Solutions of the *Algebraic Number Theory* Exercises

Pierre Le Barbenchon

Contents

1 Introduction

All these exercises come from *Algebraic Number Theory* of Ian STEWART and David TALL. This article wants to be a solution book of *Algebraic Number Theory*. The solutions that would be presented are not official. Unless otherwise specified, all the references come from *Algebraic Number Theory*. Then "Theorem 1.7" will be the 7^{th} theorem in the first part of the book.

I'm a mathematical student in the Ecole Normale Supérieure of Rennes in France. I start to write these corrections during my internship in Oxford with Konstantin Ardakov, mathematical professor of the University of Oxford.

I try to write as clearly as possible to be understood by everyone (even so with a mathematical background). It's the first book of corrections that I have

ever written, so the solutions are may be not clear enough, there are probably some mistakes. Please tell me if you find some.

I would like to thank Tobias Schmidt for teaching me the basis of Algebra and mostly Konstantin Ardakov who gave me keys and background to better understand algebraic number theory. Thanks for all his kindness and his help on the different exercises that are presented in this article.

2 Notations

We use all the same notations than in *Algebraic Number Theory* and we add the following notations :
- $[t_1, ..., \hat{t_i}, ..., \hat{t_j}, ..., t_n]$ is equivalent to $[t_1, ..., t_{i-1}, t_{i+1}, ..., t_{j-1}, t_{j+1}, ..., t_n]$. We remove t_i and t_j.
- $[\![1, n]\!]$ is equivalent to $\{1, 2, ..., n\}$.
- $A \backslash B$ is the set of the elements that are in A but not in B.
- $A^\times$ is the set of the non-zero elements of A.
- A^* is the set of the units of A.
- $\varphi : A \hookrightarrow B$ implies that φ is injective.
- $\varphi : A \twoheadrightarrow B$ implies that φ is surjective.
- $\mathrm{Im}(\varphi)$ is the image of φ.
- $\mathrm{Ker}(\varphi)$ is the kernel of φ.
- $a \equiv b\ [n]$ is equivalent to $a \equiv b \pmod{n}$, i.e. $n \mid (a - b)$.
- $\lfloor x \rfloor$ is the integer part of x, we have $\lfloor x \rfloor \leqslant x < \lfloor x \rfloor + 1$.
- ${}^tA$ is the transpose of the matrix A.

3 Theory Prerequisites

As we are still telling you, we need all the theory of *Algebraic Number Theory* and we add the following results :

- *Theorem* 1. 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

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

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

Proof. Take $\beta \in \mathfrak{O}_K \backslash (b_1\mathbb{Z} + ... + b_n\mathbb{Z})$ (it 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 $\mathrm{hcf}(N, c_1, c_2, ..., c_n) = 1$. Let p a prime such that $p \mid N$ and

it exists j such that $p \nmid c_j$. Take $\beta' = \frac{N}{p}\beta = \frac{1}{p}\sum_{i=1}^{n} c_i b_i \in \mathfrak{O}_K$ (because $p \mid N$). But $\mathrm{hcf}(c_j, p) = 1$, then it exists $k, l \in \mathbb{Z}$ such that $c_j k + pl = 1$. Take $\beta'' = k\beta' + lb_j \in \mathfrak{O}_K$, $\beta'' = \frac{1}{p}\sum_{i=1}^{n} s_i b_i$ 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 $\alpha = \beta'' - \sum m_i b_i = \frac{1}{p}\sum_{i=1}^{n} \lambda_i b_i$.

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 $p^2 \mid \Delta[b_1, ..., b_n]$.

□

We use that theorem to compute integral basis (cf [5] of the references, paragraph "Computing an integral basis"), it will help for Exercises 2.4, 2.6, 2.7, 2.8.

- We need to know how we calculate a determinant of a matrix.

- Pell's Equation (cf [3] of the references, the part 5. "Power Products" and reference [6]).

- Galois Theory and in particular the correspondance between subfields and subgroups. We give an example of exercise to show what to know :

  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), hence there are 4 monomorphisms (Theorem 2.3): $\phi_1 : \zeta \mapsto \zeta$, $\phi_2 : \zeta \mapsto \zeta^2$, $\phi_3 : \zeta \mapsto \zeta^3$, $\phi_4 : \zeta \mapsto \zeta^4$. 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 $\dfrac{-1 \pm \sqrt{5}}{2}$. 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 $\mathbb{Q}(\zeta)$.

- *Theorem* 2 (Structure Theorem for finitely generated abelian group). Let G be a finitely generated abelian group, then there exists $n \in \mathbb{N}$, $n_1, ..., n_k$ such that $n_{i+1} \mid n_i$ for all $i \in [\![1, k-1]\!]$ and we have $G \simeq \mathbb{Z}^n \times (\mathbb{Z}/n_1\mathbb{Z}) \times ... \times (\mathbb{Z}/n_k\mathbb{Z})$.

  Remark. You can find a proof in *Abstract Algebra* by Dummit and Foote (third edition) Section 5.2.

- *Theorem* 3 (First isomorphism theorem). Let A and B be rings and let $\varphi : A \to B$ be a morphism. Then $\mathrm{Im}(\varphi)$ is isomorphic to the quotient $A/\ \mathrm{Ker}(\varphi)$. In particular, if φ is surjective, we have B isomorphic to the quotient $A/\ \mathrm{Ker}(\varphi)$.

- *Theorem* 4 (Correspondence theorem for ideals). Let A be a ring, I, J ideals of A, then if $I \subset J$, we have $A/J \simeq (A/I)/\overline{J}$ where $\overline{J}$ is the projection of J in A/I.

-

Proposition 3.1. Let A be a ring. Let I and J be coprime ideals (i.e. $I + J = A$). Then $IJ = I \cap J$.

Proof. We have $IJ \subset I \cap J$ because $IJ \subset I$ and $IJ \subset J$ by definition of ideals. Conversely, let $z \in I \cap J$, we can find $x \in I$ and $y \in J$ such that $x+y = 1$ because $1 \in A = I+J$. Then $z = xz+zy \in IJ$ because $xz \in IJ$ and $zy \in IJ$. It follows that $I \cap J \subset IJ$. □

Theorem 5 (Chinese Remainder Theorem). Let A be a ring. Let I and J be coprime ideals (i.e. $I + J = A$). Then $A/IJ \simeq A/I \times A/J$.

4 Exercises

4.1 Algebraic Background p.35

Exercise 1.1.
Show that Theorem 1.1 becomes false if the word 'finite' is omitted from the hypotheses.

Solution. For instance, $\mathbb{Z}$ is an integral domain but is not a field (because, for example, 2 is not a unit) and $\mathbb{Z}$ is not finite.

Exercise 1.2.
Which of the following polynomials over $\mathbb{Z}$ are irreducible ?

(a) $x^2 + 3$

(b) $x^2 - 169$

(c) $x^3 + x^2 + x + 1$

(d) $x^3 + 2x^2 + 3x + 4$

Solution. (a) $x^2 + 3$ is irreducible. To prove it, we can use the Eisenstein's criterion with $p = 3$ because $p \nmid 1$, $p \mid 3$ and $p^2 \nmid 3$.

(b) $x^2 - 169$ is reducible. We can write $x^2 - 169 = (x + 13)(x - 13)$ and each factor is neither a unit, nor zero.

(c) x^3+x^2+x+1 is reducible. We can write $x^3+x^2+x+1 = (x^2+1)(x+1)$.

(d) $P = x^3 + 2x^2 + 3x + 4$ is irreducible. While using the Theorem 1.6 with $n = 3$, we have $\overline{P} = x^3 + 2x^2 + 1$ and we know that polynomials of degree 3 are reducible if and only if they have a zero in the field. Since $\overline{P}(0) = 1$, $\overline{P}(1) = 1$ and $\overline{P}(2) = 2$, $\overline{P}$ is irreducible and then P is irreducible because $\partial P = \partial \overline{P}$.

Exercise 1.3.
Write down some polynomials over $\mathbb{Z}$ and factorize them into irreducibles.

Solution. For example,

- $X^2 + 2X - 3 = (X - 1)(X + 3)$
- $X^3 + 2X^2 + 2X + 1 = (X + 1)(X^2 + X + 1)$
- $X^4 - 5X^2 + 4 = (X + 1)(X - 1)(X + 2)(X - 2)$

Exercise 1.4.
Does Theorem 1.2 remain true over a field of characteristic $p > 0$?

Solution. No, it doesn't because if we take the field $\mathbb{Z}/2\mathbb{Z}(X)$ which is the field of fractions of the ring $\mathbb{Z}/2\mathbb{Z}[X]$ (its characteristic is 2), we can consider the polynomial on $\mathbb{Z}/2\mathbb{Z}(X)$, $P(Y) = Y^3 - XY = Y(Y^2 - X)$ which give $P'(Y) = 3Y^2 - X = Y^2 - X$ because the characteristic is 2. And so P and P' have a commun factor but P is not divisible by the square of a polynomial of degree > 0.

Exercise 1.5.
Find the minimum polynomial over $\mathbb{Q}$ of

(i) $(1 + i)/\sqrt{2}$

(ii) $i + \sqrt{2}$

(iii) $e^{2\pi i/3} + 2$

Solution. (i) The minimum polynomial of $\theta = (1+i)/\sqrt{2}$ is $X^4 + 1$. Because $\theta^2 = i$ and $i^2 = -1$, so $\theta^4 + 1 = 0$. Then we can observe that 1, θ, θ^2 and θ^3 are $\mathbb{Q}-$linearly independant because $\theta \in \mathrm{Vect}_{\mathbb{Q}}(i\sqrt{2} + \sqrt{2})$, $\theta^2 \in \mathrm{Vect}_{\mathbb{Q}}(i)$ and $\theta^3 \in \mathrm{Vect}_{\mathbb{Q}}(i\sqrt{2} - \sqrt{2})$ and$\{1, i\sqrt{2} + \sqrt{2}, i, i\sqrt{2} - \sqrt{2}\}$ form an $\mathbb{Q}-$linearly independant family.

(ii) The minimum polynomial of $i + \sqrt{2}$ is $X^4 - 2X^2 + 9$. For the same raisons that before.

(iii) The minimum polynomial of $e^{2\pi i/3} + 2$ is $X^2 - 3X + 3$. Because we can see that $e^{2\pi i/3} \notin \mathbb{Q}$ so $e^{2\pi i/3} + 2$ neither and then we can't find a polynomial over $\mathbb{Q}$ with degree 1 that have $e^{2\pi i/3} + 2$ as a zero.

Exercise 1.6.
Find the degrees of the following field extensions :

(a) $\mathbb{Q}(\sqrt{7}) : \mathbb{Q}$

(b) $\mathbb{C}(\sqrt{7}) : \mathbb{C}$

(c) $\mathbb{Q}(\sqrt{5}, \sqrt{7}, \sqrt{35}) : \mathbb{Q}$

(d) $\mathbb{R}(\theta) : \mathbb{R}$ where $\theta^3 - 7\theta + 6 = 0$ and $\theta \notin \mathbb{R}$

(e) $\mathbb{Q}(\pi) : \mathbb{Q}$

Solution. (a) $[\mathbb{Q}(\sqrt{7}) : \mathbb{Q}] = 2$ because of the Theorem 1.8 with $X^2 - 7$ the minimum polynomial of $\sqrt{7}$. (It's the minimum polynomial because $\sqrt{7} \notin \mathbb{Q}$ so $X^2 - 7$ is irreducible in $\mathbb{Q}$)

(b) $[\mathbb{C}(\sqrt{7}) : \mathbb{C}] = 1$ because $\sqrt{7} \in \mathbb{C}$ so $\mathbb{C}(\sqrt{7}) : \mathbb{C} = \mathbb{C}$ which is a vector space on the field $\mathbb{C}$ and the dimension is 1.

(c) $[\mathbb{Q}(\sqrt{5}, \sqrt{7}, \sqrt{35}) : \mathbb{Q}] = 4$. Because $\mathbb{Q}(\sqrt{5}, \sqrt{7}, \sqrt{35}) = \mathbb{Q}(\sqrt{5}, \sqrt{7})$ (1), $[\mathbb{Q}(\sqrt{5}, \sqrt{7}) : \mathbb{Q}(\sqrt{5})] = 2$, $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2$ (as it is done in the (a) and because $\sqrt{7} \notin \mathbb{Q}(\sqrt{5})$) and
$[\mathbb{Q}(\sqrt{5}, \sqrt{7}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{5}, \sqrt{7}) : \mathbb{Q}(\sqrt{5})][\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2 \times 2 = 4$ (Theorem 1.7)
To prove (1), we can see that $\mathbb{Q}(\sqrt{5}, \sqrt{7}) \subset \mathbb{Q}(\sqrt{5}, \sqrt{7}, \sqrt{35})$ because $\sqrt{5}$ and $\sqrt{7} \in \mathbb{Q}(\sqrt{5}, \sqrt{7}, \sqrt{35})$ so $\mathbb{Q}(\sqrt{5}, \sqrt{7}) \subset \mathbb{Q}(\sqrt{5}, \sqrt{7}, \sqrt{35})$ because it's the smallest field that contains $\mathbb{Q}, \sqrt{5}$ and $\sqrt{7}$. Conversely, $\sqrt{35} = \sqrt{5}\sqrt{7}$ so $\sqrt{35} \in \mathbb{Q}(\sqrt{5}, \sqrt{7})$ because it's a field. Then $\mathbb{Q}(\sqrt{5}, \sqrt{7}, \sqrt{35}) \subset \mathbb{Q}(\sqrt{5}, \sqrt{7})$. It follows that $\mathbb{Q}(\sqrt{5}, \sqrt{7}, \sqrt{35}) = \mathbb{Q}(\sqrt{5}, \sqrt{7})$.

(d) $\mathbb{R}(\theta) : \mathbb{R}$ where $\theta^3 - 7\theta + 6 = 0$ and $\theta \notin \mathbb{R}$. We have $X^3 - 7X + 6 = (X - 1)(X - 2)(X + 3)$ then all the roots of this polynomial are real. It follows that θ doesn't exist, $\mathbb{R}(\varnothing) = \mathbb{R}$ and $[\mathbb{R} : \mathbb{R}] = 1$, so $[\mathbb{R}(\theta) : \mathbb{R}] = 1$.

(e) $[\mathbb{Q}(\pi) : \mathbb{Q}] = \infty$ because π is transcendental.

Exercise 1.7.
Let K be the field generated by the elements $e^{2\pi i/n}$ $(n = 1, 2, ...)$. Show that K is an algebraic extension of $\mathbb{Q}$, but that $[K : \mathbb{Q}]$ is not finite. (It may help to show that the minimum polynomial of $e^{2\pi i/p}$ for p prime is $t^{p-1} + t^{p-2} + ... + 1$.)

Solution. By definition of the field generated by the elements $e^{2\pi i/n}$ $(n = 1, 2, ...)$, it's all the **finite** combinaisons of generators, so for each element α of K, is in a $\mathbb{Q}(e^{2\pi i/n_1}, ..., e^{2\pi i/n_N})$ with $N < \infty$. Then α is algebraic because $\mathbb{Q}(e^{2\pi i/n_1}, ..., e^{2\pi i/n_N})$ is (Because all the generators are algebraic and there is a finite number of generators). It follows that K is an algebraic extension of $\mathbb{Q}$.

Use that $\mathbb{Q}(e^{2\pi i/p}) \subset \mathbb{Q}((e^{2\pi i/q})_{q \in \mathscr{P}}) \subset \mathbb{Q}((e^{2\pi i/n})_{n \in \mathbb{N}}) = K$ for all p prime (where $\mathscr{P}$ is the set of primes) and the minimum polynomial of $e^{2\pi i/p}$ for p prime is $t^{p-1} + t^{p-2} + ... + 1$ (Lemma 3.4). Then see that $[Q(e^{2\pi i/p}) : \mathbb{Q}] = p - 1$ is as big as we want, so $[\mathbb{Q}((e^{2\pi i/q})_{q \in \mathscr{P}}) : \mathbb{Q}] = \infty$. It follows that $[K : Q] = \infty$.

Exercise 1.8.
Express the following polynomials in terms of elementary symmetric polynomials, where this is possible.

(a)	$t_1^2 + t_2^2 + t_3^2$	$(n = 3)$
(b)	$t_1^3 + t_2^3$	$(n = 2)$
(c)	$t_1t_2^2 + t_2t_3^2 + t_3t_1^2$	$(n = 3)$
(d)	$t_1 + t_2^2 + t_3^3$	$(n = 3)$

Solution. (a) $P(t_1, t_2, t_3) = t_1^2 + t_2^2 + t_3^2$ is a symmetric polynomial and $P = s_1^2 - 2s_2$. ($s_1 = t_1 + t_2 + t_3$ and $s_2 = t_1t_2 + t_2t_3 + t_3t_1$)

(b) $P(t_1, t_2) = t_1^3 + t_2^3$ is a symmetric polynomial and $P = s_1^3 - 3s_1s_2$. ($s_1 = t_1 + t_2$ and $s_2 = t_1t_2$)

(c) $P(t_1, t_2, t_3) = t_1t_2^2 + t_2t_3^2 + t_3t_1^2$ is not a symmetric polynomial because $P(t_3, t_2, t_1) \neq P(t_1, t_2, t_3)$, so it exists a permutation π such that $P^\pi \neq P$.

(d) $P(t_1, t_2, t_3) = t_1+t_2^2+t_3^3$ is not a symmetric polynomial because $P(t_3, t_2, t_1) \neq P(t_1, t_2, t_3)$, so it exists a permutation π such that $P^\pi \neq P$.

Exercise 1.9.
A polynomial belonging to $\mathbb{Z}[t_1, ..., t_n]$ is said to be *antisymmetric* if it is invariant under even permutations of the variables, but changes sign under odd permutations. Let $\Delta = \prod_{i<j}(t_i - t_j)$.
Show that Δ is antisymmetric. If f is any antisymmetric polynomial, prove that f is expressible as a polynomial in the elementary symmetric polynomials, together with Δ. (*Hint :* consider f/Δ)

Solution. All permutations can be written as a composition of several transpositions, and if there is an odd number of transpositions, the permutation is an odd permutation and if there is an even number of transpositions, the permutation is even. Then we have just to prove that under one transposition, Δ will change its sign. Therefore, let σ be an even permutation, σ is the composition of $2k$ transpositions (with $k \in \mathbb{N}$). Then, $\Delta_\sigma = (-1)^{2k}\Delta = \Delta$. If σ is an odd permutation, σ will be the composition of $2k + 1$ transpositions (with $k \in \mathbb{N}$).Then, $\Delta_\sigma = (-1)^{2k+1}\Delta = -\Delta$. (with $\Delta_\sigma = \prod_{i<j}(t_{\sigma(i)} - t_{\sigma(j)})$.

