak{b}$ are coprime then we use the Chinese Remainder Theorem so $\mathfrak{O}_K/\mathfrak{a}\mathfrak{b} \simeq \mathfrak{O}_K/\mathfrak{a}\times\mathfrak{O}_K/\mathfrak{b}$. It follows that $N(\mathfrak{a}\mathfrak{b}) = |\mathfrak{O}_K/\mathfrak{a}\mathfrak{b}| = |\mathfrak{O}_K/\mathfrak{a}|.|\mathfrak{O}_K/\mathfrak{b}| = N(\mathfrak{a})N(\mathfrak{b})$. □

Exercise 5.3.
Calculate the norms of the ideals mentioned in Exercise 5.2 and check multiplicativity.

Solution.
By definition, $N(\mathfrak{p}) = |\mathbb{Z}[\sqrt{-5}]/\mathfrak{p}| = |\mathbb{Z}[\sqrt{-5}]/\langle 2, 1+\sqrt{-5}\rangle| = |(\mathbb{Z}[\sqrt{-5}]/\langle 1+\sqrt{-5}\rangle)/\langle\overline{2}\rangle| = |(\mathbb{Z}/6\mathbb{Z})/\langle\overline{2}\rangle| = |\mathbb{Z}/\langle 2, 6\rangle| = |\mathbb{Z}/2\mathbb{Z}| = 2$ because $\langle 2, 6\rangle = \langle 2\rangle$. The only thing that deserves a proof is $\mathbb{Z}[\sqrt{-5}]/\langle 1+\sqrt{-5}\rangle \simeq \mathbb{Z}/6\mathbb{Z}$. We will use the Correspondence Theorem for Ideals, $\mathbb{Z}[\sqrt{-5}]/\langle 1+\sqrt{-5}\rangle = (\mathbb{Z}[X]/\langle X^2+5\rangle)/\overline{\langle 1+\sqrt{-5}\rangle} = (\mathbb{Z}[X]/\langle X^2+5\rangle)/\langle 1+X\rangle = \mathbb{Z}[X]/\langle X^2+5, 1+X\rangle = (\mathbb{Z}[X]/\langle 1+$