Let prove that under one transposition, Δ will change its sign. If we take the transposition that interchanges k and l with $k < l$. We remind $\Delta = \prod_{i<j}(t_i - t_j)$. If $i, j \notin \{k, l\}$, $(t_i - t_j) = (t_{\sigma(i)} - t_{\sigma(j)})$ by definition of permutation. For $i = k$ and $j = l$, $(t_k - t_l) = -(t_{\sigma(k)} - t_{\sigma(l)})$. Let consider the factors which contain only one k or l. If $i < k < l$, $(t_i-t_k)(t_i-t_l) = (t_i-t_{\sigma(l)})(t_i-t_{\sigma(k)})$, if $k < l < j$, $(t_k - t_j)(t_l - t_j) = (t_{\sigma(l)} - t_j)(t_{\sigma(k)} - t_j)$ and if $k < i < l$, $(t_k - t_i)(t_i - t_l) = (t_{\sigma(l)} - t_i)(t_i - t_{\sigma(k)}) = -(t_{\sigma(k)} - t_i) \times -(t_i - t_{\sigma(l)}) = (t_{\sigma(k)} - t_i)(t_i - t_{\sigma(l)})$.

Then the only term that get a (-1) is when $i = k$ and $j = l$. It follows that $\Delta_\sigma = \prod_{i<j}(t_{\sigma(i)} - t_{\sigma(j)}) = -\prod_{i<j}(t_i - t_j) = -\Delta$. So, Δ is antisymmetric.

Now, prove $\frac{f}{\Delta}$ is a polynomial. We want to prove that $\Delta | f$. Simply prove that all $(t_i - t_j)$ divide f because they are irreducible in $\mathbb{Z}[t_1, ..., t_n]$ (Just factorize f in irreducible). f is antisymmetric so let σ is the transposition (ij), $f^\sigma = -f$ in $\mathbb{Z}[t_1, ..., \hat{t_i}, ..., \hat{t_j}, ..., t_n][ti, tj]$. And by change of variables : $(t_i, t_j) \to (t_i, z = t_i - t_j)$ we have $f(z) = -f(-z)$ but f is a polynomial ($f = a_0(t_i) + a_1(t_i)z + ... + a_N(t_i)z^N$), then $a_0(t_i) = 0$. So $f = z(a_1(t_i) + ...a_N(t_i)z^{N-1})$ and $z | f$.

Then $\frac{f}{\Delta}$ is symmetric because under even permutation $\frac{f^\sigma}{\Delta^\sigma} = \frac{f}{\Delta}$ and under odd permutation $\frac{f^\sigma}{\Delta^\sigma} = \frac{-f}{-\Delta} = \frac{f}{\Delta}$. We can use Theorem 1.9 and $\frac{f}{\Delta}$ can be express with elementary symmetric polynomials, then f can be expressed with Δ and elementary symmetric polynomials.

Exercise 1.10.
Find the orders of the groups G/H where G is free abelian with $\mathbb{Z}-$basis, x, y, z and H is generated by :

(a) $2x, 3y, 7z$

(b) $x + 3y - 5z, 2x - 4y, 7x + 2y - 9z$

(c) x

(d) $41x + 32y - 999z, 16y + 3z, 2y + 111z$

(e) $41x + 32y - 999z$.

Solution. (a) We use the consequency of the Theorem 1.13 and so $|G/H| = |\det(a_{i,j})| = \left|\begin{vmatrix} 2 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 7 \end{vmatrix}\right| = |2 \times 3 \times 7| = 42$

(b) Similarly, $|G/H| = \left|\begin{vmatrix} 1 & 3 & -5 \\ 2 & -4 & 0 \\ 7 & 2 & -9 \end{vmatrix}\right| = |36 - 20 - 120 + 54| = 70$

(c) $|G/H| = \infty$ because we have a control just on a variable, if we see G as $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ and H as $\mathbb{Z}$, so G/H is $\mathbb{Z} \times \mathbb{Z}$ and the order is well infinity.

(d) Again, $|G/H| = \left|\begin{vmatrix} 41 & 32 & -999 \\ 0 & 16 & 3 \\ 0 & 2 & 111 \end{vmatrix}\right| = |41(16 \times 111 - 2 \times 3)| = 72570$

(e) We can find a change of basis to be in the case (c) with the transformation matrix $\begin{bmatrix} 41 & 0 & 0 \\ 32 & 1 & 0 \\ -999 & 0 & 1 \end{bmatrix}$ then if we call this basis $\{u, v, w\}$ with $u = 41x + 32y - 999z, v = y, w = z$, we are exactly in the case (c) with H generated by u.

Exercise 1.11.
Let K be a field. Show that M is a $K-$module if and only if it is a vector space over K. Show that the submodules of are precisely the vector subspaces. Do these statements remain true if we do not use convention (d) for modules ?

Solution. If we have M a $K-$module, we want to prove that M is a vector space over K. We know that M is an abelian group (by definition) and then we take α the function of the module as the scalar multiplication (it's fine because K is a field). The four properties of a vector space are satisfied because of the four properties that α does satisfy. So M is a vector space over K. Conversely, the field K is well also a ring, the application α is the scalar multiplication of the vector space and does satisfy the four properties of the module so M is a $K-$module. Then, if N is a submodule of M which is a module and a vector space, if we take $r \in K$ and $x, y \in N$ then $rx \in N$ because N is a submodule and $rx + y \in N$ because it's a groupe, and $0 \in N$ because $0 \in K$, so N is a vector subspace of M. Conversely, if N is a vector subspace of M, if we take $r \in K$ and $x \in N$, we have $rx \in N$ so N is a submodule of M. If we don't use the convention (d) of the definition of module, we have juste the implication "vector space $\implies$ module"

Exercise 1.12.
Let $\mathbb{Z}$ be a $\mathbb{Z}-$module with the obvious action. Find all the submodules.

Solution. Let N be a sub$\mathbb{Z}-$module of $\mathbb{Z}$, so N is a subgroup of $\mathbb{Z}$ for addition and, for $n \in N$ and $m \in \mathbb{Z}$ we have $nm \in N$, so N is an ideal of $\mathbb{Z}$ by definition of ideals. And ideals are sub$\mathbb{Z}-$module of $\mathbb{Z}$. So all the submodules are the ideals of $\mathbb{Z}$ which can be written $n\mathbb{Z}$ for $n \in \mathbb{N}$.
Proof of it : Let I be an ideal of $\mathbb{Z}$, if $I = \{0\}$ then $I = 0\mathbb{Z}$, else $I \neq \{0\}$, we take $n = \min\{x \in I / x > 0\}$. We have $n \in I$, so $n\mathbb{Z} \subset I$ by definition of an ideal ($\forall m \in \mathbb{Z}$ and $n \in I$ then $nm \in I$). Conversely, let a be in I, do the euclidean division by n, we find $a = nq + r$. $a \in I$ and $nq \in I$ so $r \in I$ (because I is a subgroup of $\mathbb{Z}$ for addition) but $r < n$ by definition of euclidean division, so if $r > 0$ then there is a contradiction with the definition of n. Then $r = 0$, and now $a = nq \in n\mathbb{Z}$. It follows that $I \subset n\mathbb{Z}$ and finally $I = n\mathbb{Z}$ with $n \in \mathbb{N}$.

Exercise 1.13.
Let R be a ring, and let M be a finitely generated $R-$module. Is it true that M necessarily has only finitely many distinct $R-$submodules ? If not, is there an extra condition on R which will lead to this conclusion ?

Solution. No, it isn't. For example, let R be the ring $\mathbb{R}[X_1, X_2, ...]$. All the polynomials are with a finite number of indeterminates. So R is a finitely generated $R-$module. But the submodule $\Omega = \{P \in R / P(0) = 0\}$ is not finitely generated. (There is no finite generators for Ω because the constraint is on the constant term and the rest is free). An extra condition is to consider that R is noetherian.

Exercise 1.14.
An abelian group G is said to be *torsion-free* if $g \in G$, $g \neq 0$ and $kg = 0$ for $k \in \mathbb{Z}$ implies $k = 0$. Prove that a finitely generated torsion-free belian group is a finitely generated free group.

Solution. We can use the structure theorem for finitely generated abelian group (Theorem 2), hence $G \simeq \mathbb{Z}^n \times (\mathbb{Z}/q_1\mathbb{Z}) \times ... \times (\mathbb{Z}/q_k\mathbb{Z})$ where $q_i \in \mathbb{N}$. But G is torsion free, we assume that all $q_i = 0$. Because if one $q_i > 0$ then for $x \neq 0$, $q_i x = 0$ in $\mathbb{Z}/q_i\mathbb{Z}$ and there is a contradiction with the torsion-free property. It follows that $G \simeq \mathbb{Z}^n$, then we can find a basis $\{x_1, ...x_n\}$ of G and G is well a finitely free group.

Alternative proof without using the structure theorem: A finitely generated abelian groupe G is a finitely generated free group if there exists a basis of G (independent family that generates G). We have generators by definition, and we assume that the *torsion-free* property will gave us the independence, namely that $\sum_{k=1}^{n} \lambda_i x_i = 0$ implies that all $\lambda_i = 0$. Let take $\mathcal{G} = \{x_1, ..., x_n\}$ a minimal generating set of G ("minimal" is to understand as the smallest cardinal of a generating set of G). Suppose $\sum_{k=1}^{n} \lambda_i x_i = 0$ where $\lambda_i \in \mathbb{Z}$, let d be the hcf of the λ_i,hence for all i, $\lambda_i = d\mu_i$where $\mu_i \in \mathbb{Z}$ and $\text{hcf}((\mu_i)) = 1$ then $d\sum_{k=1}^{n} \mu_i x_i = 0$, but G is torsion-free then, since $d \neq 0$, we have $\sum_{k=1}^{n} \mu_i x_i = 0$ with $\text{hcf}((\mu_i)) = 1$.

We want to prove that if we replace x_i with $x_i' = x_i - ax_j$ where $i \neq j$ and $a \in \mathbb{Z}$, then $\mathcal{G}' = \{x_1, ..., x_i', ...x_n\}$ is still a minimum generating set of G. $\{x_1, ..., x_i', ...x_n\}$ generates G because if we take x in G, then $x = \lambda_1 x_1 + ... + \lambda_i x_i + ... + \lambda_j x_j + ... + \lambda_n x_n = \lambda_1 x_1 + ... + \lambda_i x_i' + ... + (\lambda_j - a\lambda_i)x_j + ... + \lambda_n x_n$ because $x_i' = x_i - ax_j$, hence we write x with only elements of $\{x_1, ..., x_i', ...x_n\}$. It's still minimal because we didn't change the cardinal of the set, we still have n elements.

Then we can write $\lambda_1 x_1 + ... + \lambda_i x_i' + ... + (\lambda_j - a\lambda_i)x_j + ... + \lambda_n x_n = 0$, then we use the Euclidean's algorithm to find α_i such that $\sum_{i=1}^{n} \alpha_i \lambda_i = 1$. We can do all the transformation (that we have just seen) necessarily to have a $\tilde{x}_i$ such that the new coefficient in front of it is ± 1. Now we have $\tilde{\lambda}_1\tilde{x}_1 + ... \pm \tilde{x}_i + ... + \tilde{\lambda}_n\tilde{x}_n = 0$, it follows that we can write $\pm\tilde{x}_i = \sum_{k \neq i} \tilde{\lambda}_k \tilde{x}_k$, hence there is a contradiction with the fact that it's a minimal generating set of G. Then all the coefficient are zero and we have the independence, hence G is a finitely generated free group.

Exercise 1.15.
By examining the proof of Theorem 1.12 carefully, or by other means, prove that if H is a subgroup of a free group G of rank n then there exists a basis

$u_1, ..., u_n$ for G and a basis $v_1, ..., v_s$ for H where $s \leqslant n$ and $v_i = \alpha_i u_i$ $(1 \leqslant i \leqslant s)$ where the α_i are positive integers and α_i divides α_{i+1} $(1 \leqslant i \leqslant s-1)$.

Solution. We use exactly the same proof to find all the positive α_i of the Theorem 1.12. Then we have a matrix $A = \begin{bmatrix} \alpha_1 & & 0 \\ & \ddots & \\ 0 & & \alpha_s \end{bmatrix}$ to express the generators of H in the extraction $u_1, ...u_s$ of the basis $u_1, ..., u_n$ of G.

Take the extraction $\tilde{A} = \begin{bmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{bmatrix}$ of A. If $\alpha_1 \nmid \alpha_2$ then let $d_1 = \text{hcf}(\alpha_1, \alpha_2)$ we have $\alpha_1 = d_1\alpha_1'$ and $\alpha_2 = d_1\alpha_2'$, we have $\alpha_1'\alpha_2 = \alpha_1'd_1\alpha_2' = \alpha_1\alpha_2'$ and there exist $r,\ t$ such that $\alpha_1 r + \alpha_2 t = d_1$. It follows that the matrix $C = \begin{bmatrix} r & -\alpha_2' \\ t & \alpha_1' \end{bmatrix}$ is inversible because $\det C = \alpha_1' r + \alpha_2' t = 1$, then Cu where $u = {}^t(u_1, ..., u_s)$ is still a basis of $\text{Vect}(u_1, ..., u_s)$. We have $\tilde{A}C = \begin{bmatrix} r\alpha_1 & -\alpha_2'\alpha_1 \\ t\alpha_2 & \alpha_1'\alpha_2 \end{bmatrix}$. Then add the second row to the first one to have $\begin{bmatrix} d_1 & 0 \\ t\alpha_2 & \alpha_1'\alpha_2 \end{bmatrix}$. And replace R_2 by $R_2 - \alpha_2' t R_1$ where R_1 is the first row and R_2 the second one. We have now $\begin{bmatrix} d_1 & 0 \\ 0 & \alpha_1' d_1 \alpha_2' \end{bmatrix}$ Then we have created new generators such that $d_1 \mid d_1\alpha_1'\alpha_2'$.

Now iterate the process with $\begin{bmatrix} \alpha_1'\alpha_2' & 0 \\ 0 & \alpha_3 \end{bmatrix}$ if we had $\alpha_1 \nmid \alpha_2$ and with $\begin{bmatrix} \tilde{\alpha_2} & 0 \\ 0 & \alpha_3 \end{bmatrix}$ if we had $\alpha_1 \mid \alpha_2$ where $\alpha_2 = \alpha_1\tilde{\alpha_2}$. The process ends because there is a finite number of iterations.

Then we find a new basis where $d_1 \mid d_1 d_2 \mid ... \mid d_1 d_2 ... d_{s-1}\alpha_{s-1}'\alpha_s'$.

4.2 Algebraic Numbers p.56

Exercise 2.1.
Which of the following complex numbers are algebraic ? Which are algebraic integers ?

(a) $355/113$

(b) $e^{2\pi i/23}$

(c) $e^{\pi i/23}$

(d) $\sqrt{17} + \sqrt{19}$

(e) $(1 + \sqrt{17})/(2\sqrt{-19})$

(f) $\sqrt{1 + \sqrt{2}} + \sqrt{1 - \sqrt{2}}$.

Solution. We consider that it's algebraic over $\mathbb{Q}$.

(a) $\theta = 355/113$ is algebraic because $113\theta - 355 = 0$ but θ is not an algebraic integer because the algebraic integers of $\mathbb{Q}$ are the rational integers (Lemma 2.13).

(b) $\theta = e^{2\pi i/23}$ is algebraic and an algebraic integer because $\theta^{23} - 1 = 0$

(c) $\theta = e^{\pi i/23}$ is algebraic and an algebraic integer because $\theta^{23} + 1 = 0$

(d) $\theta = \sqrt{17}+\sqrt{19}$ is algebraic and an algebraic integer because $\theta^4-72\theta^2+4 = 0$

(e) $\theta = (1 + \sqrt{17})/(2\sqrt{-19})$ is algebraic because $5776\theta^4 + 2736\theta^2 - 256 = 0$ but it's not an algebraic integer because its minimal polynomial over $\mathbb{Q}$ has not its coefficients in $\mathbb{Z}$. (Theorem 2.12) (the definition of minimal polynomial implies that the leading coefficient is 1)

(f) $\theta = \sqrt{1+\sqrt{2}} + \sqrt{1-\sqrt{2}}$ is algebraic and an algebraic integer because $\theta^4 - 4\theta^2 + 8 = 0$

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

Solution. 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's 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 $\sqrt{3} = \dfrac{1}{267}(8\theta^5 + 5\theta^4 - 80\theta^3 - 130\theta^2 + 335\theta - 455)$ and $\sqrt[3]{5} = \dfrac{1}{267}(-8\theta^5 - 5\theta^4 + 80\theta^3 + 130\theta^2 - 68\theta + 455)$ (it takes juste 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 $\mathbb{Q}(\sqrt{3}, \sqrt[3]{5}) = \mathbb{Q}(\theta)$.

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

Solution. We use the Theorem 2.3, 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 $\sigma_{|\mathbb{Q}} = I_{d|\mathbb{Q}}$)

Exercise 2.4.
(Version of the third edition because the discriminant was wrong in the first edition) Find the discriminant of $K = \mathbb{Q}(\sqrt{3}, \sqrt{5})$.