$X\rangle)/\langle\overline{X^2+5}\rangle = \mathbb{Z}/\langle 6\rangle = \mathbb{Z}/6\mathbb{Z}$ because $X^2+5 = (X+1)^2 - 2(X+1) + 6 \equiv 6\ [X+1]$. We have to prove that $\mathbb{Z}[X]/\langle X^2+5\rangle \simeq \mathbb{Z}[\sqrt{-5}]$ and $\mathbb{Z}[X]/\langle 1+X\rangle \simeq \mathbb{Z}$.
Proof of $\mathbb{Z}[X]/\langle X^2+5\rangle \simeq \mathbb{Z}[\sqrt{-5}]$: Take the morphism $\varphi : \mathbb{Z} \hookrightarrow \mathbb{Z}[\sqrt{-5}]$ (inclusion). Then take the evaluation map $\varphi_{X\to\sqrt{-5}} : \mathbb{Z}[X] \to \mathbb{Z}[\sqrt{-5}]$, it is surjective, and we want to prove that $\mathrm{Ker}(\varphi_{X\to\sqrt{-5}}) = \langle X^2+5\rangle$, to use the First Isomorphism Theorem. $\varphi_{X\to\sqrt{-5}}(X^2+5) = \sqrt{-5}^2 + 5 = 0$, hence $X^2+5 \in \mathrm{Ker}(\varphi_{X\to\sqrt{-5}})$ and the smallest ideal that contains X^2+5 is included in $\mathrm{Ker}(\varphi_{X\to\sqrt{-5}})$ because $\mathrm{Ker}(\varphi_{X\to\sqrt{-5}})$ is an ideal, so $\langle X^2+5\rangle \subset \mathrm{Ker}(\varphi_{X\to\sqrt{-5}})$, conversely let P be in $\mathrm{Ker}(\varphi_{X\to\sqrt{-5}})$, use Euclidean division by X^2+5, then $P = Q(X^2+5)+R$ with $R(X) = a+bX$, but we know that $0 = \varphi_{X\to\sqrt{-5}}(P) = \varphi_{X\to\sqrt{-5}}(R) = a + b\sqrt{5}$, it follows that $R = 0$, since $a = b = 0$. Then $P \in \langle X^2+5\rangle$, so $\mathrm{Ker}(\varphi_{X\to\sqrt{-5}}) \subset \langle X^2+5\rangle$. Now $\mathrm{Ker}(\varphi_{X\to\sqrt{-5}}) = \langle X^2+5\rangle$ and, by the First Isomorphism Theorem, $\mathbb{Z}[X]/\ \mathrm{Ker}(\varphi_{X\to\sqrt{-5}}) \simeq \mathbb{Z}[\sqrt{-5}]$. The result follows.
Proof of $\mathbb{Z}[X]/\langle X+1\rangle \simeq \mathbb{Z}$: Take the morphism $\varphi : \mathbb{Z} \hookrightarrow \mathbb{Z}$ (inclusion). Then take the evaluation map $\varphi_{X\to -1} : \mathbb{Z}[X] \to \mathbb{Z}$, it is surjective, and we want to prove that $\mathrm{Ker}(\varphi_{X\to -1}) = \langle X+1\rangle$, to use the First Isomorphism Theorem. $\varphi_{X\to -1}(X+1) = -1+1 = 0$, hence $\langle X+1\rangle \subset \mathrm{Ker}(\varphi_{X\to -1})$, conversely let P be in $\mathrm{Ker}(\varphi_{X\to -1})$, use Euclidean division by $X+1$, then $P = Q(X+1)+a$ with $a \in \mathbb{Z}$, but we know that $0 = P(-1) = a$, it follows that $a = 0$. Then $P \in \langle X+1\rangle$, so $\mathrm{Ker}(\varphi_{X\to -1}) \subset \langle X+1\rangle$. Now $\mathrm{Ker}(\varphi_{X\to -1}) = \langle X+1\rangle$ and, by the First Isomorphism Theorem, $\mathbb{Z}[X]/\ \mathrm{Ker}(\varphi_{X\to -1}) \simeq \mathbb{Z}$. The result follows.
Then, $N(\mathfrak{q}) = |\mathbb{Z}[\sqrt{-5}]/\mathfrak{q}| = |\mathbb{Z}[\sqrt{-5}]/\langle 3, 1+\sqrt{-5}\rangle| = |(\mathbb{Z}[\sqrt{-5}]/\langle 1+\sqrt{-5}\rangle)/\langle\overline{3}\rangle| = |\mathbb{Z}/\langle 3,6\rangle| = |\mathbb{Z}/3\mathbb{Z}| = 3$ and $N(\mathfrak{r}) = |\mathbb{Z}[\sqrt{-5}]/\mathfrak{r}| = |\mathbb{Z}[\sqrt{-5}]/\langle 3, 1-\sqrt{-5}\rangle| = |(\mathbb{Z}/\langle 3,6\rangle| = |\mathbb{Z}/3\mathbb{Z}| = 3$. (This is almost the same proof than above)
$N(\mathfrak{p}^2) = N(\langle 2\rangle) = N(2) = 4 = N(\mathfrak{p}).N(\mathfrak{p})$ (Corollary 5.9), $N(\mathfrak{q}\mathfrak{r}) = N(\langle 3\rangle) = N(3) = 9 = N(\mathfrak{q}).N(\mathfrak{r})$. $N(\mathfrak{p}\mathfrak{q}) = N(\langle 1+\sqrt{-5}\rangle) = N(1+\sqrt{-5}) = 1+5 = 6 = N(\mathfrak{p}).N(\mathfrak{q})$, $N(\mathfrak{p}\mathfrak{r}) = N(\langle 1-\sqrt{-5}\rangle) = N(1-\sqrt{-5}) = 1+5 = 6 = N(\mathfrak{p}).N(\mathfrak{r})$, $N(\langle 6\rangle) = N(6) = 6^2 = 36 = 2^2.3.3 = N(\mathfrak{p}).N(\mathfrak{p}).N(\mathfrak{q}).N(\mathfrak{r})$.