Solution. We will use the Theorem 1. Start with the basis $B = \{1, \sqrt{3}, \sqrt{5}, \sqrt{15}\}$ which is a $\mathbb{Q}-$basis with integral generators. The monomorphisms are

$$\begin{array}{cc} \sigma_1 : \sqrt{3} \mapsto \sqrt{3} & \sigma_1 : \sqrt{5} \mapsto \sqrt{5} \\ \sigma_2 : \sqrt{3} \mapsto -\sqrt{3} & \sigma_2 : \sqrt{5} \mapsto \sqrt{5} \\ \sigma_3 : \sqrt{3} \mapsto \sqrt{3} & \sigma_3 : \sqrt{5} \mapsto -\sqrt{5} \\ \sigma_4 : \sqrt{3} \mapsto -\sqrt{3} & \sigma_4 : \sqrt{5} \mapsto -\sqrt{5} \end{array}$$

Then $\Delta(B) = \begin{vmatrix} 1 & \sqrt{3} & \sqrt{5} & \sqrt{15} \\ 1 & -\sqrt{3} & \sqrt{5} & -\sqrt{15} \\ 1 & \sqrt{3} & -\sqrt{5} & -\sqrt{15} \\ 1 & -\sqrt{3} & -\sqrt{5} & \sqrt{15} \end{vmatrix}^2 = 3.5.15. \begin{vmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{vmatrix}^2 = 3^2.5^2.16^2 = 2^8.3^2.5^2$. Then $2^2 \mid \Delta(B)$, we try to find an α of the form $\frac{1}{2}(a+b\sqrt{3}+c\sqrt{5}+d\sqrt{15})$ with $a, b, c, d \in \{0, 1\}$. We use the trace and the norm that must be in $\mathbb{Z}$. Calculate the trace : $T_K(\alpha) = \frac{1}{2}4a \in \mathbb{Z}$, so the trace doesn't give informations. Calculate the norm : $N_K(\alpha) = \frac{1}{2^4}(a + b\sqrt{3} + c\sqrt{5} + d\sqrt{15})(a - b\sqrt{3} + c\sqrt{5} - d\sqrt{15})(a + b\sqrt{3} - c\sqrt{5} - d\sqrt{15})(a - b\sqrt{3} - c\sqrt{5} + d\sqrt{15})$. There is 15 cases (the case 0,0,0,0 is not in the theorem because it must exist j such that $\lambda_j = 1$) :

a, b, c, d	$2^4.N_K(\alpha)$	$N_K(\alpha) \in \mathbb{Z}$? (i.e. $2^4 \mid 2^4.N_K(\alpha)$?)
$1, 0, 0, 0$	1	NO
$0, 1, 0, 0$	3^2	NO
$0, 0, 1, 0$	5^2	NO
$0, 0, 0, 1$	$3^2.5^2$	NO
$1, 1, 0, 0$	2^2	NO
$1, 0, 1, 0$	2^4	YES
$1, 0, 0, 1$	$2^2.7^2$	NO
$0, 1, 1, 0$	2^2	NO
$0, 1, 0, 1$	$2^4.3^2$	YES
$0, 0, 1, 1$	$2^2.5^2$	NO
$1, 1, 1, 0$	-11	NO
$0, 1, 1, 1$	-11	NO
$1, 0, 1, 1$	61	NO
$1, 1, 0, 1$	109	NO
$1, 1, 1, 1$	2^6	YES

We use $\omega = \frac{1+\sqrt{5}}{2}$ and we start again the process. Let $B' = \{1, \sqrt{3}, \omega, \sqrt{3}\omega\}$, calculate $\Delta(B') = \begin{vmatrix} 1 & \sqrt{3} & \frac{1+\sqrt{5}}{2} & \sqrt{3}\frac{1+\sqrt{5}}{2} \\ 1 & -\sqrt{3} & \frac{1+\sqrt{5}}{2} & -\sqrt{3}\frac{1+\sqrt{5}}{2} \\ 1 & \sqrt{3} & \frac{1-\sqrt{5}}{2} & \sqrt{3}\frac{1-\sqrt{5}}{2} \\ 1 & -\sqrt{3} & \frac{1-\sqrt{5}}{2} & -\sqrt{3}\frac{1-\sqrt{5}}{2} \end{vmatrix}^2 = \frac{3^2}{2^4} \begin{vmatrix} 1 & 1 & 1+\sqrt{5} & 1+\sqrt{5} \\ 1 & -1 & 1+\sqrt{5} & -1-\sqrt{5} \\ 1 & 1 & 1-\sqrt{5} & 1-\sqrt{5} \\ 1 & -1 & 1-\sqrt{5} & -1+\sqrt{5} \end{vmatrix}^2 =$

$$\frac{3^2}{2^4}\begin{vmatrix}1 & 1 & 1+\sqrt{5} & 1+\sqrt{5}\\ 0 & -2 & 0 & -2-2\sqrt{5}\\ 0 & 0 & -2\sqrt{5} & -2\sqrt{5}\\ 0 & -2 & -2\sqrt{5} & -2\end{vmatrix}^2 = \frac{3^2}{2^4}\begin{vmatrix}1 & 1 & 1+\sqrt{5} & 1+\sqrt{5}\\ 0 & -2 & 0 & -2-2\sqrt{5}\\ 0 & 0 & -2\sqrt{5} & -2\sqrt{5}\\ 0 & 0 & -2\sqrt{5} & 2\sqrt{5}\end{vmatrix}^2 =$$
$$\frac{3^2}{2^4}\begin{vmatrix}1 & 1 & 1+\sqrt{5} & 1+\sqrt{5}\\ 0 & -2 & 0 & -2-2\sqrt{5}\\ 0 & 0 & -2\sqrt{5} & -2\sqrt{5}\\ 0 & 0 & 0 & 4\sqrt{5}\end{vmatrix}^2 = \frac{2^8.3^2.5^2}{2^4} = 2^4.3^2.5^2.$$ We have a candidate for being an integral basis but we have to prove it is. We use the Theorem 1. Let $\alpha = \dfrac{a+b\sqrt{3}+c\omega+d\sqrt{3}\omega}{p}$ for $p \in \{2,3,5\}$ and $a,b,c \in \mathbb{Z}$ with$(a,b,c) \neq (0,0,0)$. $\{2,3,5\}$ is choose like that because for all $p \in \{2,3,5\}$ we have $p^2 \mid \Delta(B')$. Calculate $T_K(\alpha) = \dfrac{4a}{p}$ and $N_K(\alpha) = \dfrac{1}{p^4}(a^4+9b^4+c^4+9d^4-a^2c^2-27b^2d^2-6b^2a^2-9a^2d^2+2a^3c-6bda^2-9b^2c^2-xb^2ac+18b^3d-6c^2d^2-2ac^3+6bdc^2+6d^2ac-18bd^3-24abcd)$ (an exhausting calculation which is at the limit of what is doable) that have to be in $\mathbb{Z}$. After studying all the cases with $a,b,c,d \in [\![0,p-1]\!]$, there is no solution. It follows that B' is an integral basis and the discriminant is $2^4.3^2.5^2$. To be sure, we can look at the reference [4] which helps on biquadratic fields.

Exercise 2.5.
Let $K = \mathbb{Q}(\sqrt[4]{2})$. Find all monomorphisms $\sigma : K \to \mathbb{C}$ and the minimum polynomials (over $\mathbb{Q}$) and field polynomials (over K) of

(i) $\sqrt[4]{2}$

(ii) $\sqrt{2}$

(iii) 2

(iv) $\sqrt{2}+1$.

Compare with Theorem 2.5.

Solution. The minimum polynomial of $\sqrt[4]{2}$ is $P = X^4 - 2$ which have a degree 4, so there are 4 monomorphisms $\sigma : K \to \mathbb{C}$. The roots of P are : $\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}$, Then the four monomorphisms are :

$$\begin{array}{ll}\sigma_1 : \sqrt[4]{2} \mapsto \sqrt[4]{2} & \text{(Identity function)}\\ \sigma_2 : \sqrt[4]{2} \mapsto -\sqrt[4]{2} & \\ \sigma_3 : \sqrt[4]{2} \mapsto i\sqrt[4]{2} & \\ \sigma_4 : \sqrt[4]{2} \mapsto -i\sqrt[4]{2} & \end{array}$$

As the Exercice 2.3.

(i) The minimum polynomial of $\sqrt[4]{2}$ is X^4-2 and the field polynomial is $(X-\sigma_1(\sqrt[4]{2}))(X-\sigma_2(\sqrt[4]{2}))(X-\sigma_3(\sqrt[4]{2}))(X-\sigma_4(\sqrt[4]{2}))=(X-\sqrt[4]{2})(X+\sqrt[4]{2})(X-i\sqrt[4]{2})(X+i\sqrt[4]{2})=X^4-2$. Then we see, as the Theorem 2.5 deals with, $f_{\sqrt[4]{2}}(t)=p_{\sqrt[4]{2}}(t)$

(ii) The minimum polynomial of $\sqrt{2}$ is X^2-2 and the field polynomial is $(X-\sigma_1(\sqrt{2}))(X-\sigma_2(\sqrt{2}))(X-\sigma_3(\sqrt{2}))(X-\sigma_4(\sqrt{2}))=(X-\sqrt{2})(X-\sqrt{2})(X+\sqrt{2})(X+\sqrt{2})=(X^2-2)^2$. ($\sigma_i(\sqrt{2})=\sigma_i((\sqrt[4]{2})^2)=(\sigma_i(\sqrt[4]{2}))^2$.) Then we see, as the Theorem 2.5 deals with, $f_{\sqrt{2}}(t)=(p_{\sqrt{2}}(t))^2$

(iii) The minimum polynomial of 2 is $X-2$ and the field polynomial is $(X-\sigma_1(2))(X-\sigma_2(2))(X-\sigma_3(2))(X-\sigma_4(2))=(X-2)^4$. Then we see, as the Theorem 2.5 deals with, $f_2(t)=(p_2(t))^4$

(iv) The minimum polynomial of $\sqrt{2}+1$ is X^2-2X-1 and the field polynomial is $(X-\sigma_1(1+\sqrt{2}))(X-\sigma_2(1+\sqrt{2}))(X-\sigma_3(1+\sqrt{2}))(X-\sigma_4(1+\sqrt{2}))=(X-1-\sqrt{2})(X-1-\sqrt{2})(X-1+\sqrt{2})(X-1+\sqrt{2})=(X^2-2X-1)^2$. Then we see, as the Theorem 2.5 deals with, $f_{1+\sqrt{2}}(t)=(p_{1+\sqrt{2}}(t))^2$

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

Solution. We will use the Theorem 1 to compute an integral basis of $\mathbb{Q}(\sqrt[3]{5})$. Start with $B=\{1,\sqrt[3]{5},(\sqrt[3]{5})^2\}$. The 3 monomorphisms (because the degree of the minimal polynomial X^3-5 of $\sqrt[3]{5}$ over $\mathbb{Q}$ is 3) 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 $\Delta[1,\sqrt[3]{5},(\sqrt[3]{5})^2]=\begin{vmatrix}1 & \sqrt[3]{5} & (\sqrt[3]{5})^2\\ 1 & j\sqrt[3]{5} & j^2(\sqrt[3]{5})^2\\ 1 & j^2\sqrt[3]{5} & j(\sqrt[3]{5})^2\end{vmatrix}^2=(5j^2+5j^2+5j^2-5j-5j-5j)^2=$
$15^2(j^2-j)^2=15^2(j^4-2j^3+j^2)=15^2(j+1+j^2-3)=-3^3.5^2$.

Use the Theorem 1. Let $p=3$ (we have $p^2\mid\Delta(B)$) and $\alpha=\dfrac{a+b\sqrt[3]{5}+c(\sqrt[3]{5})^2}{3}$ with $a,b,c\in\{0,1,2\}$ and $(a,b,c)\neq(0,0,0)$. $T_K(\alpha)=\frac{1}{3}3a\in\mathbb{Z}$, the trace doesn't give informations. $N_K(\alpha)=\dfrac{1}{3^3}(a+b\sqrt[3]{5}+c(\sqrt[3]{5})^2)(a+bj\sqrt[3]{5}+cj^2(\sqrt[3]{5})^2)(a+bj^2\sqrt[3]{5}+cj(\sqrt[3]{5})^2)=\dfrac{1}{27}(a^3+5b^3+25c^3-15abc)$ (a long and exhausting calculation gives that). So we need that $3^3\mid(a^3+5b^3+25c^3-15abc)$

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

So we can't find an α of this form.

Let $p = 5$ is such that $p^2 \mid \Delta(B)$ and $\alpha = \dfrac{a + b\sqrt[3]{5} + c(\sqrt[3]{5})^2}{5}$ with $a, b, c \in \{0, 1, 2, 3, 4\}$ and $(a, b, c) \neq (0, 0, 0)$. $T_K(\alpha) = \frac{3}{5}a$ must be in $\mathbb{Z}$ then $a \in 5\mathbb{Z} \cap \{0, 1, 2, 3, 4\}$, hence $a = 0$. Now $N_K(\alpha) = \dfrac{1}{5^3}(5b^3 + 25c^3) = \dfrac{b^3 + 5c^3}{25}$.

b, c	$\sigma' = b^3 + 5c^3$	$25 \mid \sigma'$?	b, c	$\sigma' = b^3 + 5c^3$	$25 \mid \sigma'$?
$0, 1$	5	NO	$2, 3$	11.13	NO
$0, 2$	$2^3.5$	NO	$2, 4$	$2^3.41$	NO
$0, 3$	$3^3.5$	NO	$3, 0$	3^3	NO
$0, 4$	$2^6.5$	NO	$3, 1$	2^5	NO
$1, 0$	1	NO	$3, 2$	67	NO
$1, 1$	2.3	NO	$3, 3$	2.3^4	NO
$1, 2$	41	NO	$3, 4$	347	NO
$1, 3$	$2^3.17$	NO	$4, 0$	2^6	NO
$1, 4$	3.107	NO	$4, 1$	3.23	NO
$2, 0$	2^3	NO	$4, 2$	$2^3.13$	NO
$2, 1$	13	NO	$4, 3$	199	NO
$2, 2$	$2^4.3$	NO	$4, 4$	$2^7.3$	NO

So we can't find an α of this form.

But $p = 3$ and $p = 5$ are the only primes such that $p^2 \mid \Delta(B)$. And it doesn't exist α of the form of the Theorem 1. It follows that our basis B was already an integral basis. $\{1, \sqrt[3]{5}, (\sqrt[3]{5})^2\}$ is an integral basis of $\mathbb{Q}(\sqrt[3]{5})$.

Exercise 2.7.
Show that $B = \{1, \sqrt[3]{175}, \sqrt[3]{245}\}$ is a $\mathbb{Z}-$basis for $K = \mathbb{Q}(\sqrt[3]{175})$ and prove that there is no $\mathbb{Z}-$basis of the form $\{1, \theta, \theta^2\}$.

Solution. $X^3 - 175$ is the minimum polynomial of $\sqrt[3]{175}$ in K, so $[K : \mathbb{Q}] = 3$ and the 3 monomorphisms are $\sigma_1 : \sqrt[3]{175} \mapsto \sqrt[3]{175}$, $\sigma_2 : \sqrt[3]{175} \mapsto j\sqrt[3]{175}$ and $\sigma_3 : \sqrt[3]{175} \mapsto j^2\sqrt[3]{175}$ where $j = e^{2\pi i/3}$. Calculate $\Delta(B) = \begin{vmatrix} 1 & \sqrt[3]{175} & \sqrt[3]{245} \\ 1 & j\sqrt[3]{175} & j^2\sqrt[3]{245} \\ 1 & j^2\sqrt[3]{175} & j\sqrt[3]{245} \end{vmatrix}^2 =$ $(3j^2\sqrt[3]{175}\sqrt[3]{245} - 3j\sqrt[3]{175}\sqrt[3]{245})^2 = 3^2\sqrt[3]{5^2.7.5.7^2}^2(j^2 - j)^2 = 3^2.5^2.7^2(j - 2 + j^2) = 3^2.5^2.7^2(-3) = -3^3.5^2.7^2$ because $1 + j + j^2 = 0$ and $j^3 = 1$.

We use the Theorem 1. Let $\alpha = \dfrac{a + b\sqrt[3]{175} + c\sqrt[3]{245}}{p}$ for $p \in \{3, 5, 7\}$ and $a, b, c \in \mathbb{Z}$ with$(a, b, c) \neq (0, 0, 0)$. $\{3, 5, 7\}$ is choose like that because for all $p \in \{3, 5, 7\}$ we have $p^2 \mid \Delta(B)$. Calculate $T_K(\alpha) = \dfrac{3a}{p}$ and $N_K(\alpha) = \dfrac{a^3 + 175b^3 + 245c^3 - 105abc}{p^3}$ (just an exhausting calculation but it's doable) that have to be in $\mathbb{Z}$.

For $p = 3$, the trace doesn't give informations. we need $3^3 \mid (a^3 + 175b^3 + 245c^3 - 105abc)$:

a, b, c	$\sigma = (a^3 + 175b^3 + 245c^3 - 105abc)$	$3^3 \mid \sigma$?
$0, 0, 1$	5.7^2	NO
$0, 0, 2$	$2^3.5.7^2$	NO
$0, 1, 0$	$5^2.7$	NO
$0, 1, 1$	$2^2.3.5.7$	NO
$0, 1, 2$	$5.7.61$	NO
$0, 2, 0$	$2^3.5^2.7$	NO
$0, 2, 1$	$5.7.47$	NO
$0, 2, 2$	$2^5.3.5.7$	NO
$1, 0, 0$	1	NO
$1, 0, 1$	$2.3.41$	NO
$1, 0, 2$	37.53	NO
$1, 1, 0$	$2^4.11$	NO
$1, 1, 1$	$2^2.79$	NO
$1, 1, 2$	$2.3^2.107$	NO
$1, 2, 0$	3.467	NO
$1, 2, 1$	$2^2.359$	NO
$1, 2, 2$	17.173	NO
$2, 0, 0$	2^3	NO
$2, 0, 1$	11.23	NO
$2, 0, 2$	$2^4.3.41$	NO
$2, 1, 0$	3.61	NO
$2, 1, 1$	2.109	NO
$2, 1, 2$	1723	NO
$2, 2, 0$	$2^7.11$	NO
$2, 2, 1$	$3^2.137$	NO
$2, 2, 2$	$2^5.79$	NO

So we can't find an α of this form.

Let try with $p = 5$, the trace give us that $a \in 5\mathbb{Z} \cap \{0, 1, 2, 3, 4\}$, hence $a = 0$. Now $N_K(\alpha) = \dfrac{175b^3 + 245c^3}{5^3} = \dfrac{35b^3 + 49c^3}{25}$ that must be in $\mathbb{Z}$. We need $25 \mid 35b^3 + 49c^3$:

b, c	$\sigma = 35b^3 + 49c^3$	$25 \mid \sigma$?	b, c	$\sigma = 35b^3 + 49c^3$	$25 \mid \sigma$?
$0, 1$	7^2	NO	$2, 3$	7.229	NO
$0, 2$	$2^3.7^2$	NO	$2, 4$	$2^3.7.61$	NO
$0, 3$	$3^3.7^2$	NO	$3, 0$	$3^3.5.7$	NO
$0, 4$	$2^6.7^2$	NO	$3, 1$	$2.7.71$	NO
$1, 0$	5.7	NO	$3, 2$	7.191	NO
$1, 1$	$2^2.3.7$	NO	$3, 3$	$2^2.3^4.7$	NO
$1, 2$	7.61	NO	$3, 4$	$7.11.53$	NO
$1, 3$	$2.7.97$	NO	$4, 0$	$2^6.5.7$	NO
$1, 4$	$3.7.151$	NO	$4, 1$	$3.7.109$	NO
$2, 0$	$2^3.5.7$	NO	$4, 2$	$2^3.7.47$	NO
$2, 1$	7.47	NO	$4, 3$	7.509	NO
$2, 2$	$2^5.3.7$	NO	$4, 4$	$2^8.3.7$	NO

So we can't find an α of this form.

Let try with $p = 7$, the trace give us that $a \in 7\mathbb{Z} \cap \{0, 1, 2, 3, 4, 5, 6\}$, hence $a = 0$. Now $N_K(\alpha) = \dfrac{175b^3 + 245c^3}{7^3} = \dfrac{25b^3 + 35c^3}{49}$ that must be in $\mathbb{Z}$. We need $49 \mid 25b^3 + 35c^3$:

b, c	$25b^3 + 35c^3$	$49 \mid \sigma$?	b, c	$25b^3 + 35c^3$	$49 \mid \sigma$?	b, c	$25b^3 + 35c^3$	$49 \mid \sigma$?
$0, 1$	5.7	NO	$2, 3$	5.229	NO	$4, 5$	$5^2.239$	NO
$0, 2$	$2^3.5.7$	NO	$2, 4$	$2^3.5.61$	NO	$4, 6$	$2^3.5.229$	NO
$0, 3$	$3^3.5.7$	NO	$2, 5$	$3.5^2.61$	NO	$5, 0$	5^5	NO
$0, 4$	$2^6.5.7$	NO	$2, 6$	$2^4.5.97$	NO	$5, 1$	$2^3.5.79$	NO
$0, 5$	$5^4.7$	NO	$3, 0$	$3^3.5^2$	NO	$5, 2$	$3.5.227$	NO
$0, 6$	$2^3.3^3.5.7$	NO	$3, 1$	$2.5.71$	NO	$5, 3$	$2.5.11.37$	NO
$1, 0$	5^2	NO	$3, 2$	5.191	NO	$5, 4$	$5.29.37$	NO
$1, 1$	$2^2.3.5$	NO	$3, 3$	$2^2.3^4.5$	NO	$5, 5$	$2^2.3.5^4$	NO
$1, 2$	5.61	NO	$3, 4$	$5.11.53$	NO	$5, 6$	5.2137	NO
$1, 3$	$2.5.97$	NO	$3, 5$	$2.5^2.101$	NO	$6, 0$	$2^3.3^3.5^2$	NO
$1, 4$	$3.5.151$	NO	$3, 6$	$3^3.5.61$	NO	$6, 1$	5.1087	NO
$1, 5$	$2^4.5^2.11$	NO	$4, 0$	$2^6.5^2$	NO	$6, 2$	$2^4.5.71$	NO
$1, 6$	$5.37.41$	NO	$4, 1$	$3.5.109$	NO	$6, 3$	$3^3.5.47$	NO
$2, 0$	$2^3.5^2$	NO	$4, 2$	$2^3.5.47$	NO	$6, 4$	$2^3.5.191$	NO
$2, 1$	5.47	NO	$4, 3$	5.509	NO	$6, 5$	$5^2.17.23$	NO
$2, 2$	$2^5.3.5$	NO	$4, 4$	$2^8.3.5$	NO	$6, 6$	$2^5.3^4.5$	NO

So we can't find an α of this form.

But $p = 3$, $p = 5$ and $p = 7$ are the only primes such that $p^2 \mid \Delta(B)$. And it doesn't exist α of the form of the Theorem 1. It follows that our basis B was already an integral basis. $\{1, \sqrt[3]{175}, \sqrt[3]{245}\}$ is an integral basis of $\mathbb{Q}(\sqrt[3]{175})$.

If a $\mathbb{Z}-$basis was of the form $\{1, \theta, \theta^2\}$, we would have $\Delta(B) = \Delta[1, \theta, \theta^2]$. Then if we write θ with the basis B, we will have a change of basis matrix C that should have $\det(C) = \pm 1$. $\theta = a + b\sqrt[3]{175} + c\sqrt[3]{245}$ but $\{1, \theta, \theta^2\}$ is an integral basis if and only if $\{1, (\theta - a), (\theta - a)^2\}$, because $a \in \mathbb{Z}$. Hence, we can consider that $a = 0$. $\theta = b\sqrt[3]{175} + c\sqrt[3]{245}$ and $\theta^2 = 5b^2\sqrt[3]{245} + 70bc + 7c^2\sqrt[3]{175}$.
$\det(C) = \begin{vmatrix} 1 & 0 & 0 \\ 0 & b & c \\ 70bc & 7c^2 & 5b^2 \end{vmatrix} = 5b^3 - 7c^3$ We want to prove that $5b^3 - 7c^3 \neq \pm 1$.
we look in $\mathbb{Z}/7\mathbb{Z}$, we have $1^3 \equiv 1[7]$, $2^3 \equiv 1[7]$, $3^3 \equiv 6[7]$, $4^3 \equiv 1[7]$, $5^3 \equiv 6[7]$, $6^3 \equiv 6[7]$, then $5b^3 - 7c^3 \equiv 5b^3 \equiv 5$ or $2[7]$, hence $5b^3 \not\equiv \pm 1[7]$. It follows that $5b^3 - 7c^3 = \pm 1$ is impossible. Hence there is no $\mathbb{Z}-$basis of the form $\{1, \theta, \theta^2\}$.

Exercise 2.8.
Compute integral bases and discriminants of

(a) $\mathbb{Q}(\sqrt{2}, \sqrt{3})$

(b) $\mathbb{Q}(\sqrt{2}, i)$

(c) $\mathbb{Q}(\sqrt[3]{2})$

(d) $\mathbb{Q}(\sqrt[4]{2})$.

Solution. For each case, we will use the Theorem 1.

(a) Now $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. $B = \{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is a $\mathbb{Q}-$basis of K. $\Delta(B) = 2^{10}.3^2$, then $p = 2$ and $p = 3$ are primes such that $p^2 \mid \Delta(B)$. Start with $p = 2$, we are looking for an α of the form $\frac{1}{2}(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6})$. By Exercise 2.5 similar calculations, we find $T_p(\alpha) = \frac{4a}{p}$ and $N_p(\alpha) = \frac{1}{p^4}((a^2 - 2b^2 - 3c^2 + 6d^2)^2 - 24(ad - bc)^2)$.

a, b, c, d	$p^4.N_p(\alpha)$	$N_2(\alpha) \in \mathbb{Z}$?
$0, 0, 0, 1$	36	NO
$0, 0, 1, 0$	9	NO
$0, 0, 1, 1$	9	NO
$0, 1, 0, 0$	4	NO
$0, 1, 0, 1$	16	YES
$0, 1, 1, 0$	1	NO
$0, 1, 1, 1$	-23	NO
$1, 0, 0, 0$	1	NO
$1, 0, 0, 1$	25	NO
$1, 0, 1, 0$	4	NO
$1, 0, 1, 1$	-8	NO
$1, 1, 0, 0$	1	NO
$1, 1, 0, 1$	1	NO
$1, 1, 1, 0$	-8	NO
$1, 1, 1, 1$	4	NO

Then we find the only α possible: $\alpha = \frac{\sqrt{2}+\sqrt{6}}{2}$.

Then we do the same process with the basis $B' = \{1, \sqrt{2}, \sqrt{3}, \alpha\}$. $\Delta(B') = 2^8.3^2$. We looking for a $\beta = \frac{1}{p}(a + b\sqrt{2} + c\sqrt{3} + d\alpha)$. $\tilde{T}_p(\beta) = \frac{4a}{p}$ and $\tilde{N}_p(\beta) = \frac{1}{p^4}(a + b\sqrt{2} + c\sqrt{3} + d\frac{\sqrt{2}+\sqrt{6}}{2})(a - b\sqrt{2} + c\sqrt{3} - d\frac{\sqrt{2}+\sqrt{6}}{2})(a + b\sqrt{2} - c\sqrt{3} + d\frac{\sqrt{2}-\sqrt{6}}{2})(a - b\sqrt{2} - c\sqrt{3} - d\frac{\sqrt{2}-\sqrt{6}}{2})$. Start with $p = 2$.

a,b,c,d	$p^4.\tilde{N}_p(\beta)$	$\tilde{N}_2(\beta) \in \mathbb{Z}$?
$0,0,0,1$	1	NO
$0,0,1,0$	9	NO
$0,0,1,1$	-2	NO
$0,1,0,0$	4	NO
$0,1,0,1$	9	NO
$0,1,1,0$	1	NO
$0,1,1,1$	-18	NO
$1,0,0,0$	1	NO
$1,0,0,1$	-1	NO
$1,0,1,0$	4	NO
$1,0,1,1$	1	NO
$1,1,0,0$	1	NO
$1,1,0,1$	-2	NO
$1,1,1,0$	-8	NO
$1,1,1,1$	1	NO

Now try with $p = 3$. The trace gives $a = 0$ because we have $a \in \{0, 1, 2\}$ and $\tilde{T}_3(\beta) = \frac{4a}{3} \in \mathbb{Z}$.

b,c,d	$p^4.\tilde{N}_p(\beta)$	$\tilde{N}_3(\beta) \in \mathbb{Z}$?	b,c,d	$p^4.\tilde{N}_p(\beta)$	$\tilde{N}_3(\beta) \in \mathbb{Z}$?
$0,0,1$	1	NO	$1,1,2$	-71	NO
$0,0,2$	16	NO	$1,2,0$	100	NO
$0,1,0$	9	NO	$1,2,1$	9	NO
$0,1,1$	-2	NO	$1,2,2$	-188	NO
$0,1,2$	-23	NO	$2,0,0$	64	NO
$0,2,0$	144	NO	$2,0,1$	121	NO
$0,2,1$	97	NO	$2,0,2$	144	NO
$0,2,2$	-32	NO	$2,1,0$	25	NO
$1,0,0$	4	NO	$2,1,1$	46	NO
$1,0,1$	9	NO	$2,1,2$	9	NO
$1,0,2$	4	NO	$2,2,0$	16	NO
$1,1,0$	1	NO	$2,2,1$	-71	NO
$1,1,1$	-18	NO	$2,2,2$	-288	NO

So we can't find an β of this form. Then $B' = \{1, \sqrt{2}, \sqrt{3}, \frac{\sqrt{2}+\sqrt{6}}{2}\}$ is an integral basis for $\mathbb{Q}(\sqrt{2}, i)$ and the discriminant is $2^8.3^2$.

(b) Now $K = \mathbb{Q}(\sqrt{2}, i)$. $B = \{1, i, \sqrt{2}, i\sqrt{2}\}$ is a $\mathbb{Q}-$basis of K. $\Delta(B) = 1024$, then the only prime p such that $p^2 \mid \Delta(B)$ is 2. As the Theorem 1 deals with, let consider α is of the form $\frac{1}{2}(a+bi+c\sqrt{2}+di\sqrt{2})$. By Exercise 2.5 similar calculations, we find $N(\alpha) = \frac{1}{2^4}((a^2+b^2-2c^2-2d^2)^2+8(ad-bc)^2)$.

a,b,c,d	$2^4.N(\alpha)$	$N(\alpha) \in \mathbb{Z}$?
$0,0,0,1$	4	NO
$0,0,1,0$	4	NO
$0,0,1,1$	16	YES
$0,1,0,0$	1	NO
$0,1,0,1$	9	NO
$0,1,1,0$	17	NO
$0,1,1,1$	33	NO
$1,0,0,0$	1	NO
$1,0,0,1$	17	NO
$1,0,1,0$	9	NO
$1,0,1,1$	33	NO
$1,1,0,0$	4	NO
$1,1,0,1$	24	NO
$1,1,1,0$	24	NO
$1,1,1,1$	36	NO

We find $\alpha = \frac{\sqrt{2}+i\sqrt{2}}{2}$ which is an algebraic integer (minimum polynomial is X^4+1).

Then we do the same process with the basis $B' = \{1, i, \sqrt{2}, \alpha\}$. $\Delta(B') = 256$. We looking for a $\beta = \frac{1}{2}(a + bi + c\sqrt{2} + d\alpha)$

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

So we can't find an β of this form. Then $B' = \{1, i, \sqrt{2}, \frac{\sqrt{2}+i\sqrt{2}}{2}\}$ is an integral basis for $\mathbb{Q}(\sqrt{2}, i)$ and the discriminant is 256.

(c) Now $K = \mathbb{Q}(\sqrt[3]{2})$. $B = \{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ is a $\mathbb{Q}-$basis of K. $\Delta(B) = -2^2.3^3$ (Similar as the calculation in the Exercise 2.7), then the only primes p such that $p^2 \mid \Delta(B)$ is 2 and 3. As the Theorem 1 deals with, let consider

α of the form $\frac{1}{p}(a+b\sqrt[3]{2}+c\sqrt[3]{4})$ where $a,b,c \in [\![0,p-1]\!]$. We can calculate $T_p(\alpha) = \frac{3a}{p}$ and $N_p(\alpha) = \frac{1}{p^3}(a^3+2b^3+4c^3-6abc)$. Then for $p=2$ (we remind that $a,b,c \in \{0,1\}$), we have $a=0$ (because of the trace), now $N_2(\alpha) = \frac{1}{2^3}(2b^3+4c^3) = \frac{1}{2^2}(b^3+2c^3)$. It follows that $b=0$ because if $b=1$, $1+2c^3$ will be odd then not divisible by 4. And $c=0$ because we want $4 \mid 2c^3$. We find no α for $p=2$.

Let try $p=3$, the trace doesn't give any information.

a,b,c	$p^4.N_p(\alpha)$	$N_3(\alpha) \in \mathbb{Z}$?	a,b,c	$p^4.N_p(\alpha)$	$N_3(\alpha) \in \mathbb{Z}$?
$0,0,1$	4	NO	$1,1,2$	23	NO
$0,0,2$	32	NO	$1,2,0$	17	NO
$0,1,0$	2	NO	$1,2,1$	9	NO
$0,1,1$	6	NO	$1,2,2$	25	NO
$0,1,2$	34	NO	$2,0,0$	8	NO
$0,2,0$	16	NO	$2,0,1$	12	NO
$0,2,1$	20	NO	$2,0,2$	40	NO
$0,2,2$	48	NO	$2,1,0$	10	NO
$1,0,0$	1	NO	$2,1,1$	2	NO
$1,0,1$	5	NO	$2,1,2$	18	NO
$1,0,2$	33	NO	$2,2,0$	24	NO
$1,1,0$	3	NO	$2,2,1$	4	NO
$1,1,1$	1	NO	$2,2,2$	8	NO

Then we can't find some α of the form $\frac{1}{p}(a+b\sqrt[3]{2}+c\sqrt[3]{4})$, so our basis $B = \{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ was already an integral basis and the discriminant is still $-2^2.3^3$.

(d) Now $K = \mathbb{Q}(\sqrt[4]{2})$. $B = \{1, \sqrt[4]{2}, (\sqrt[4]{2})^2, (\sqrt[4]{2})^3\}$ is a $\mathbb{Q}-$basis of K. $\Delta(B) = -2^{11}$ (Similar as the calculation in the Exercise 2.7), then the only prime p such that $p^2 \mid \Delta(B)$ is 2. As the Theorem 1 deals with, let consider α of the form $\frac{1}{2}(a+b\sqrt[4]{2}+c(\sqrt[4]{2})^2+d(\sqrt[4]{2})^3)$ where $a,b,c,d \in \{0,1\}$. We can calculate $T(\alpha) = \frac{4a}{2}$ it doesn't give any information. Then study all cases possible.

a,b,c,d	$2^4.N(\alpha)$	$N(\alpha) \in \mathbb{Z}$?	a,b,c,d	$2^4.N(\alpha)$	$N(\alpha) \in \mathbb{Z}$?
$0,0,0,1$	-8	NO	$1,0,0,1$	-7	NO
$0,0,1,0$	4	NO	$1,0,1,0$	1	NO
$0,0,1,1$	-4	NO	$1,0,1,1$	9	NO
$0,1,0,0$	-2	NO	$1,1,0,0$	-1	NO
$0,1,0,1$	-2	NO	$1,1,0,1$	-9	NO
$0,1,1,0$	2	NO	$1,1,1,0$	7	NO
$0,1,1,1$	-14	NO	$1,1,1,1$	-1	NO
$1,0,0,0$	1	NO			

Then we can't find some α of the form $\frac{1}{2}(a+b\sqrt[4]{2}+c(\sqrt[4]{2})^2+d(\sqrt[4]{2})^3)$,

so our basis $B = \{1, \sqrt[4]{2}, (\sqrt[4]{2})^2, (\sqrt[4]{2})^3\}$ was already an integral basis and the discriminant is still -2^{11}.

Exercise 2.9.
Let $K = \mathbb{Q}(\theta)$ where $\theta \in \mathfrak{O}_K$. Among the elements

$$\frac{1}{d}(a_0 + ... + a_i\theta^i)$$

$(0 \neq a_i; a_0, ..., a_i \in \mathbb{Z})$, where d is the discriminant, pick one with minimal value of $|a_i|$ and call it x_i. Do this for $i = 1, ..., n = [K : \mathbb{Q}]$ show that $F = \{x_1, x_2, ..., x_n\}$ is an integral basis.

Solution. By Theorem 2.15, $\mathfrak{O}_K$ is a free abelian group of rank n. All the x_i are in $\mathfrak{O}_K$ because we choose the x_i to be in $\mathfrak{O}_K$. We have to prove that F is $\mathbb{Z}-$linear independent. But $B = \{1, \theta, ..., \theta^{n-1}\}$ is a $\mathbb{Q}-$basis of K. We can write all x_i on the basis B and the change of basis matrix C is a upper triangular matrix with the $a_i/d \neq 0$ on the diagonal. Then $\det C = \frac{\prod_{i=1}^{n} a_i}{d^n} \neq 0$ It follows that $\Delta(F) = (\det C)^2\Delta(B) \neq 0$ because $\Delta(B) \neq 0$ (Theorem 2.6), hence F is well $\mathbb{Z}-$linear independent. It's an integral basis because $\det(C)$ is as small as possible because each a_i is choose to be the smallest (in absolute value). See the proof of Theorem 2.15, the condition of having a discriminant as small as possible implies that it's an integral basis.

Exercise 2.10.
If $\alpha_i, ..., \alpha_n$ are $\mathbb{Q}-$linearly independant algebraic integers in $\mathbb{Q}(\theta)$, and if $\Delta[\alpha_1, ..., \alpha_n] = d$ where d is the discriminant of $\mathbb{Q}(\theta)$, show that $\{\alpha_1, ..., \alpha_n\}$ is an integral basis for $\mathbb{Q}(\theta)$.

Solution. We know that $\alpha_1\mathbb{Z} + ... + \alpha_n\mathbb{Z} \subset \mathfrak{O}_{\mathbb{Q}(\theta)}$, if we take an integral basis B, we can write all α_i in this basis B. Then we know that the discriminant of B is d. We have $\Delta[\alpha_1, ..., \alpha_n] = (\det(C))^2\Delta(B)$ with C the change of basis matrix. But $\Delta(B) = d$ and $\Delta[\alpha_1, ..., \alpha_n] = d$. So $\det C = \pm 1$, then C is inversible in $\mathbb{Z}$ and we can express every element of B with α_i. It follows that $\{\alpha_1, ..., \alpha_n\}$ is an integral basis for $\mathbb{Q}(\theta)$.

Exercise 2.11.
If $[K : \mathbb{Q}] = n, \alpha \in \mathbb{Q}$, show

$$N_K(\alpha) = \alpha^n,$$
$$T_K(\alpha) = n\alpha.$$

Solution. For all the monomorphisms σ of $K : \mathbb{Q}$ and for all $\alpha \in \mathbb{Q}$ we have $\sigma(\alpha) = \alpha$. Then by definition, $N_K(\alpha) = \prod_{k=1}^{n} \sigma_k(\alpha) = \prod_{k=1}^{n} \alpha = \alpha^n$ and $T_K(\alpha) = \sum_{k=1}^{n} \sigma_k(\alpha) = \sum_{k=1}^{n} \alpha = n\alpha$.

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 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 $T_{K_1}(\alpha) = 2$, $T_{K_2}(\alpha) = 4$

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 Theorem 2.3 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 $T_{K/L}(\sqrt[4]{3} + \sqrt{3}) = \sigma_1(\sqrt[4]{3} + \sqrt{3}) + \sigma_2(\sqrt[4]{3} + \sqrt{3}) = 2\sqrt{3}$.

Exercise 2.14.
For $K = \mathbb{Q}(\sqrt[4]{3}), L = \mathbb{Q}(\sqrt{3})$, calculate $N_{K/L}(\sqrt{3})$ and $N_{K/\mathbb{Q}}(\sqrt{3})$. Deduce that $N_{K/L}(\alpha)$ depends on K and L (provided that $\alpha \in K$). Do the same for $T_{K/L}$.

Solution. $N_{K/L}(\sqrt{3}) = \sqrt{3}^2 = 3$ (using the Solution of the Exercise 2.13) and $T_{K/L}(\sqrt{3}) = 2\sqrt{3}$.