Theorem 6.13. (a) Every ideal $\mathfrak{a}$ of $\mathfrak{O}_K$ with $\mathfrak{a} \neq 0$ has a $\mathbb{Z}-$basis $\{\alpha_1, ..., \alpha_n\}$ where n is the degree of K,

(b) We have $N(\mathfrak{a}) = \left|\dfrac{\Delta[\alpha_1, ..., \alpha_n]}{\Delta}\right|^{1/2}$ where Δ is the discriminant of K.

Proof. You can find a proof in [1] (Theorem 5.8 of [1]). □

Corollary 6.14. If $\mathfrak{a} = \langle a\rangle$ is a principal ideal then $N(\mathfrak{a}) = |N(a)|$.

Proof. A $\mathbb{Z}-$basis for $\mathfrak{a}$ is given by $\{a\omega_1, ..., a\omega_n\}$ where $\{a\omega_1, ..., a\omega_n\}$ is an integral basis of $\mathfrak{O}_K$. Use the Theorem 6.13, $N(\mathfrak{a}) = \left|\dfrac{\Delta[\alpha_1, ..., \alpha_n]}{\Delta}\right|^{1/2} = |\dfrac{det(\sigma_i(a\omega_j))^2}{det(\sigma_i(\omega_j))^2}|^{1/2} = |\dfrac{det(\sigma_i(a)\sigma_i(\omega_j))}{det(\sigma_i(\omega_j))}| = |\dfrac{\prod_k \sigma_k(a) det(\sigma_i(\omega_j))}{det(\sigma_i(\omega_j))}| = |N(a)|$. □

Exercise 5.4.
Prove that the ideals $\mathfrak{p}$, $\mathfrak{q}$, $\mathfrak{r}$ of Exercise 5.2 cannot be principal.

Solution.
If $\mathfrak{p}$ was principle then $\mathfrak{p} = \langle l \rangle$ where $l = a + b\sqrt{-5}$ with $a, b \in \mathbb{Z}$ and $N(\mathfrak{p}) = |N(l)| = a^2 + 5b^2$ (Corollary 6.14). But we have seen that $N(\mathfrak{p}) = 2$ in Exercise 5.3 and $a^2 + 5b^2 = 2$ has no solution, since it implies $b = 0$ and $a^2 = 2$ has no solution in $\mathbb{Z}$. For $\mathfrak{q}$ and $\mathfrak{r}$, use the same argue, because $a^2 + 5b^2 = 3$ has no solution either.

We will say that if $\mathfrak{b} \subset \mathfrak{a}$ then $\mathfrak{a}$ divides $\mathfrak{b}$ (or $\mathfrak{a} \mid \mathfrak{b}$) and if a is an element of $\mathfrak{a}$ then $\mathfrak{a}$ divides a (or $\mathfrak{a} \mid a$).

Theorem 6.15. Let $\mathfrak{a}$ be an ideal of $\mathfrak{O}_K$, $\mathfrak{a} \neq 0$.

(a) If $N(\mathfrak{a})$ is prime, then so is $\mathfrak{a}$.

(b) $N(\mathfrak{a})$ is an element of $\mathfrak{a}$, or equivalently $\mathfrak{a} \mid N(\mathfrak{a})$.

(c) If $\mathfrak{a}$ is prime it divides exactly one rational prime p, and then $N(\mathfrak{a}) = p^m$ where $m \leqslant n$, the degree of K.

Proof. You can find a proof in [1] (Theorem 5.11 of [1]). □

Theorem 6.16. Let $\mathfrak{a} \neq 0$ be an ideal of $\mathfrak{O}_K$, and $0 \neq \beta \in \mathfrak{a}$. Then there exists $\alpha \in \mathfrak{a}$ such that $\mathfrak{a} = \langle \alpha, \beta \rangle$.

Proof. You can find a proof in [1] (Theorem 5.14 of [1]) □

Remark 6.17. Hence every ideal of $\mathfrak{O}_K$ have at most 2 generators.

Theorem 6.18. Factorization of elements of $\mathfrak{O}_K$ into irreducibles is unique if and only if every ideal of $\mathfrak{O}_K$ is principal.

Proof. You can find a proof in [1] (Theorem 5.15 of [1]). □

Exercise 5.12.
Find all the ideals in $\mathbb{Z}[\sqrt{-5}]$ which contain the element 6.