$X^4 - 3$ is the minimum polynomial of $\sqrt[4]{3}$ in $\mathbb{Q}[X]$, so $[K : \mathbb{Q}] = 4$ and the four monomorphisms are:

$$\begin{array}{ll} \sigma_1 : \sqrt[4]{3} \mapsto \sqrt[4]{3} & \text{(Identity function)} \\ \sigma_2 : \sqrt[4]{3} \mapsto -\sqrt[4]{3} & \\ \sigma_3 : \sqrt[4]{3} \mapsto i\sqrt[4]{3} & \\ \sigma_4 : \sqrt[4]{3} \mapsto -i\sqrt[4]{3} & \end{array}$$

$N_{K/\mathbb{Q}}(\sqrt{3}) = \sigma_1(\sqrt{3})\sigma_2(\sqrt{3})\sigma_3(\sqrt{3})\sigma_4(\sqrt{3}) = (\sqrt{3})(\sqrt{3})(-\sqrt{3})(-\sqrt{3}) = 9$ and $T_{K/\mathbb{Q}}(\sqrt{3}) = \sqrt{3} + \sqrt{3} - \sqrt{3} - \sqrt{3} = 0$

Then $N_{K/L}$ and $T_{K/L}$ depend on K and L, it's a generalization of the result of the Exercise 2.12.

4.3 Quadratic and cyclotomic fields p.68

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 the Theorem 3.3.

(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 $\{1, \frac{1}{2} + \frac{1}{2}\sqrt{-7}\}$ 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 $\{1, \frac{1}{2} + \frac{1}{2}\sqrt{-11}\}$ 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 $4d = 4 \times -6 = -24$.

Exercise 3.2.
Let $K = \mathbb{Q}(\zeta)$ where $\zeta = e^{2\pi i/5}$. Calculate $N_K(\alpha)$ and $T_K(\alpha)$ for the following values of α :

(i) ζ^2

(ii) $\zeta + \zeta^2$

(iii) $1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4$

Solution. (i) $N_K(\zeta^2) = \prod_{k=1}^{4} \sigma_k(\zeta^2) = \prod_{k=1}^{4} \zeta^{2k} = \exp\left(\frac{2\pi i}{5} \times \sum_{k=1}^{4} k\right) = \exp\left(\frac{2\pi i}{5} \times 10\right) =$ 1 and $T_K(\zeta^2) = \sum_{k=1}^{4} \sigma_k(\zeta^2) = \sum_{k=1}^{4} \zeta^{2k} = -1$ because $\sum_{k=0}^{4} e^{2\pi i/5} = 0$.

(ii) $N_K(\zeta + \zeta^2) = N_K((\zeta)(1+\zeta)) = N_K(\zeta)N_K(1+\zeta) = N_K(1+\zeta) = \prod_{k=1}^{4}(1 + \sigma_k(\zeta)) = (1+\zeta)(1+\zeta^2)(1+\zeta^3)(1+\zeta^4) = (-1)^4(-1-\zeta)(-1-\zeta^2)(-1-\zeta^3)(-1-\zeta^4) = f(-1) = 1$ with f the minimal polynomial of ζ, $f(t) = \frac{t^5-1}{t-1} = (t-\zeta)(t-\zeta^2)(t-\zeta^3)(t-\zeta^4)$
and $T_K(\zeta + \zeta^2) = T_K(\zeta) + T_K(\zeta^2) = -1 - 1 = -2$.

(iii) $1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 = 0$ so $N_K(1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4) = 0$ and $T_K(1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4) = 0$.

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 it 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 (because $\mathbb{Z}[\zeta]$ is the ring of integers of $\mathbb{Q}(\zeta)$ since Theorem 3.5), 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 looking for a and b in $\mathbb{Z}$ such that $\frac{1}{4}(a^2+3b^2) = \pm 1$ (Exercise 3.3). That's 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 $\mathbb{Z}[\zeta]$.

Exercise 3.5.
If $\zeta = e^{2\pi i/5}$, $K = \mathbb{Q}(\zeta)$, prove that the norm of $\alpha \in \mathbb{Z}[\zeta]$ is of the form $\frac{1}{4}(a^2 - 5b^2)$ are rational integers.(Hint : in calculating $N(\alpha)$, first calculate $\sigma_1(\alpha)\sigma_4(\alpha)$ where $\sigma_i(\zeta) = \zeta^i$. Show that this is of the form $q + r\theta + s\phi$ where q, r, s are rational integers, $\theta = \zeta + \zeta^4, \phi = \zeta^2 + \zeta^3$. In the same way, establish $\sigma_2(\alpha)\sigma_3(\alpha) = q + s\theta + r\phi$.) Using Question 3.3, prove that $\mathbb{Z}[\zeta]$ has an infinite number of units.

Solution. $N(\alpha) = \sigma_1(\alpha)\sigma_2(\alpha)\sigma_3(\alpha)\sigma_4(\alpha)$. First, calculate $\sigma_1(\alpha)\sigma_4(\alpha)$ with $\alpha = a + b\zeta + c\zeta^2 + d\zeta^3$. $\sigma_1(\alpha)\sigma_4(\alpha) = (a + b\zeta + c\zeta^2 + d\zeta^3)(a + b\zeta^4 + c\zeta^8 + d\zeta^{12}) = (a + b\zeta + c\zeta^2 + d\zeta^3)(a + b\zeta^4 + c\zeta^3 + d\zeta^2) = a^2 + b^2 + c^2 + d^2 + (ab + bc + dc)(\zeta + \zeta^4) + (ac + ad + bd)(\zeta^2 + \zeta 3)$ while using $1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 = 0$. So $q = a^2 + b^2 + c^2 + d^2$, $r = ab + bc + dc$ and $s = ac + ad + bd$. Then

calculate $\sigma_2(\alpha)\sigma_3(\alpha) = (a+b\zeta^2+c\zeta^4+d\zeta^6)(a+b\zeta^3+c\zeta^6+d\zeta^9) = (a+b\zeta^2+c\zeta^4+d\zeta)(a+b\zeta^3+c\zeta+d\zeta^4) = q+s(\zeta+\zeta^4)+r(\zeta^2+\zeta^3)$. Hence $N(\alpha) = (q+r\theta+s\phi)(q+s\theta+r\phi) = q^2+q(r+s)(\theta+\phi)+(s^2+r^2)\phi\theta+rs(\phi^2+\theta^2)$. After calculation, $\theta\phi = -1$, $\theta+\phi = -1$ and $\phi^2+\theta^2 = 3$. Now we want to prove that $q^2-q(r+s)-(s^2+r^2)+3rs$ can be express as $\frac{1}{4}(a^2-5b^2)$. $(q-\frac{r+s}{2})^2-(\frac{r+s}{2})^2-(s^2+r^2)+3rs = \frac{1}{4}(2q-r-s)^2-\frac{5}{4}(r^2+s^2)+\frac{5}{4}(2rs) = \frac{1}{4}((2q-r-s)^2-5(r-s)^2)$. Hence we find the form $\frac{1}{4}(a^2-5b^2)$.

Thanks to the Exercise 3.3, we looking for $a, b \in \mathbb{Z}$ such that $\frac{1}{4}(a^2-5b^2) = \pm 1$. We start to solve $a^2-5b^2 = 1$. It's the same thing that find the units of $\mathbb{Z}[\sqrt{5}]$. Use Pell's Equation (cf. [3]), with $a = 9$ and $b = 4$ which is a fundamental solution. Then all $(9+4\sqrt{5})^n = x_n + y_n\sqrt{5}$ with $n \in \mathbb{N}$ give a solution of $a^2-5b^2 = 1$, but $(x_n)_{n\in\mathbb{N}}$ is a strictly increasing sequence. So there is an infinite number of solutions of $a^2-5b^2 = 1$. Then for each solution, multiply it by 2 and you have $\frac{1}{4}((2a)^2-5(2b)^2) = a^2-5b^2 = 1$. It follows that we find an infinite number of solutions, hence an infinite number of units in $\mathbb{Z}[\zeta]$.

Exercise 3.6.
Let $\zeta = e^{2\pi i/5}$. For $K = \mathbb{Q}(\zeta)$, use the formula $N_K(a+b\zeta) = \frac{a^5+b^5}{a+b}$ to calculate the following norms:

(i) $N_K(\zeta+2)$

(ii) $N_K(\zeta-2)$

(iii) $N_K(\zeta+3)$.

Using the fact that if $\alpha\beta = \gamma$, then $N_K(\alpha)N_K(\beta) = N_K(\gamma)$, deduce that $\zeta+2$, $\zeta-2$, $\zeta+3$ have no proper factors (i.e. factors which are not units) in $\mathbb{Z}[\zeta]$. Factorize $11, 31, 61$ in $\mathbb{Z}[\zeta]$.

Solution. (i) $N_K(\zeta+2) = \frac{2^5+1^5}{1+2} = \frac{33}{3} = 11$. If $\zeta+2 = \alpha\beta$, $N_K(\zeta+2) = 11 = N_K(\alpha)N_K(\beta)$ in $\mathbb{Z}$, but 11 is prime, so $N_K(\alpha)$ or $N_K(\beta)$ is equal to ± 1. Use the Exercise 3.3 and α or β is a unit. It follows that $\zeta+2$ has no proper factors in $\mathbb{Z}[\zeta]$. And $11 = (\zeta+2)(\zeta^2+2)(\zeta^3+2)(\zeta^4+2)$

(ii) $N_K(\zeta-2) = \frac{(-2)^5+1^5}{1-2} = \frac{-31}{-1} = 31$. 31 is also prime so we can do the same proof than above. And $31 = (\zeta-2)(\zeta^2-2)(\zeta^3-2)(\zeta^4-2)$

(iii) $N_K(\zeta+3) = \frac{3^5+1^5}{1+3} = \frac{244}{4} = 61$. 61 is also prime so we can do the same proof than above. And $61 = (\zeta+3)(\zeta^2+3)(\zeta^3+3)(\zeta^4+3)$

Exercise 3.7.
If $\zeta = e^{2\pi i/5}$, as in Question 3.6, calculate

(i) $N_K(\zeta+4)$

(ii) $N_K(\zeta-3)$.

Deduce that any proper factors of $\zeta + 4$ in $[\zeta]$ have norm 5 or 41. Given $\zeta - 1$ is a factor of $\zeta + 4$, find another factor. Verify $\zeta - 3$ is a unit times $(\zeta + 2)^2$ in $\mathbb{Z}[\zeta]$.

Solution. (i) $N_K(\zeta + 4) = \dfrac{4^5 + 1^5}{4 + 1} = \dfrac{1025}{5} = 205 = 41 \times 5$. If $\zeta + 4 = \alpha\beta$ with α and β not units, then $N(\alpha)N(\beta) = N(\zeta+4) = 41\times 5$. 5 and 41 are primes and we can't have $N(\alpha) = \pm 1$ because α and β are not unit. Then any proper factors of $\zeta+4$ have norm 5 or 41. Let $t = \zeta-1$, we know that $\dfrac{\zeta^5 - 1}{\zeta - 1} = 0$. So $0 = \dfrac{(t+1)^5 - 1}{t} = \dfrac{t^5 + 5t^4 + 10t^3 + 10t^2 + 5t + 1 - 1}{t} = t^4 + 5t^3 + 10t^2 + 10t + 5 = 0$. Then $5 = -t(t^3 + 5t^2 + 10t + 10)$, and $\zeta + 4 = \zeta - 1 + 5 = \zeta - 1 - (\zeta - 1)((\zeta - 1)^3 + 5(\zeta - 1)^2 + 10(\zeta - 1) + 10) = (\zeta - 1)(-9 - 10(\zeta - 1) - 5(\zeta - 1)^2 - (\zeta - 1)^3) = \zeta + 4$.

(ii) $N_K(\zeta - 3) = \dfrac{(-3)^5 + 1^5}{-3 + 1} = \dfrac{-242}{-2} = 121$. While developing a system we can find that $\zeta - 3 = (\zeta^2 + 2)^2(\zeta + \zeta^2)$, we have to prove that $(\zeta + \zeta^2)$ is a unit. We use the Exercise 3.3 and the Exercise 3.2(ii). $N(\zeta + \zeta^2) = 1$ and it follows that it's a unit.

Exercise 3.8.
Show that the multiplicative group of non-zero elements of $\mathbb{Z}_7$ is cyclic with generator the residue class of 3. If $\zeta = e^{2\pi i/7}$, define the monomorphism $\sigma : \mathbb{Q}(\zeta) \to \mathbb{C}$ by $\sigma(\zeta) = \zeta^3$. Show that all other monomorphisms from $\mathbb{Q}(\zeta)$ to $\mathbb{C}$ are of the form σ^i $(1 \leqslant i \leqslant 6)$ where $\sigma^6 = 1$. For any $\alpha \in \mathbb{Q}(\zeta)$, define $c(\alpha) = \alpha\sigma^2(\alpha)\sigma^4(\alpha)$, and show $N(\alpha) = c(\alpha).\sigma c(\alpha)$. Demonstrate that $c(\alpha) = \sigma^2 c(\alpha) = \sigma^4 c(\alpha)$. Using the relation $1 + \zeta + ... + \zeta^6 = 0$, show that every element $\alpha \in \mathbb{Q}(\zeta)$ can be written uniquely as $\sum_{i=1}^{6} a_i\zeta^i$ $(a_i \in \mathbb{Q})$. Deduce that $c(\alpha) = a_1\theta_1 + a_3\theta_2$ where $\theta_1 = \zeta + \zeta^2 + \zeta^4$, $\theta_2 = \zeta^3 + \zeta^5 + \zeta^6$. Show $\theta_1 + \theta_2 = -1$ and calculate $\theta_1\theta_2$. Verify that $c(\alpha)$ may be written in the form $b_0 + b_1\theta_1$ where $b_0, b_1 \in \mathbb{Q}$, and show $\sigma c(\alpha) = b_0 + b_1\theta_2$. Deduce $N(\alpha) = b_0^2 - b_0b_1 + 2b_1^2$. Now calculate $N(\zeta + 5\zeta^6)$.

Solution. The multiplicative group G of non-zero elements of $\mathbb{Z}_7$ is $\{1, 2, 3, 4, 5, 6\}$. And $3 \equiv 3[7]$, $3^2 \equiv 2[7]$, $3^3 \equiv 6[7]$, $3^4 \equiv 4[7]$, $3^5 \equiv 5[7]$, $3^6 \equiv 1[7]$ So 3 is a generator of G. The monomorphisms are $\phi_i(\zeta) = \zeta^i$ for $i \in [\![1; 6]\!]$ and $\sigma = \phi_3, \sigma^2 = \phi_2, \sigma^3 = \phi_6, \sigma^4 = \phi_4, \sigma^5 = \phi_5$ and $\sigma^6 = \phi_1 = 1$ (identity function).

By definition $N(\alpha) = \sigma(\alpha)\sigma^2(\alpha)\sigma^3(\alpha)\sigma^4(\alpha)\sigma^5(\alpha)\sigma^6(\alpha)$ and $\sigma c(\alpha) = \sigma(\alpha)\sigma^3(\alpha)\sigma^5(\alpha)$, so $c(\alpha).\sigma c(\alpha) = \sigma(\alpha)\sigma^3(\alpha)\sigma^5(\alpha)\alpha\sigma^2(\alpha)\sigma^4(\alpha) = \sigma(\alpha)\sigma^3(\alpha)\sigma^5(\alpha)\sigma^6(\alpha)\sigma^2(\alpha)\sigma^4(\alpha) = N(\alpha)$. $\sigma^2 c(\alpha) = \sigma^2(\alpha)\sigma^4(\alpha)\sigma^6(\alpha) = c(\alpha)$ and $\sigma^4 c(\alpha) = \sigma^4(\alpha)\sigma^6(\alpha)\sigma^2(\alpha) = c(\alpha)$.

$1 + X + X^2 + X^3 + X^4 + X^5 + X^6$ is the minimum polynomial of ζ in $\mathbb{Q}[X]$, so $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 6$ and $\{1, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5\}$ is a $\mathbb{Q}-$basis of $\mathbb{Q}(\zeta)$. But $1 = -\zeta^6 - \zeta^5 - \zeta^4 - \zeta^3 - \zeta^2 - \zeta$, so $\{\zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5, \zeta^6\}$ is also a $\mathbb{Q}-$basis of $\mathbb{Q}(\zeta)$. For $\alpha \in \mathbb{Q}(\zeta)$, $c(\alpha) = a_1\zeta + a_2\zeta^2 + a_3\zeta^3 + a_4\zeta^4 + a_5\zeta^5 + a_6\zeta^6$ with

$a_i \in \mathbb{Q}$. $c(\alpha) = \sigma^2 c(\alpha) = a_1\sigma^2(\zeta) + a_2\sigma^2(\zeta^2) + a_3\sigma^2(\zeta^3) + a_4\sigma^2(\zeta^4) + a_5\sigma^2(\zeta^5) + a_6\sigma^2(\zeta^6) = a_4\zeta + a_1\zeta^2 + a_6\zeta^3 + a_2\zeta^4 + a_3\zeta^5 + a_5\zeta^6 = \sigma^4 c(\alpha) = a_2\zeta + a_4\zeta^2 + a_5\zeta^3 + a_1\zeta^4 + a_6\zeta^5 + a_3\zeta^6$, then by identification we have $a_1 = a_2 = a_4$ and $a_3 = a_5 = a_6$, hence $c(\alpha) = a_1\theta_1 + a_3\theta_2$.

$\theta_1+\theta_2 = \zeta+\zeta^2+\zeta^3+\zeta^4+\zeta^5+\zeta^6 = -1$ because $1+X+X^2+X^3+X^4+X^5+X^6$ is the minimum polynomial of ζ. $\theta_1\theta_2 = (\zeta+\zeta^2+\zeta^4)(\zeta^3+\zeta^5+\zeta^6) = \zeta^4+\zeta^6+\zeta^7+\zeta^5+\zeta^7+\zeta^8+\zeta^7+\zeta^9+\zeta^10 = \zeta^4+\zeta^6+1+\zeta^5+1+\zeta+1+\zeta^2+\zeta^3 = 2$ because $1+\zeta+\zeta^2+\zeta^3+\zeta^4+\zeta^5+\zeta^6 = 0$. $c(\alpha) + a_3\theta_1 = a_1\theta_1 + a_3(\theta_2+\theta_1) = a_1\theta_1 - a_3$, then $c(\alpha) = -a_3 + (a_1 - a_3)\theta_1$. We have $b_0 = -a_3$ and $b_1 = a_1 - a_3$. $\sigma c(\alpha) = \sigma(b_0 + b_1\theta_1) = b_0 + b_1\sigma(\theta_1) = b_0 + b_1\theta_2$ (look at the definition of θ_1 and θ_2). $N(\alpha) = c(\alpha)\sigma c(\alpha) = (b_0 + b_1\theta_1)(b_0 + b_1\theta_2) = b_0^2 - b_1b_0 + 2b_1^2$.