Solution.
We will use the Correspondence Theorem for Ideals, there is a bijection between ideals of $\mathbb{Z}[\sqrt{-5}]$ that contain 6 and the ideals of $\mathbb{Z}[\sqrt{-5}]/\langle 6 \rangle$. Look at $\mathbb{Z}[\sqrt{-5}]/\langle 6 \rangle \simeq (\mathbb{Z}[X]/\langle X^2+5 \rangle)/\langle \overline{6} \rangle \simeq (\mathbb{Z}/6\mathbb{Z})[X]/\langle X^2+5 \rangle \simeq (\mathbb{Z}/2\mathbb{Z})[X]/\langle \overline{X^2+5} \rangle \times (\mathbb{Z}/3\mathbb{Z})[X]/\langle \overline{X^2+5} \rangle$, by the Chinese Remainder Theorem and the same ideas of Exercise 5.3.
Study $(\mathbb{Z}/2\mathbb{Z})[X]/\langle \overline{X^2+5} \rangle$. $(\mathbb{Z}/2\mathbb{Z})[X]/\langle \overline{X^2+5} \rangle \simeq (\mathbb{Z}/2\mathbb{Z})[X]/\langle X^2+1 \rangle \simeq (\mathbb{Z}/2\mathbb{Z})[X]/\langle (X+1)^2 \rangle \simeq (\mathbb{Z}/2\mathbb{Z})[Y]/\langle Y^2 \rangle$ by using the morphism $X \mapsto X + 1$. There are 3 ideals of $(\mathbb{Z}/2\mathbb{Z})[Y]/\langle Y^2 \rangle$, $\langle 0 \rangle$, $\langle 1 \rangle$ and $\langle X \rangle$. ($\langle X + 1 \rangle$ is equal to

$\langle 1\rangle$ because $(X+1)(X+1) = X^2+2X+1 = X^2+1$ in $(\mathbb{Z}/2\mathbb{Z})[X]$ and equal to 1 in $(\mathbb{Z}/2\mathbb{Z})[X]/\langle X^2\rangle)$
Study $(\mathbb{Z}/3\mathbb{Z})[X]/\langle X^2+5\rangle$. $(\mathbb{Z}/3\mathbb{Z})[X]/\langle X^2+2\rangle \simeq (\mathbb{Z}/3\mathbb{Z})[X]/\langle (X+1)(X+2)\rangle$ and while using the Chinese Remainder Theorem (because $(X+2)-(X+1) = 1$, then $\langle X+1\rangle + \langle X+2\rangle = \langle 1\rangle$), we have $(\mathbb{Z}/3\mathbb{Z})[X]/\langle (X+1)(X+2)\rangle \simeq (\mathbb{Z}/3\mathbb{Z})[X]/\langle X+1\rangle \times (\mathbb{Z}/3\mathbb{Z})[X]/\langle X+2\rangle \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ but $\mathbb{Z}/3\mathbb{Z}$ is a field so the only ideals are $\langle 0\rangle$ and $\langle 1\rangle$.
Then there are 12 ideals of $\mathbb{Z}[\sqrt{-5}]$ which contain the element 6. ($12 = 3.2.2$). They are : $\mathbb{Z}[\sqrt{-5}]$, $\langle 6\rangle$, $\langle 2\rangle$, $\langle 3\rangle$, $\langle 1+\sqrt{-5}\rangle$, $\langle 1-\sqrt{-5}\rangle$, $\langle 2, 1+\sqrt{-5}\rangle$, $\langle 6, 3(1+\sqrt{-5})\rangle$, $\langle 3, 1+\sqrt{-5}\rangle$, $\langle 3, 1-\sqrt{-5}\rangle$, $\langle 6, 2(1+\sqrt{-5})\rangle$, $\langle 6, 2(1-\sqrt{-5})\rangle$. We find it while using the prime ideals $\mathfrak{p} = \langle 2, 1+\sqrt{-5}\rangle$, $\mathfrak{q} = \langle 3, 1+\sqrt{-5}\rangle$, $\mathfrak{r} = \langle 3, 1-\sqrt{-5}\rangle$.

6.3 How to make an ideal principal

We will work with several rings, hence write $\langle x\rangle_R$ to denote the ideal generated by x in the ring R.