$\alpha = \zeta + 5\zeta^6$. $c(\alpha) = (\zeta + 5\zeta^6)(\zeta^2 + 5\zeta^5)(\zeta 4 + 5\zeta^3) = -101\theta_1 - 121\theta_2 = 121 + 20\theta_1$. So $b_0 = 121$ and $b_1 = 20$, hence $N(\alpha) = b_0^2 - b_1b_0 + 2b_1^2 = 121^2 - 20.121 + 2.20^2 = 13021$.

Exercise 3.9.
Suppose p is a rational prime and $\zeta = e^{2\pi i/p}$. Given that the group of non-zero elements of $\mathbb{Z}_p$ is cyclic (see Appendix 1, Proposition 6 for a proof) show that there exists a monomorphism $\sigma : \mathbb{Q}(\zeta) \to \mathbb{C}$ such that σ^{p-1} is the identity and all monomorphisms from $\mathbb{Q}(\zeta)$ to $\mathbb{C}$ are of the form σ^i $(1 \leqslant i \leqslant p-1)$. If $p-1 = kr$, define $c_k(\alpha) = \alpha\sigma^r(\alpha)\sigma^{2r}(\alpha)...\sigma^{(k-1)r}(\alpha)$. Show $N(\alpha) = c_k(\alpha).\sigma c_k(\alpha)...\sigma^{r-1}c_k(\alpha)$. Prove every element of $\mathbb{Q}(\zeta)$ is uniquely of the form $\sum_{i=1}^{p-1} a_i\zeta^i$, and by demonstrating that $\sigma^r(c_k(\alpha)) = c_k(\alpha)$, deduce that $c_k(\alpha) = b_1\eta_1 + ... + b_n\eta_n$, where $\eta_1 = \zeta + \sigma^r(\zeta) + \sigma^{2r}(\zeta) + ... + \sigma^{(k-1)r}(\zeta)$ and $\eta_{i+1} = \sigma^i(\eta_1)$. Interpret these results in the case $p = 5$, $k = r = 2$, by showing that the residue class of 2 is a generator of the multiplicative group of non-zero elements of $\mathbb{Z}_5$. Demonstrate that $c_2(\alpha)$ is of the form $b_1\eta_1 + b_2\eta_2$ where $\eta_1 = \zeta + \zeta^4$, $\eta_2 = \zeta^2 + \zeta^3$.Calculate the norms of the following elements in $\mathbb{Q}(\zeta)$:

(i) $\zeta + 2\zeta^2$

(ii) $\zeta + \zeta^4$

(iii) $15\zeta + 15\zeta^4$

(iv) $\zeta + \zeta^2 + \zeta^3 + \zeta^4$.

Solution. $\mathbb{Z}_p$ is cyclic, so there exists an element k that generates $\mathbb{Z}_p^\times$ (i.e. for all j in $\mathbb{Z}_p$ there exists i such that $j = k^i$ and $k^{p-1} = 1$). We define the monomorphism $\sigma : \zeta \mapsto \zeta^k$. All the monomorphisms $\phi_j : \zeta \mapsto \zeta^j$ can be written as σ^i because for all j, we can find i such that $j = k^i$ and $\sigma^{p-1}(\zeta) = \zeta^{k^{p-1}} = \zeta^1 = \zeta$, hence σ^{p-1} is the identity. $N(\alpha) = \prod_{i=1}^{p-1}\sigma^i(\alpha)$ and $c_k(\alpha).\sigma c_k(\alpha)...\sigma^{r-1}c_k(\alpha) = \alpha\sigma^r(\alpha)\sigma^{2r}(\alpha)...\sigma^{(k-1)r}(\alpha).\sigma(\alpha)\sigma^{r+1}(\alpha)\sigma^{2r+1}(\alpha)...\sigma^{(k-1)r+1}(\alpha). ... .\sigma^{r-1}(\alpha).\sigma^{2r-1}(\alpha)\sigma^{3r-1}(\alpha)...\sigma^{kr-1}(\alpha)$ but $kr-1 = p-2$ and $\alpha = \sigma^{p-1}(\alpha)$, then while changing the order of the factors, we find exactly the norm. As the Exercise 3.8, we can write every element of $\mathbb{Q}(\zeta)$ uniquely with the form $\sum_{i=1}^{p-1} a_i\zeta^i$ because $B = \{\zeta, \zeta^2, ..., \zeta^{p-1}\}$ is a $\mathbb{Q}$-basis

of $\mathbb{Q}(\zeta)$. $\sigma^r c_k(\alpha) = \sigma^r(\alpha\sigma^r(\alpha)\sigma^{2r}(\alpha)...\sigma^{(k-1)r}(\alpha)) = \sigma^r(\alpha)\sigma^{2r}(\alpha)...\sigma^{kr}(\alpha) = c_k(\alpha)$ because $kr = p-1$ and σ^{p-1} is the identity. Let $c_k(\alpha)$ be written as $\sum_{i=1}^{p-1} a_i\zeta^i$, then apply σ^r and identify the coefficient of the basis B. then we will find $a_1 = a_r = a_{2r} = ... = a_{(k-1)r}$ that we will call b_1 and the same thing happens for all b_j. (It's the same idea than in the Exercise 3.8).

$2^1 \equiv 2[5]$, $2^2 \equiv 4[5]$, $2^3 \equiv 3[5]$, $2^4 \equiv 1[5]$, so 2 generates $\mathbb{Z}_5^\times$. We have $\sigma : \zeta \mapsto \zeta^2$ and σ^4 is the identity. $c_2(\alpha) = \alpha\sigma^2(\alpha)$ and $\sigma^2 c_2(\alpha) = c_2(\sigma)$ because $\sigma^4(\alpha) = \alpha$. We can write $c_2(\alpha) = a_1\zeta + a_2\zeta^2 + a_3\zeta^3 + a_4\zeta^4 = \sigma^2(a_1\zeta + a_2\zeta^2 + a_3\zeta^3 + a_4\zeta^4) = a_1\zeta^4 + a_2\zeta^3 + a_3\zeta^2 + a_4\zeta$, then $a_1 = a_4$ and $a_2 = a_3$. So $c_2(\alpha) = b_1\eta_1 + b_2\eta_2$ with $\eta_1 = \zeta + \zeta^4$ and $\eta_2 = \zeta^2 + \zeta^3$.

(i) $\alpha = \zeta + 2\zeta^2$. $c_2(\alpha) = (\zeta+2\zeta^2)(\zeta^4+2\zeta^3) = -3\eta_1 - 5\eta_2$ where $\eta_1 = \zeta+\zeta^4$ and $\eta_2 = \zeta^2+\zeta^3$. By calculating, we have $\sigma c_2(\alpha) = -3\eta_2 - 5\eta_1$, $\eta_1 + \eta_2 = -1$, $\eta_1\eta_2 = -1$, $\eta_2^2 = 2+\eta_1$ and $\eta_1^2 = 2+\eta_2$. Then, $N(\alpha) = (-3\eta_1 - 5\eta_2)(-3\eta_2 - 5\eta_1) = -9 - 25 + 15(2+\eta_1) + 15(2+\eta_2) = 30 + 30 - 9 - 25 - 15 = 11$.

(ii) $\alpha = \zeta + \zeta^4$. $c_2(\alpha) = (\zeta + \zeta^4)(\zeta^4 + \zeta) = 2 + \eta_2$ where $\eta_1 = \zeta + \zeta^4$ and $\eta_2 = \zeta^2 + \zeta^3$. By calculating, we have $\sigma c_2(\alpha) = 2 + \eta_1$, $\eta_1 + \eta_2 = -1$ and $\eta_1\eta_2 = -1$. Then, $N(\alpha) = (2+\eta_1)(2+\eta_2) = 4 + 2(\eta_1+\eta_2) + \eta_1\eta_2 = 4 - 2 - 1 = 1$.

(iii) $N(15\zeta + 15\zeta^4) = N(15)N(\zeta + \zeta^4) = 15^4.1 = 50625$

(iv) $N(\zeta + \zeta^2 + \zeta^3 + \zeta^4) = N(-1) = (-1)^4 = 1$.

Exercise 3.10.
In $\mathbb{Z}[\sqrt{-5}]$, prove 6 factorizes in two ways as

$$6 = 2.3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

Verify that 2, 3, $1 + \sqrt{-5}$, $1 - \sqrt{-5}$ have no proper factors in $\mathbb{Z}[\sqrt{-5}]$. (Hint: Take norms and note that if γ factorizes as $\gamma = \alpha\beta$, then $N(\gamma) = N(\alpha)N(\beta)$ is a factorization of rational integers.) Deduce that it is possible in $\mathbb{Z}[\sqrt{-5}]$ for 2 to have no proper factors, yet 2 divides a product $\alpha\beta$ without dividing either α or β.

Solution. $2.3 = 6$ and $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 1^2 - (-5) = 6$.

$N(2) = 2^2 = 4$ but if $2 = \alpha\beta$ with α, β not units (i.e $N(\alpha)$ and $N(\beta)$ are different than ± 1), therefore $N(2) = 4 = N(\alpha)N(\beta)$. It follows $N(\alpha) = 2$ but it's impossible in $\mathbb{Z}$ because if $\alpha = a + b\sqrt{-5}$, then $N(\alpha) = a^2 + 5b^2 = 2$ that implies $b = 0$ (because a^2 and $5b^2$ are positives and for $b > 0$, $N(\alpha) > 5$) and $a = \sqrt{2} \notin \mathbb{Z}$. It follows that 2 have no proper factors in $\mathbb{Z}[\sqrt{-5}]$.

$N(3) = 3^2 = 9$, for the same raisons and because $a = \sqrt{3} \notin \mathbb{Z}$, 3 have no proper factors in $\mathbb{Z}[\sqrt{-5}]$.

$N(1 + \sqrt{-5}) = 1 + 5 = 6$. If $1 + \sqrt{-5} = \alpha\beta$, then $N(\alpha) = 2$ and $N(\beta) = 3$ (or vice versa) and it is not possible for the same raisons than above. It follows that $1 + \sqrt{-5}$ have no proper factors in $\mathbb{Z}[\sqrt{-5}]$.

$N(1-\sqrt{-5}) = 1+5 = 6$. Same case than $1+\sqrt{-5}$.

So 2 have no proper factors and 2 divides 6(= 2.3) then 2 divides $(1+\sqrt{-5})(1-\sqrt{-5})$ but 2 divides either $1+\sqrt{-5}$ or $1-\sqrt{-5}$.

4.4 Factorization into irreducibles p.102

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's 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 $a^2+b^2 = 7$ have 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 for $1+i$, $N(-4+5i) = 4^2+5^2 = 41$ which is irreducible (because prime in $\mathbb{Z}$), hence $-4+5i$ is irreducible.

Exercise 4.2.
Write down the group of units of the ring of integers of: $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{-5})$, $\mathbb{Q}(\sqrt{-6})$.

Solution. We use the Proposition 4.2, then $U(\mathbb{Q}(\sqrt{-1})) = \{\pm 1, \pm i\}$, $U(\mathbb{Q}(\sqrt{-2})) = \{\pm 1\}$, $U(\mathbb{Q}(\sqrt{-3})) = \{\pm 1, \pm\omega, \pm\omega^2\}$ where $\omega = e^{2\pi i/3}$, $U(\mathbb{Q}(\sqrt{-5})) = \{\pm 1\}$ and $U(\mathbb{Q}(\sqrt{-6})) = \{\pm 1\}$.

Exercise 4.3.
Is the group of units of the integers in $\mathbb{Q}(\sqrt{3})$ finite ?

Solution. The norm in $\mathbb{Q}(\sqrt{3})$ is $N(a+b\sqrt{3}) = a^2-3b^2$. If $\alpha\beta = 1$ (with $\alpha, \beta \in \mathbb{Z}$), then $N(\alpha)N(\beta) = 1$. But $N(\alpha) \in \mathbb{Z}$, then $N(\alpha) = \pm 1$. We looking for $a, b \in \mathbb{Z}$ such that $a^2-3b^2 = \pm 1$. We will prove that $a^2-3b^2 = 1$ have an infinite number of solutions. Use Pell's equation, $a = 2$ and $b = 1$ is the fundamental solution, $2+\sqrt{3}$ is a unit and all $(2+\sqrt{3})^n$ are a unit (for $n \in \mathbb{N}$), but if we write $(2+\sqrt{3})^n = x_n + y_n\sqrt{3}$, we see that $(x_n)_{n\in\mathbb{N}}$ is a strictly increasing sequence. It follows that the group of units of the integers in $\mathbb{Q}(\sqrt{3})$ is infinite.

Exercise 4.4.
Show that a homomorphic image of a noetherian ring is noetherian.

Solution. Let $\phi : A \to B$ be a ring homomorphism with A a noetherian ring. We want to prove that $\phi(A)$ is also noetherian. Let J be an ideal of $\phi(A)$, $\phi^{-1}(J) =: I$ is an ideal of A, but A is noetherian, so each ideal of A is finite generated, hence it exists $\{x_1, x_2, ..., x_n\}$ that generate I. Then $\{\phi(x_1), ..., \phi(x_n)\}$ generate J (because $I = \phi^{-1}(J)$), so J is finite generated and it follows that $\phi(A)$ is noetherian.

Exercise 4.5.
Find all ideals of $\mathbb{Z}$ contained in $\langle 120\rangle$. Show that every ascending chain of ideals of $\mathbb{Z}$ starting with $\langle 120\rangle$ stops, by direct examination of the possibilities.

Solution. All the ideals of $\mathbb{Z}$ can be written $\langle a\rangle$ where $a \in \mathbb{Z}$ because $\mathbb{Z}$ is principal. Then we use the Proposition 4.4 and see that $\langle x\rangle \subset \langle 120\rangle$ if and only if $120 \mid x$. It follows that all ideals of $\mathbb{Z}$ contained in $\langle 120\rangle$ are $\langle 120n\rangle$ where $n \in \mathbb{Z}$.

We can use again the Proposition 4.4, see $\langle 120\rangle \subset \langle x\rangle$ if and only if $x \mid 120$. The only positive divisors of 120 are $2, 3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30, 40, 60$, so every ascending chain of ideals starting with $\langle 120\rangle$ stops. (We can do that with every rational integer, that's why $\mathbb{Z}$ is noetherian.)

Exercise 4.6.
Find a ring which is not noetherian.

Solution. We can reuse the example of the Exercise 1.13, the ring $\mathbb{R}[X_1, X_2, ...]$. While using Proposition 4.5, we see that the ascending chain $\langle X_1\rangle \subset \langle X_1, X_2\rangle \subset \langle X_1, X_2, X_3\rangle \subset ...$ does not stop, then the ring $\mathbb{R}[X_1, X_2, ...]$ cannot be noetherian.

Exercise 4.7.
Check the calculations required to complete Theorems 4.10, 4.11.

Solution. Theorem 4.10

(i) 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 $b = 0$ and 2 and 3 are not a square. It follows that $2, 3, \sqrt{-6}$ are irreducible. Using Proposition 4.9(b) and definition of unique factorization, factorization in $\mathbb{Q}(\sqrt{-6})$ is not unique.

(ii) In $\mathbb{Q}(\sqrt{-10})$, $14 = 2.7 = (2+\sqrt{-10})(2-\sqrt{-10})$. We want to prove that $2, 7, 2+\sqrt{-10}, 2-\sqrt{-10}$ are irreducible. The norm in $\mathbb{Q}(\sqrt{-10})$ is $N(a+b\sqrt{-10}) = a^2+10b^2$. The norm of $2, 7, 2+\sqrt{-10}, 2-\sqrt{-10}$ are respectively $4, 49, 14, 14$. 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 $7, 2+\sqrt{-10}, 2-\sqrt{-10}$. The proper factors of $4, 49, 14, 14$ are 2 and 7. But $a^2+10b^2 = 2$ or 7 have no solutions, because that implies $b = 0$ and 2 and 7 are not a square. It follows that $2, 7, 2+\sqrt{-10}, 2-\sqrt{-10}$ are irreducible. Using Proposition 4.9(b) and definition of unique factorization, factorization in $\mathbb{Q}(\sqrt{-10})$ is not unique.

(iii) In $\mathbb{Q}(\sqrt{-13})$, $14 = 2.7 = (1+\sqrt{-13})(1-\sqrt{-13})$. We want to prove that $2, 7, 1+\sqrt{-13}, 1-\sqrt{-13}$ are irreducible. The norm in $\mathbb{Q}(\sqrt{-13})$ is $N(a+b\sqrt{-13}) = a^2+13b^2$. The norm of $2, 7, 1+\sqrt{-13}, 1-\sqrt{-13}$ are respectively $4, 49, 14, 14$. 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 $7, 1+\sqrt{-13}, 1-\sqrt{-13}$. The proper factors of $4, 49, 14, 14$ are 2 and 7. But $a^2+13b^2 = 2$ or 7 have no solutions, because that implies $b = 0$ and 2 and 7 are not a square. It follows that $2, 7, 1+\sqrt{-13}, 1-\sqrt{-13}$ are irreducible. Using Proposition 4.9(b) and definition of unique factorization, factorization in $\mathbb{Q}(\sqrt{-13})$ is not unique.

(iv) In $\mathbb{Q}(\sqrt{-14})$, $15 = 3.5 = (1+\sqrt{-14})(1-\sqrt{-14})$. We want to prove that $3, 5, 1+\sqrt{-14}, 1-\sqrt{-14}$ are irreducible. The norm in $\mathbb{Q}(\sqrt{-14})$ is $N(a+b\sqrt{-14}) = a^2+14b^2$. The norm of $3, 5, 1+\sqrt{-14}, 1-\sqrt{-14}$ are respectively $9, 25, 15, 15$. If $3 = \alpha\beta$, then $N(3) = 9 = N(\alpha)N(\beta)$ with $N(\alpha)$ and $N(\beta)$ proper factors of 9 and we can also do that for $5, 1+\sqrt{-14}, 1-\sqrt{-14}$. The proper factors of $9, 25, 15, 15$ are 3 and 5. But $a^2+14b^2 = 3$ or 5 have no solutions, because that implies $b = 0$ and 3 and 5 are not a square. It follows that $3, 5, 1+\sqrt{-14}, 1-\sqrt{-14}$ are irreducible. Using Proposition 4.9(b) and definition of unique factorization, factorization in $\mathbb{Q}(\sqrt{-14})$ is not unique.

(v) In $\mathbb{Q}(\sqrt{-15})$, $4 = 2.2 = (\frac{1+\sqrt{-15})}{2}(\frac{1-\sqrt{-15}}{2})$. We want to prove that $2, \frac{1+\sqrt{-15}}{2}, \frac{1-\sqrt{-15}}{2}$ are irreducible. An integral basis in $\mathbb{Q}(\sqrt{-15})$ is $\{1, \frac{1+\sqrt{-15}}{2}\}$ because $-15 \equiv 1[4]$. The norm in $\mathbb{Q}(\sqrt{-15})$ is $N(a+b\frac{1+\sqrt{-15}}{2}) = (a+\frac{b}{2})^2+15(\frac{b}{2})^2 = a^2+ab+4b^2$. The norm of $2, \frac{1+\sqrt{-15}}{2}, \frac{1-\sqrt{-15}}{2}$ are respectively $4, 4, 6$. 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 $\frac{1+\sqrt{-15}}{2}, \frac{1-\sqrt{-15}}{2}$. The proper factors of $4, 4, 6$ are 2 and 3. But $a^2+ab+4b^2 = 2$ or 3 have no solutions, because that implies $b = 0$ (because $(a+\frac{b}{2})^2+15(\frac{b}{2})^2 = 2$ implies $b = 0$) and 2 and 3 are not a square. It follows that $2, \frac{1+\sqrt{-15}}{2}, \frac{1-\sqrt{-15}}{2}$ are irreducible. Using Proposition 4.9(b) and definition of unique factorization, factorization in $\mathbb{Q}(\sqrt{-15})$ is not unique.