Theorem 6.19. Let K be a number field, $\mathfrak{a}$ an ideal in the ring of integers $\mathfrak{O}_K$ of K. Then there exists an algebraic integer κ such that for $\mathfrak{O}' = \mathfrak{O}_{K(\kappa)}$ the ring of integers of $K(\kappa)$, we have:

(i) $\langle \kappa\rangle_{\mathfrak{O}'} = \langle \mathfrak{a}\rangle_{\mathfrak{O}'}$

(ii) $\langle \kappa\rangle_{\mathfrak{O}'} \cap \mathfrak{O}_K = \mathfrak{a}$

(iii) If $\mathbb{B}$ is the ring of all algebraic integers, then $\langle \kappa\rangle_{\mathbb{B}} \cap K = \mathfrak{a}$.

Proof. You can find a proof in [1] (Theorem 9.10 of [1]). □

Theorem 6.20. Let K be a number field with integers $\mathfrak{O}_K$, then there exists a number field $L \supseteq K$ with ring of integers $\mathfrak{O}_L$ such that for every ideal $\mathfrak{a}$ in $\mathfrak{O}_K$ we have:

(i) $\langle \mathfrak{a}\rangle_{\mathfrak{O}_L}$ is a principal idea,

(ii) $\langle \mathfrak{a}\rangle_{\mathfrak{O}_L} \cap \mathfrak{O}_K = \mathfrak{a}$.

Proof. You can find a proof in [1] (Theorem 9.12 of [1]). □

6.4 Unique factorization of elements in an extension ring

We have seen that there is always factorization into irreducibles in a noetherian ring but not always the unicity of that factorization. Then we try to find bigger rings where there is unique factorization.

Theorem 6.21. Suppose K is a number field with integers $\mathfrak{O}_K$. Then there exists an extension field $L \supseteq K$ with integers $\mathfrak{O}_L$ such that every non-zero, non-unit $a \in \mathfrak{O}_K$ has a factorization

$$a = p_1 p_2 ... p_r \quad (p_i \in \mathfrak{O}_L)$$

where the p_i are non-units in $\mathfrak{O}_L$, and the following property is satisfied:
Given any factorization in $\mathfrak{O}_K$: $a = a_1 ... a_s$ where the a_i are non units in $\mathfrak{O}_K$, there exist integers $1 \leqslant n_1 < ... n_s = r$ and a permutation π of $\{1, ..., r\}$ such that the following elements are associates in $\mathfrak{O}_L$:

$$\begin{gathered} a_1, p_{\pi(1)} p_{\pi(2)} \cdots p_{\pi(n_1)} \\ \cdots\cdots\cdots\cdots \\ a_s, p_{\pi(n_{s-1}+1)} p_{\pi(n_{s-1}+2)} \cdots p_{\pi(n_s)} \end{gathered}$$

Proof. You can find a proof in [1] (Theorem 9.13 of [1]). □

The following exercises are **not** a consequence of the three last theorems because $\mathbb{Z}[\sqrt{2}, \sqrt{-3}]$ is not the ring of integers of $\mathbb{Q}(\sqrt{2}, \sqrt{-3})$ and $\mathbb{Z}[\sqrt{-5}, \sqrt{2}]$ is not the ring of integers of $\mathbb{Q}(\sqrt{-5}, \sqrt{2})$. But we find an extension ring where respectively 6 and 14 have unique factorization and all the factorizations in $\mathbb{Z}[\sqrt{-6}]$ and $\mathbb{Z}[\sqrt{-10}]$ come from different groupings of the element of the unique factorization.

Exercise 5.6.
In $\mathbb{Z}[\sqrt{-6}]$ we have $6 = 2.3 = (\sqrt{-6})(-\sqrt{-6})$. Factorize these elements further in the extension ring $\mathbb{Z}[\sqrt{2}, \sqrt{-3}]$ as $6 = (-1)\sqrt{2}\sqrt{2}\sqrt{-3}\sqrt{-3}$. Show that if $\mathfrak{I}_1$ is the principal ideal in $\mathbb{Z}[\sqrt{2}, \sqrt{-3}]$ generated by $\sqrt{2}$, then $\mathfrak{p}_1 = \mathfrak{I}_1 \cap \mathbb{Z}[\sqrt{-6}] = \langle 2, \sqrt{-6} \rangle$. Demonstrate that $\mathfrak{p}_1$ is maximal in $\mathbb{Z}[\sqrt{-6}]$, hence prime; and find another prime ideal $\mathfrak{p}_2$ in $\mathbb{Z}[\sqrt{-6}]$ such that $\langle 6 \rangle = \mathfrak{p}_1^2 \mathfrak{p}_2^2$.

Solution.
We want to prove $\mathfrak{I}_1 \cap \mathbb{Z}[\sqrt{-6}] = \langle 2, \sqrt{-6} \rangle$ where $\mathfrak{I}_1$ is the principal ideal in $\mathbb{Z}[\sqrt{2}, \sqrt{-3}]$ generated by $\sqrt{2}$. If $\alpha \in \langle 2, \sqrt{-6} \rangle$ then $\alpha \in \mathbb{Z}[\sqrt{-6}]$ because $\langle 2, \sqrt{-6} \rangle$ is an ideal of $\mathbb{Z}[\sqrt{-6}]$. $2 = \sqrt{2}\sqrt{2} \in \mathfrak{I}_1$ and $\sqrt{-6} = \sqrt{2}\sqrt{-3} \in \mathfrak{I}_1$. Then $\langle 2, \sqrt{-6} \rangle \subset \mathfrak{I}_1$. It follows that $\langle 2, \sqrt{-6} \rangle \subset \mathfrak{I}_1 \cap \mathbb{Z}[\sqrt{-6}]$. Conversely, if $\alpha \in \mathfrak{I}_1$ then $\alpha = \sqrt{2}(a + b\sqrt{2} + c\sqrt{-3} + d\sqrt{-6}) = a\sqrt{2} + 2b + c\sqrt{-6} + 2d\sqrt{-3}$, and to have $\alpha \in \mathbb{Z}[\sqrt{-6}]$ then $a = d = 0$ so $\alpha = 2b + c\sqrt{-6} \in \langle 2, \sqrt{-6} \rangle$. It follows that $\mathfrak{I}_1 \cap \mathbb{Z}[\sqrt{-6}] = \langle 2, \sqrt{-6} \rangle$.
To prove that $\mathfrak{p}_1$ is maximal, it is the same approach than in Exercise 5.2, let I such that $\mathfrak{p}_1 \subsetneq I$, we want to prove that $I = \mathbb{Z}[\sqrt{-6}]$. Let α be in I but not in $\mathfrak{p}_1$. $\alpha = a + b\sqrt{-6}$ then $\alpha - b\sqrt{-6} = a$ and $\alpha - b\sqrt{-6}$ are still in I but not in $\mathfrak{p}_1$ otherwise α would be in $\mathfrak{p}_1$. Then use Euclidean division by 2. $a = 2q + r$ and $r = 1$ otherwise a would be in $\mathfrak{p}_1$. Then $1 = \alpha - b\sqrt{-6} - 2q \in I$, it follows that $I = \mathbb{Z}[\sqrt{-6}]$. We just proved that $\mathfrak{p}_1$ is maximal and then prime because all ideal maximal are prime (Corollary 6.5).
We can use the same operation with $\mathfrak{p}_2 = \mathfrak{I}_2 \cap \mathbb{Z}[\sqrt{-6}] = \langle 3, \sqrt{-6} \rangle$ where $\mathfrak{I}_2$ is the principal ideal in $\mathbb{Z}[\sqrt{2}, \sqrt{-3}]$ generated by $\sqrt{-3}$.

Then $\mathfrak{p}_1^2 = \langle 2, \sqrt{-6}\rangle\langle 2, \sqrt{-6}\rangle = \langle 4, -6, 2\sqrt{-6}\rangle \subset \langle 2\rangle$ and $\mathfrak{p}_2^2 = \langle 3, \sqrt{-6}\rangle\langle 3, \sqrt{-6}\rangle = \langle 9, -6, 3\sqrt{-6}\rangle \subset \langle 3\rangle$. It follows that $\mathfrak{p}_1^2\mathfrak{p}_2^2 \subset \langle 6\rangle$. Conversely, $54 = -3.3.\sqrt{-6}.\sqrt{-6} \in \mathfrak{p}_1^2\mathfrak{p}_2^2$ and $24 = -2.2.\sqrt{-6}\sqrt{-6} \in \mathfrak{p}_1^2\mathfrak{p}_2^2$, then $54 - 2 \times 24 = 6 \in \mathfrak{p}_1^2\mathfrak{p}_2^2$, it follows that $\langle 6\rangle \subset \mathfrak{p}_1^2\mathfrak{p}_2^2$ and now $\langle 6\rangle = \mathfrak{p}_1^2\mathfrak{p}_2^2$.