(vi) In $\mathbb{Q}(\sqrt{-17})$, $18 = 2.3.3 = (1+\sqrt{-17})(1-\sqrt{-17})$. We want to prove

that $2, 3, 1+\sqrt{-17}, 1-\sqrt{-17}$ are irreducible. The norm in $\mathbb{Q}(\sqrt{-17})$ is $N(a+b\sqrt{-17}) = a^2+17b^2$. The norm of $2, 3, 1+\sqrt{-17}, 1-\sqrt{-17}$ are respectively $4, 9, 18, 18$. 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 $3, 1+\sqrt{-17}, 1-\sqrt{-17}$. The proper factors of $4, 9, 18, 18$ are 2, 3 (9 doesn't matter because $18 = 9.2$ so there is at least a proper factor in $\{2, 3\}$). But $a^2+17b^2 = 2$ or 3 have no solutions, because that implies $b = 0$ and 2 and 3 are not a square. It follows that $2, 3, 1+\sqrt{-17}, 1-\sqrt{-17}$ are irreducible. Using Proposition 4.9(b) and definition of unique factorization, factorization in $\mathbb{Q}(\sqrt{-17})$ is not unique.

(vii) In $\mathbb{Q}(\sqrt{-21})$, $22 = 2.11 = (1+\sqrt{-21})(1-\sqrt{-21})$. We want to prove that $2, 11, 1+\sqrt{-21}, 1-\sqrt{-21}$ are irreducible. The norm in $\mathbb{Q}(\sqrt{-21})$ is $N(a+b\sqrt{-21}) = a^2+21b^2$. The norm of $2, 11, 1+\sqrt{-21}, 1-\sqrt{-21}$ are respectively $4, 121, 22, 22$. 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 $11, 1+\sqrt{-21}, 1-\sqrt{-21}$. The proper factors of $4, 121, 22, 22$ are 2, 11. But $a^2+21b^2 = 2$ or 11 have no solutions, because that implies $b = 0$ and 2 and 11 are not a square. It follows that $2, 11, 1+\sqrt{-21}, 1-\sqrt{-21}$ are irreducible. Using Proposition 4.9(b) and definition of unique factorization, factorization in $\mathbb{Q}(\sqrt{-21})$ is not unique.

(viii) In $\mathbb{Q}(\sqrt{-22})$, $26 = 2.13 = (2+\sqrt{-22})(2-\sqrt{-22})$. We want to prove that $2, 13, 2+\sqrt{-22}, 2-\sqrt{-22}$ are irreducible. The norm in $\mathbb{Q}(\sqrt{-22})$ is $N(a+b\sqrt{-22}) = a^2+22b^2$. The norm of $2, 13, 2+\sqrt{-22}, 2-\sqrt{-22}$ are respectively $4, 169, 26, 26$. 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 $13, 2+\sqrt{-22}, 2-\sqrt{-22}$. The proper factors of $4, 169, 26, 26$ are 2, 13. But $a^2+22b^2 = 2$ or 13 have no solutions, because that implies $b = 0$ and 2 and 13 are not a square. It follows that $2, 13, 2+\sqrt{-22}, 2-\sqrt{-22}$ are irreducible. Using Proposition 4.9(b) and definition of unique factorization, factorization in $\mathbb{Q}(\sqrt{-22})$ is not unique.

(ix) In $\mathbb{Q}(\sqrt{-23})$, $6 = 2.3 = (\frac{1+\sqrt{-23})}{2}(\frac{1-\sqrt{-23}}{2})$. We want to prove that $2, 3, \frac{1+\sqrt{-23}}{2}, \frac{1-\sqrt{-23}}{2}$ are irreducible. An integral basis in $\mathbb{Q}(\sqrt{-23})$ is $\{1, \frac{1+\sqrt{-23}}{2}\}$ because $-23 \equiv 1[4]$. The norm in $\mathbb{Q}(\sqrt{-23})$ is $N(a+b\frac{1+\sqrt{-23}}{2}) = (a+\frac{b}{2})^2+23(\frac{b}{2})^2 = a^2+ab+6b^2$. The norm of $2, 3, \frac{1+\sqrt{-23}}{2}, \frac{1-\sqrt{-23}}{2}$ are respectively $4, 9, 6, 8$. 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 $3, \frac{1+\sqrt{-23}}{2}, \frac{1-\sqrt{-23}}{2}$. The proper factors of $4, 9, 6, 8$ are 2, 3 and 4 (But 4 doesn't matter because 8=4.2 so there is at least a proper factor which is 2). But $a^2+ab+6b^2 = 2$ or 3 have no solutions, because that implies $b = 0$ (because $(a+\frac{b}{2})^2+23(\frac{b}{2})^2 = 2$ implies $b = 0$) and 2 and 3 are not a square. It follows that $2, 3, \frac{1+\sqrt{-23}}{2}, \frac{1-\sqrt{-23}}{2}$ are irreducible. Using Proposition 4.9(b) and definition of unique factorization, factorization in $\mathbb{Q}(\sqrt{-23})$ is not unique.

(x) In $\mathbb{Q}(\sqrt{-26})$, $27 = 3.3.3 = (1+\sqrt{-26})(1-\sqrt{-26})$. We want to prove that $3, 1+\sqrt{-26}, 1-\sqrt{-26}$ are irreducible. The norm in $\mathbb{Q}(\sqrt{-26})$ is $N(a+b\sqrt{-26}) = a^2+26b^2$. The norm of $3, 1+\sqrt{-26}, 1-\sqrt{-26}$ are respectively $9, 27, 27$. If $3 = \alpha\beta$, then $N(3) = 9 = N(\alpha)N(\beta)$ with $N(\alpha)$ and $N(\beta)$ proper factors of 4 and we can also do that for $3, 1+\sqrt{-26}, 1-\sqrt{-26}$. The proper factors of $9, 27, 27$ are 3 and 9. (But 9 doesn't matter because 27=9.3 so there is at least a proper factor which is 3). But $a^2+26b^2 = 3$ have no solutions, because that implies $b = 0$ and 3 is not a square. It follows that $3, 1+\sqrt{-26}, 1-\sqrt{-26}$ are irreducible. Using Proposition 4.9(b) and definition of unique factorization, factorization in $\mathbb{Q}(\sqrt{-26})$ is not unique.

(xi) In $\mathbb{Q}(\sqrt{-29})$, $30 = 2.3.5 = (1+\sqrt{-29})(1-\sqrt{-29})$. We want to prove that $2, 3, 5, 1+\sqrt{-29}, 1-\sqrt{-29}$ are irreducible. The norm in $\mathbb{Q}(\sqrt{-29})$ is $N(a+b\sqrt{-29}) = a^2+29b^2$. The norm of $2, 3, 5, 1+\sqrt{-29}, 1-\sqrt{-29}$ are respectively $4, 9, 25, 30, 30$. 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 $3, 5, 1+\sqrt{-29}, 1-\sqrt{-29}$. The proper factors of $4, 9, 25, 30, 30$ are 2, 3, 5. ($10, 6, 15$ doesn't matter because $30 = 15.2 = 10.3 = 6.5$ so there is at least a proper factor in $\{2, 3, 5\}$). But $a^2+29b^2 = 2$ or 3 or 5 have no solutions, because that implies $b = 0$ and 2, 3 and 5 are not a square. It follows that $2, 3, 5, 1+\sqrt{-29}, 1-\sqrt{-29}$ are irreducible. Using Proposition 4.9(b) and definition of unique factorization, factorization in $\mathbb{Q}(\sqrt{-29})$ is not unique.

(xii) In $\mathbb{Q}(\sqrt{-30})$, $34 = 2.17 = (2+\sqrt{-30})(2-\sqrt{-30})$. We want to prove that $2, 17, 2+\sqrt{-30}, 2-\sqrt{-30}$ are irreducible. The norm in $\mathbb{Q}(\sqrt{-30})$ is $N(a+b\sqrt{-30}) = a^2+30b^2$. The norm of $2, 17, 2+\sqrt{-30}, 2-\sqrt{-30}$ are respectively $4, 289, 34, 34$. 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 $17, 2+\sqrt{-30}, 2-\sqrt{-30}$. The proper factors of $4, 289, 34, 34$ are 2, 17. But $a^2+30b^2 = 2$ or 17 have no solutions, because that implies $b = 0$ and 2 and 17 are not a square. It follows that $2, 17, 2+\sqrt{-30}, 2-\sqrt{-30}$ are irreducible. Using Proposition 4.9(b) and definition of unique factorization, factorization in $\mathbb{Q}(\sqrt{-30})$ is not unique.

Theorem 4.11

(i) In $\mathbb{Q}(\sqrt{15})$, $10 = 2.5 = (5+\sqrt{15})(5-\sqrt{15})$. We want to prove that $2, 5, 5+\sqrt{15}, 5-\sqrt{15}$ are irreducible. The norm in $\mathbb{Q}(\sqrt{15})$ is $N(a+b\sqrt{15}) = a^2-15b^2$. The norm of $2, 5, 5+\sqrt{5}, 5-\sqrt{5}$ are respectively $4, 25, 10, 10$. 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 $5, 5+\sqrt{15}, 5-\sqrt{15}$. The proper factors of $4, 25, 10, 10$ are 2, 5. But $a^2-15b^2 = \pm 2$ or ± 5 have no solutions, because if we looked in $\mathbb{Z}_5$, $1^2 \equiv 1[5]$, $2^2 \equiv 4[5]$, $3^2 \equiv 4[5]$, $4^2 \equiv 1[5]$ and $a^2-15b^2 \equiv a^2[5]$ so ± 2 is not possible ($\pm 2 = 2$ or 3 [5]) and for ± 5, the only possibility is $a \equiv 0[5]$, then we looking for u, b such that $(5u)^2-15b^2 = \pm 5$

which is equivalent to $5u^2 - 3b^2 = \pm 1$. We looked in $\mathbb{Z}_5$, $-3.1^2 \equiv 2[5]$, $-3.2^2 \equiv 3[5]$, $-3.3^2 \equiv 3[5]$, $-3.4^2 \equiv 2[5]$ but $\pm 1 \equiv 1$ or 4 [5], hence there is no solution. It follows that $2, 5, 5+\sqrt{15}, 5-\sqrt{15}$ are irreducible. Using Proposition 4.9(b) and definition of unique factorization, factorization in $\mathbb{Q}(\sqrt{15})$ is not unique.

(ii) In $\mathbb{Q}(\sqrt{26})$, $10 = 2.5 = (6+\sqrt{26})(6-\sqrt{26})$. We want to prove that $2, 5, 6+\sqrt{26}, 6-\sqrt{26}$ are irreducible. The norm in $\mathbb{Q}(\sqrt{26})$ is $N(a+b\sqrt{26}) = a^2 - 26b^2$. The norm of $2, 5, 6+\sqrt{26}, 6-\sqrt{26}$ are respectively $4, 25, 10, 10$. 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 $5, 6+\sqrt{26}, 6-\sqrt{26}$. The proper factors of $4, 25, 10, 10$ are 2, 5. But $a^2 - 26b^2 = \pm 2$ or ± 5 have no solutions, because if we looked in $\mathbb{Z}_{13}$, $1^2 \equiv 1[13]$, $2^2 \equiv 4[13]$, $3^2 \equiv 9[13]$, $4^2 \equiv 3[13]$, $5^2 \equiv 12[13]$, $6^2 \equiv 10[13]$, $7^2 \equiv 10[13]$, $8^2 \equiv 12[13]$, $9^2 \equiv 3[13]$, $10^2 \equiv 9[13]$, $11^2 \equiv 4[13]$, $12^2 \equiv 1[13]$ and $a^2 - 26b^2 \equiv a^2[13]$ so ± 2 and ± 5 are not possible ($\pm 2 = 2$ or 11 [13] and $\pm 5 = 5$ or 8 [13]). It follows that $2, 5, 6+\sqrt{26}, 6-\sqrt{26}$ are irreducible. Using Proposition 4.9(b) and definition of unique factorization, factorization in $\mathbb{Q}(\sqrt{26})$ is not unique.

(iii) In $\mathbb{Q}(\sqrt{30})$, $6 = 2.3 = (6+\sqrt{30})(6-\sqrt{30})$. We want to prove that $2, 3, 6+\sqrt{30}, 6-\sqrt{30}$ are irreducible. The norm in $\mathbb{Q}(\sqrt{30})$ is $N(a+b\sqrt{30}) = a^2 - 30b^2$. The norm of $2, 3, 6+\sqrt{30}, 6-\sqrt{30}$ are respectively $4, 9, 6, 6$. 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 $3, 6+\sqrt{30}, 6-\sqrt{30}$. The proper factors of $4, 9, 6, 6$ are 2, 3. But $a^2 - 30b^2 = 2$ or 3 have no solutions, because if we looked in $\mathbb{Z}_5$, $1^2 \equiv 1[5]$, $2^2 \equiv 4[5]$, $3^2 \equiv 4[5]$, $4^2 \equiv 1[5]$ and $a^2 - 30b^2 \equiv a^2[5]$ so 2 and 3 are not possible ($\pm 2 = 2$ or 3 [5] and $\pm 3 = 2$ or 3 [5]), hence there is no solutions. It follows that $2, 3, 6+\sqrt{30}, 6-\sqrt{30}$ are irreducible. Using Proposition 4.9(b) and definition of unique factorization, factorization in $\mathbb{Q}(\sqrt{30})$ is not unique.

Exercise 4.8.
Is $10 = (3+i)(3-i) = 2.5$ an example of non-unique factorization in $\mathbb{Z}[i]$? Give reasons for your answer.

Solution. $\mathbb{Z}[i]$ is well a domain where there is not a unique factorization. But this example doesn't prove it, because 5 is not irreducible $5 = (2+i)(2-i)$. This "proof" is like saying that $24 = 4.6 = 2.12$ is an example of non-unique factorization in $\mathbb{Z}$ (but we know that it's not possible because $\mathbb{Z}$ is principle, hence there is a unique factorization in $\mathbb{Z}$).

Exercise 4.9.
Show that 6 and $2(1+\sqrt{-5})$ both have 2 and $1+\sqrt{-5}$ as factors, but do not have a highest common factors in $\mathbb{Z}[\sqrt{-5}]$. Do they have a least common multiple ? (consider norms.)

Solution. $6 = 2.3 = (1+\sqrt{-5})(1-\sqrt{-5})$, then 6 and $2(1+\sqrt{-5})$ have 2 and $1+\sqrt{-5}$ as factors. The only common factors of 6 and $2(1+\sqrt{-5})$ are 2 and $1+\sqrt{-5}$. If 2 was the highest common factor, we have well $2 \mid 6$ and $2 \mid 2(1+\sqrt{-5})$, but $1+\sqrt{-5}$ works too and $2 \nmid 1+\sqrt{-5}$. It's the same idea for $1+\sqrt{-5}$ because $1+\sqrt{-5} \nmid 2$. It follows that there are no highest common factor in $\mathbb{Z}[\sqrt{-5}]$.

We remind that $\langle ab\rangle = \langle a\rangle\langle b\rangle$. To prove that 6 and $2(1+\sqrt{-5})$ have no least common multiple, we have to prove that $\langle 6\rangle \cap \langle 2(1+\sqrt{-5})\rangle$ can't be written as $\langle l\rangle$ for l in $\mathbb{Z}[\sqrt{-5}]$. But $\langle 6\rangle \cap \langle 2(1+\sqrt{-5})\rangle = \langle 2\rangle(\langle 3\rangle \cap \langle 1+\sqrt{-5}\rangle)$, so if we can express $\langle 6\rangle \cap \langle 2(1+\sqrt{-5})\rangle$ as $\langle l\rangle$ then since $2 \mid 6$ and $2 \mid 2(1+\sqrt{-5})$, we will have $2 \mid l$, hence we can write $l = 2\tilde{l}$ Then we will have $\langle 3\rangle \cap \langle 1+\sqrt{-5}\rangle = \langle \tilde{l}\rangle$. So if we prove that $\langle 3\rangle \cap \langle 1+\sqrt{-5}\rangle$ can't be written as $\langle \tilde{l}\rangle$ for $\tilde{l}$ in $\mathbb{Z}[\sqrt{-5}]$, then $\langle 6\rangle \cap \langle 2(1+\sqrt{-5})\rangle$ can't be written as $\langle l\rangle$.

We want to prove $\langle 3\rangle\langle 1+\sqrt{-5}\rangle \overset{(1)}{\subsetneq} \langle 3\rangle \cap \langle 1+\sqrt{-5}\rangle \overset{(2)}{\subsetneq} \langle 3\rangle$.

Prove of (1): let $\alpha \in \langle 3\rangle\langle 1+\sqrt{-5}\rangle$, then $\alpha = 3(1+\sqrt{-5})\beta$ with $\beta \in \mathbb{Z}[\sqrt{-5}]$. Then $\alpha \in \langle 3\rangle$ and $\alpha \in \langle 1+\sqrt{-5}\rangle$, hence $\alpha \in \langle 3\rangle \cap \langle 1+\sqrt{-5}\rangle$. It follows that $\langle 3\rangle\langle 1+\sqrt{-5}\rangle \subset \langle 3\rangle \cap \langle 1+\sqrt{-5}\rangle$. And $6 \in \langle 3\rangle \cap \langle 1+\sqrt{-5}\rangle$, because $6 = 2.3 = (1+\sqrt{-5})(1-\sqrt{-5})$. But $6 \notin \langle 3\rangle\langle 1+\sqrt{-5}\rangle$, because if $6 = 3(1+\sqrt{-5})(a+b\sqrt{-5})$ with $a, b \in \mathbb{Z}$, $2 = (1+\sqrt{-5})(a+b\sqrt{-5}) = a-5b+(a+b)\sqrt{-5}$, then $a = -b$ and $2 = -6b$. It's impossible because $b \in \mathbb{Z}$. Then $6 \notin \langle 3\rangle\langle 1+\sqrt{-5}\rangle$. It follows (1).

Prove of (2): let $\alpha \in \langle 3\rangle \cap \langle 1+\sqrt{-5}\rangle$, then $\alpha = 3(a+b\sqrt{-5})$ and $\alpha \in \langle 3\rangle$. And 3 is in $\langle 3\rangle$ but $3 \notin \langle 3\rangle \cap \langle 1+\sqrt{-5}\rangle$. It follows (2).