Exercise 5.7.
Factorize $14 = 2.7 = (2 + \sqrt{-10})(2 - \sqrt{-10})$ further in $\mathbb{Z}[\sqrt{-5}, \sqrt{2}]$ and by intersecting appropriate ideals with $\mathbb{Z}[\sqrt{-10}]$, factorize the ideal $\langle 14\rangle$ into prime (maximal) ideals in $\mathbb{Z}[\sqrt{-10}]$.

Solution.
We remind that $\mathbb{Z}[\sqrt{-10}]$ is well a ring of integers (Theorem 4.3) $14 = \sqrt{2}.\sqrt{2}.(\sqrt{2}+\sqrt{-5}).(\sqrt{2} - \sqrt{-5})$ is a factorization in $\mathbb{Z}[\sqrt{-5}, \sqrt{2}]$. Then we define $\mathfrak{p_1} = \mathfrak{J_1} \cap \mathbb{Z}[\sqrt{-10}] = \langle 2, \sqrt{-10}\rangle$ where $\mathfrak{J_1}$ is the principal ideal in $\mathbb{Z}[\sqrt{-5}, \sqrt{2}]$ generated by $\sqrt{2}$, $\mathfrak{p_2} = \mathfrak{J_2} \cap \mathbb{Z}[\sqrt{-10}] = \langle 2 + \sqrt{-10}, -5 + \sqrt{-10}\rangle$ where $\mathfrak{J_2}$ is the principal ideal in $\mathbb{Z}[\sqrt{-5}, \sqrt{2}]$ generated by $\sqrt{2}+\sqrt{-5}$ and $\mathfrak{p_3} = \mathfrak{J_3}\cap\mathbb{Z}[\sqrt{-10}] = \langle 2 - \sqrt{-10}, 5 + \sqrt{-10}\rangle$ where $\mathfrak{J_3}$ is the principal ideal in $\mathbb{Z}[\sqrt{-5}, \sqrt{2}]$ generated by $\sqrt{2} - \sqrt{-5}$. We assume that $\langle 14\rangle = \mathfrak{p_1^2p_2p_3}$.
For $\mathfrak{p_1}$ is the same proof than Exercise 5.6 while replacing $\sqrt{-6}$ by $\sqrt{-10}$ and $\sqrt{-3}$ by $\sqrt{-5}$. And we have that $\mathfrak{p_1}$ is maximal, hence prime.
For $\mathfrak{p_2}$, we have $2 + \sqrt{-10} \in \mathbb{Z}[\sqrt{-10}]$ and $-5 + \sqrt{-10} \in \mathbb{Z}[\sqrt{-10}]$. Then $2+\sqrt{-10} = \sqrt{2}(\sqrt{2}+\sqrt{-5})$ and $-5+\sqrt{-10} = \sqrt{-5}(\sqrt{2}+\sqrt{-5})$, it follows that $\langle 2 + \sqrt{-10}, -5 + \sqrt{-10}\rangle \subset \mathfrak{J_2} \cap \mathbb{Z}[\sqrt{-10}]$. Conversely, $\alpha = (\sqrt{2} + \sqrt{-5})(a + b\sqrt{2} + c\sqrt{-5} + d\sqrt{-10}) = (2b - 5c) + (a - 5d)\sqrt{2} + (a + 2d)\sqrt{-5} + (b + c)\sqrt{-10}$ where $a, b, c, d \in \mathbb{Z}$. Then $a = d = 0$ because α have to be in $\mathbb{Z}[\sqrt{-10}]$. Then $\alpha = b(2 + \sqrt{-10}) + c(-5 + \sqrt{-10}) \in \langle 2 + \sqrt{-10}, -5 + \sqrt{-10}\rangle$. It follows that $\mathfrak{J_2} \cap \mathbb{Z}[\sqrt{-10}] \subset \langle 2 + \sqrt{-10}, -5 + \sqrt{-10}\rangle$. And we have the equality.
To prove that $\mathfrak{p_2}$ is prime, we use Theorem 6.15. So we want to prove that $N(\mathfrak{p_2})$ is prime. We use the same ideas than Exercise 5.3. $N(\mathfrak{p_2}) = |\mathbb{Z}[\sqrt{-10}]/\mathfrak{p_2}| = |\mathbb{Z}[\sqrt{-10}]/\langle 2+\sqrt{-10}, -5+\sqrt{-10}\rangle| = |(\mathbb{Z}[\sqrt{-10}]/\langle -5+\sqrt{-10}\rangle)/\overline{\langle 2 + \sqrt{-10}\rangle}| = |(\mathbb{Z}[X]/\langle X^2 + 10\rangle/\overline{\langle -5 + \sqrt{-10}\rangle})/\langle 7\rangle| = |(\mathbb{Z}[X]/\langle X^2 + 10\rangle/\langle X - 5\rangle)/\langle 7\rangle| = \overline{|(\mathbb{Z}[X]/\langle X - 5\rangle/\overline{\langle X^2 + 10\rangle})/\langle 7\rangle|} = |(\mathbb{Z}/\langle 35\rangle)/\langle 7\rangle| = |\mathbb{Z}/\langle 7\rangle| = 7$. Because $\overline{2 + \sqrt{-10}} = 2+5$ in $(\mathbb{Z}[\sqrt{-10}]/\langle -5+\sqrt{-10}\rangle)$ since $-5+\sqrt{-10} \equiv 0$, $\overline{-5 + \sqrt{-10}} = X - 5$ in $\mathbb{Z}[X]/\langle X^2 + 10\rangle$ since $\sqrt{-10} \equiv X$, $\overline{X^2 + 10} = 35$ in $\mathbb{Z}[X]/\langle X - 5\rangle$ because $X \equiv 5$ and $\langle 35, 7\rangle = \langle 7\rangle$. It follows that $\mathfrak{p_2}$ is prime because 7 is also a prime.
We can do the same proof for $\mathfrak{p_3}$, while using the same ideas.
Now we have to prove that $\langle 14\rangle = \mathfrak{p_1^2p_2p_3}$ since they are all primes. $\mathfrak{p_1^2} = \langle 4, -10, 2\sqrt{-10}\rangle$, $\mathfrak{p_2p_3} = \langle 14, -35, 7\sqrt{-10}\rangle$ then $\mathfrak{p_1^2p_2p_3} = \langle 56, 140, 350, 28\sqrt{-10}, 70\sqrt{-10}\rangle$. But $14 = 350 - 2 \times 140 - 56$, it follows that $14 \in \mathfrak{p_1^2p_2p_3}$. Now we use the norm, we have seen that $N(\mathfrak{p_1}) = 2$, $N(\mathfrak{p_2}) = 7$,$N(\mathfrak{p_3}) = 7$, hence $N(\mathfrak{p_1^2p_2p_3}) = N(\mathfrak{p_1})^2N(\mathfrak{p_2})N(\mathfrak{p_3}) = 2^2.7.7 = 14^2$ (Proposition 6.12). And $N(\langle 14\rangle) = |N(14)| = 14^2$ (Corollary 6.14). It follows that $\langle 14\rangle = \mathfrak{p_1^2p_2p_3}$ because they have the same norm and we have an inclusion.

7 References

[1] I.STEWART and D.TALL, *Algebraic Number Theory*, First Edition LONDON CHAPMAN AND HALL

[2] I.STEWART, *Galois Theory*, Third Edition CHAPMAN AND HALL

[3] HENDRIK W. LENSTRA, JR., *Solving the Pell's equation*, 2008

[4] CONRAD, *Discriminant of Composite Fields*, Stanford

[5] K.WILLIAMS, *Integers of Biquadratic Field*, Canadian Mathematical Bulletin, Volume 13, Number 4, December 1970

[6] D. DUSAN, *Pell's Equations*, IMO Maths, 2007

[7] D.S. DUMMIT and R.M. FOOTE, *Abstract Algebra*, 3rd Edition 2003