Now we use the norm. $N(\langle 3\rangle\langle 1+\sqrt{-5}\rangle) = N(3)N(1+\sqrt{-5}) = 9 \times 6 = 54$ and $N(\langle 3\rangle) = 9$ so $N(\langle 3\rangle \cap \langle 1+\sqrt{-5}\rangle) \in \{9, 18, 27, 54\}$ (because it's the multiple of 9 and divisors of 54) but cause of inequalities, $N(\langle 3\rangle \cap \langle 1+\sqrt{-5}\rangle) \in \{18, 27\}$. However if $\langle 3\rangle \cap \langle 1+\sqrt{-5}\rangle = \langle l\rangle$, then $N(\langle 3\rangle \cap \langle 1+\sqrt{-5}\rangle) = N(l) = a^2+5b^2$ with $l = a+b\sqrt{-5}$ where $a, b \in \mathbb{Z}$. But $a^2+5b^2 = 18$ or 27 have no solutions, because $b \leqslant 2$ and for $b = 0$, $a^2 = 18$ or 27 is impossible, for $b = 1$, $a^2 = 13$ or 22 is impossible, for $b = 2$, $a^2 = -2$ or 7 is impossible. It follows that $\langle 3\rangle \cap \langle 1+\sqrt{-5}\rangle$ can't be written as $\langle l\rangle$ for l in $\mathbb{Z}[\sqrt{-5}]$.

Exercise 4.10.
Let D be any integral domain. Suppose an element $x \in D$ has a factorization $x = up_1...p_n$ where u is a unit and $p_1, ..., p_n$ are primes. Show that given any factorization $x = vq_1...q_n$ where v is a unit and $q_1, ..., q_n$ are irreducible, there exists a permutation π of $\{1, ..., n\}$ such that $p_i, q_{\pi(i)}$ are associates ($1 \leqslant i \leqslant n$).

Solution. By induction, if $n = 1$, then $up = vq$, so $uv^{-1}p = q$, hence p and q are associate. Now the inductive step ($n > 1$), we have $up_1...p_n = vq_1...q_n$, so $p_1 \mid vq_1...q_n$, but p_1 is prime, so $p_1 \mid q_{i_1}$ for i_1 in $[\![1, n]\!]$ (because $p_1 \mid q_1$ or $p_1 \mid vq_2...q_n$, then if $p_1 \mid q_1$, it's done and if $p_1 \mid vq_2...q_n$, we can do the same process which will end because there is a finite number of factor), then $q_{i_1} = p_1\alpha$ but q_{i_1} is irreducible, then α is a unit and p_1, q_{i_1} are associates. Now $up_2...p_n = v'q_1...q_{i_1-1}q_{i_1+1}...q_n$ while divising by p_1 (the v can change because

$q_{i_1} = p_1\alpha$ with α a unit). And we use the induction hypothesis, because there are $n-1$ factors (that are not unit).

Exercise 4.11.
Show in $\mathbb{Z}[\sqrt{-5}]$ that $\sqrt{-5} \mid (a+b\sqrt{-5})$ if and only if $5 \mid a$. Deduce that $\sqrt{-5}$ is prime in $\mathbb{Z}[\sqrt{-5}]$. Hence conclude that the element 5 factorizes uniquely into irreducibles in $\mathbb{Z}[\sqrt{-5}]$ although $\mathbb{Z}[\sqrt{-5}]$ does not have unique factorization.

Solution. Suppose $5 \mid a$, we have $\sqrt{-5} \mid 5$, then $\sqrt{-5} \mid a$ and $\sqrt{-5} \mid b\sqrt{-5}$, hence $\sqrt{-5} \mid (a+b\sqrt{-5})$. Conversely, $\sqrt{-5} \mid (a+b\sqrt{-5})$, then $a+b\sqrt{-5} = \sqrt{-5}(k+l\sqrt{-5}) = -5l + k\sqrt{-5}$. It follows that $a = -5l$ and $5 \mid a$.

$\sqrt{-5}$ is a prime if $\sqrt{-5} \mid ab$ implies $\sqrt{-5} \mid a$ or $\sqrt{-5} \mid b$. If $\sqrt{-5} \mid (a+b\sqrt{-5})(c+d\sqrt{-5})$ $(a,b,c,d \in \mathbb{Z})$, then $\sqrt{-5} \mid ac-5bd+(ad+bc)\sqrt{-5}$ which is equivalent to $5 \mid ac-5bd$ (first part of the exercise). But $5 \mid 5bd$, so we have $5 \mid ac$. But 5 is a prime in $\mathbb{Z}$, so $5 \mid a$ or $5 \mid c$ which is equivalent to $\sqrt{-5} \mid a+b\sqrt{-5}$ or $\sqrt{-5} \mid c+d\sqrt{-5}$. Hence $\sqrt{-5}$ is a prime in $\mathbb{Z}[\sqrt{-5}]$.

$5 = -\sqrt{-5}\sqrt{-5}$. If $5 = \alpha\beta$, then $\sqrt{-5} \mid \alpha$ or $\sqrt{-5} \mid \beta$ and $\sqrt{-5}$ is a prime so it's an irreducible (Theorem 4.12), hence $(\alpha = \pm\sqrt{-5}$ or $\alpha = \pm 1)$ or $(\beta = \pm\sqrt{-5}$ or $\beta = \pm 1)$. It follows that the factorization of 5 in irreducible is unique. (It's the same ideas than the Theorem 4.13).

Exercise 4.12.
Suppose D is a unique factorization domain, and a, b are coprime non-units. Deduce that if $ab = c^n$ for $c \in D$, then there exists a unit $e \in D$ such that ea and $e^{-1}b$ are nth powers in D.

Solution. D is a unique factorization domain, hence $a = u\prod p_i^{\alpha_i}$, $b = v\prod p_i^{\beta_i}$ and $c = w\prod p_i^{\gamma_i}$ where u, v, w are unit, p_i are prime and $\alpha_i, \beta_i, \gamma_i \in \mathbb{N}$. a, b are coprime so for all i $\alpha_i = 0$ or $\beta_i = 0$. $ab = uv\prod p_i^{\alpha_i+\beta_i} = c^n = w^n\prod p_i^{\gamma_i.n}$, then $uv = w^n$ and $\alpha_i + \beta_i = n.\gamma_i$, but α_i and β_i can be both non zero for one i, hence for $\alpha_i \neq 0$, $\alpha_i = n.\gamma_i$ and for $\beta_i \neq 0$, $\beta_i = n.\gamma_i$. And $uv = w^n$, so if we take $e = u^{-1}$, $ea = \prod p_i^{n.\gamma_i.\mathbb{1}_{\alpha_i\neq 0}}$ and $e^{-1}b = uv\prod p_i^{n.\gamma_i.\mathbb{1}_{\beta_i\neq 0}} = w^n\prod p_i^{n.\gamma_i.\mathbb{1}_{\beta_i\neq 0}}$which are nth powers in D.

Exercise 4.13.
Let p be an odd rational prime and $\zeta = e^{2\pi i/p}$. If α is a prime element in $\mathbb{Z}[\zeta]$, prove that the rational integers which are divisible by α are precisely the rational integer multiples of some prime rational integer q. (Hint: $\alpha \mid N(\alpha)$, so α divides some rational prime factor q of $N(\alpha)$. Now show α is not a factor of any $m \in \mathbb{Z}$ prime to q.)

Solution. We have $\alpha \mid N(\alpha)$ because Identity function is a monomorphism for $\mathbb{Q}(\zeta)$ and the norm is defined as $N_K(\alpha) = \prod \sigma_i(\alpha)$ where σ_i are all the monomorphism of K. But $N(\alpha) \in \mathbb{Z}$ because α is an algebraic integer (Theorem 3.5) and

the norm of an algebraic integer is an integer (let P_α be the minimum 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 $N(\alpha)$ is also an algebraic integer because it's the product of $\sigma(\alpha)$ for all monomorphism σ. But the norm is always in $\mathbb{Q}$, because $N(\alpha) = (-1)^n f_\alpha(0)$ which is a polynomial in $\mathbb{Q}$ (Theorem 2.4). Then use Lemma 2.13 to see that $N(\alpha)$ is an algebraic integer and rational, hence it's a rational integer.) Then we can write $N(\alpha) = p_1...p_k$ where p_i are prime (in $\mathbb{Z}$) not necessarily different. So we have $\alpha \mid p_1...p_k$ and α is a prime (in $\mathbb{Z}[\zeta]$) then $\alpha \mid p_{i_0}$ (because $\alpha \mid p_1$ or $\alpha \mid p_2...p_k$, then use induction). Let q is p_{i_0}. Let m be a rational integers such that $\alpha \mid m$. We want to prove that $q \mid m$. We have $m = \alpha\beta$ where $\beta \in \mathbb{Z}[\zeta]$, then using the norm $N(m) = N(\alpha)N(\beta)$, but $q \mid N(\alpha)$ then $q \mid N(\alpha)N(\beta)$, so $q \mid N(m)$ but $N(m) = m^n$ where n is the degree of the field extension $\mathbb{Q}(\zeta)$. Then because q is prime we have $q \mid m$ or $q \mid m^{n-1}$, if we have the first case then it's done, if not we have $q \mid m^{n-1}$ and we continue until $q \mid m^2$ and then $q \mid m$. It follows that m is a multiple of q.

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 idea than the proof of Theorem 4.17. 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 prove (c), hence the ring of integers of $\mathbb{Q}(\zeta)$ is Euclidean with the norm as Euclidean function.

Exercise 4.15.
Prove that the ring of integers of $K=\mathbb{Q}(\sqrt{2},i)$ is Euclidean.

Solution. We will use the same ideas than Theorem 4.17 and the solution of Exercise 4.14, hence we just have to prove (c): For any $\alpha\in\mathbb{Q}(\sqrt{2},i)$ there exists $\kappa\in\mathfrak{O}_K$ such that $|N(\alpha-\kappa)|<1$. An integral basis of K is $B=\{1,i,\sqrt{2},\frac{\sqrt{2}+i\sqrt{2}}{2}\}$ (Exercise 2.8) then the basis $B'=\{1,\sqrt{2},\sqrt{2}\frac{1+i}{2},1+i\}$ is an integral basis (Exercise 2.10). See $\mathbb{Q}(\sqrt{2},i)$ as $\mathbb{Q}(\sqrt{2})(\zeta)$ and $\mathfrak{O}_K=\mathbb{Z}[\sqrt{2}][\zeta]$ where $\zeta=\sqrt{2}\frac{1+i}{2}=e^{2\pi i/8}$. (We can write $B'=\{1,\sqrt{2},\zeta,\sqrt{2}\zeta\}$). For $\alpha=\alpha_1+\alpha_2\zeta$ and $\kappa=\kappa_1+\kappa_2\zeta$ where $\alpha_i\in\mathbb{Q}(\sqrt{2})$ and $\kappa_i\in\mathbb{Z}[\sqrt{2}]$, let $\sigma:=\alpha-\kappa$, $\sigma_1:=\alpha_1-\kappa_1$ and $\sigma_2:=\alpha_2-\kappa_2$. $N_{\mathbb{Q}(\sqrt{2})}(\alpha-\kappa)=N_{\mathbb{Q}(\sqrt{2})}(\sigma_1+\sigma_2\zeta)=(\sigma_1+\sigma_2\zeta)(\sigma_1+\sigma_2\overline{\zeta})=\sigma_1^2+\sigma_2^2+\sqrt{2}\sigma_1\sigma_2$.

Claim: For all $r\in\mathbb{R}$, for all $\epsilon>0$, there exists $s\in\mathbb{Z}[\sqrt{2}]$ such that $|r-s|<\epsilon$.

Proof of the claim: We do the same proof than in Exercise 4.14 while replacing $\sqrt{5}-2$ by $\sqrt{2}-1$ which is less than 1 and replacing $\mathbb{Z}[\sqrt{5}]$ by $\mathbb{Z}[\sqrt{2}]$.

We use the claim with $r=\alpha_i$ where $i=1$ and $i=2$ 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 $N(\alpha-\kappa)\leqslant\frac{1}{4}+\frac{1}{4}+\frac{\sqrt{2}}{4}<\frac{1+1+2}{4}=1$. We have prove (c), hence the ring of integers of $\mathbb{Q}(\sqrt{2},i)$ is Euclidean with the norm as Euclidean function.

Exercise 4.16.
Let $\mathbb{Q}_2$ be the set of all rational numbers a/b, where $a,b\in\mathbb{Z}$ and b is odd. Prove that $\mathbb{Q}_2$ is a domain, and that the only irreducibles in $\mathbb{Q}_2$ are 2 and its associates.

Solution. $\mathbb{Q}_2$ is a ring because $1\in\mathbb{Q}_2$ and for $\frac{a}{b},\frac{c}{d}\in\mathbb{Q}_2$, we have $\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}\in\mathbb{Q}_2$ (bd is odd because b and d are odd) and $\frac{a}{b}.\frac{c}{d}=\frac{ac}{bd}\in\mathbb{Q}_2$ (still because bd is odd). And there is no zero-divisors because if $\frac{ac}{bd}=0$, then $ac=0$ and $\mathbb{Z}$ is a domain so $a=0$ or $c=0$, then $\frac{a}{b}=0$ or $\frac{c}{d}=0$.

$\mathbb{Q}_2^*=\{\frac{p}{q}\in\mathbb{Q}_2$ with p odd$\}$ because we can consider $\frac{p}{q}\in\mathbb{Q}_2$ with $\mathrm{hcf}(p,q)=1$ (If $p/q\in\mathbb{Q}_2$ with $\mathrm{hcf}(p,q)=d$, q is odd so d is odd then $\frac{p}{q}=\frac{p/d}{q/d}$ with q/d is odd and $\mathrm{hcf}(p/d,q/d)=1$). $(\frac{p}{q})^{-1}=\frac{q}{p}$ which is in $\mathbb{Q}_2$ if and only if p is odd ($\mathrm{hcf}(p,q)=1$).

Let $\frac{p}{q}\in\mathbb{Q}_2\backslash\mathbb{Q}_2^*$ with p even, q odd and $\mathrm{hcf}(p,q)=1$. If $p=2k$ with k even, then $\frac{p}{q}=2.\frac{k}{q}$, but 2 and $\frac{k}{q}$ are not in $\mathbb{Q}_2^*$, hence $\frac{p}{q}$ is reducible. If $p=2k$ with

k odd, then $\frac{p}{q} = 2.\frac{k}{q}$, so $\frac{p}{q}$ is an associate of 2 because $\frac{k}{q} \in \mathbb{Q}_2^*$. Last point we have to prove is that 2 is irreducible. $2 = \frac{a}{b}.\frac{c}{d} = \frac{ac}{bd}$. Then $2bd = ac$ with bd odd, so $2 \mid ac$ but $4 \nmid ac$. Hence $2 \mid a$ or $2 \mid c$ but not both. Suppose $2 \mid a$ with no loss of generality, then $\frac{c}{d} \in \mathbb{Q}_2^*$. So 2 is an irreducible.

Exercise 4.17.
Generalize 4.16 to the ring $\mathbb{Q}_\pi$, where π is a finite set of ordinary primes, this being defined as the set of all rationals a/b with b prime to the elements of π.

Solution. $\mathbb{Q}_\pi$ is a ring because $1 \in \mathbb{Q}_\pi$ and for $\frac{p_1...p_n}{q_1...q_k}, \frac{r_1....r_m}{s_1...s_l} \in \mathbb{Q}_\pi$ where $p_i, q_i, r_i, s_i \notin \pi$ and are prime, we have $\frac{p_1...p_n}{q_1...q_k} + \frac{r_1....r_m}{s_1...s_l} = \frac{\alpha}{q_1...q_k s_1...s_l} \in \mathbb{Q}_\pi$ ($\alpha \in \mathbb{Z}$) because π is a set of prime and $\frac{p_1...p_n}{q_1...q_k}.\frac{r_1....r_m}{s_1...s_l} = \frac{\alpha'}{q_1...q_k s_1...s_l} \in \mathbb{Q}_2$ ($\alpha' \in \mathbb{Z}$). Moreover there is no zero-divisors because if $\frac{ac}{bd} = 0$, then $ac = 0$ and $\mathbb{Z}$ is a domain so $a = 0$ or $c = 0$, then $\frac{a}{b} = 0$ or $\frac{c}{d} = 0$.

$\mathbb{Q}_\pi^* = \left\{ \frac{p_1...p_n}{q_1...q_k} \text{ where } p_i, q_i \notin \pi \text{ and } \{p_1, ...p_n\} \cap \{q_1, ...q_k\} = \varnothing \right\}$ because $\frac{p_1...p_n}{q_1...q_k}, \frac{q_1...q_k}{p_1...p_n}$ have to be in $\mathbb{Q}_\pi$ and we can choose a numerator and denominator that are coprime.

Let $\frac{a}{b} \in \mathbb{Q}_\pi \backslash \mathbb{Q}_\pi^*$, $\frac{a}{b} = \frac{\alpha_1...\alpha_j p_1...p_n}{q_1...q_k}$ where $p_i, q_i \notin \pi$, $\alpha_i \in \pi$ and $j > 0$. If $j > 1$ then $\frac{a}{b} = \alpha_1.\frac{\alpha_2...\alpha_j p_1...p_n}{q_1...q_k}$ but $\alpha_1 \notin \mathbb{Q}_\pi^*$ and $\frac{\alpha_2...\alpha_j p_1...p_n}{q_1...q_k} \notin \mathbb{Q}_\pi^*$, so $\frac{a}{b}$ is reducible. If $j = 1$ then $\frac{a}{b} = \alpha_1.\frac{p_1...p_n}{q_1...q_k}$ and $\frac{p_1...p_n}{q_1...q_k}$ is in $\mathbb{Q}_\pi^*$, so $\frac{a}{b}$ is an associate of $\alpha_1 \in \pi$.

Last point we have to prove is all the elements of π are irreducible. Let p be in π. $p = \frac{p_1...p_n}{q_1...q_k}.\frac{r_1...r_m}{s_1...s_l} \in \mathbb{Q}_\pi$, hence $pq_1...q_k s_1...s_l = p_1...p_n r_1...r_m$. $p \mid pq_1...q_k s_1...s_l$, hence $p \mid p_1...p_n r_1...r_m$ but $p^2 \nmid pq_1...q_k s_1...s_l$, so $p^2 \nmid p_1...p_n r_1...r_m$. With no loss of generality, $p \mid p_1...p_n$ then $p \nmid r_1...r_m$ and for all other element q of π, $q \nmid pq_1...q_k s_1...s_l$ (because $p \neq q$ and $\frac{p_1...p_n r_1...r_m}{q_1...q_k s_1...s_l} \in \mathbb{Q}_\pi$), then $q \nmid p_1...p_n r_1...r_m$, hence $q \nmid r_1...r_m$. It follows that $\frac{r_1...r_m}{s_1...s_l}$ is in $\mathbb{Q}_\pi^*$. And then, p is irreducible.

Exercise 4.18.
The following purports to be a proof that in any number field K the ring of integers contains infinitely many irreducibles. Find the error.
'Assume $\mathfrak{O}$ has only finitely many irreducibles $p_1, ..., p_n$. The number $1 + p_1 p_2 ... p_n$ must be divisible by some irreducible q, and this cannot be any of $p_1, ..., p_n$. This is a contradiction. Of course the argument breaks down unless we can find at least one irreducible in $\mathfrak{O}$; but since not every element of $\mathfrak{O}$ is a

unit this is easy: let x be any non-unit and let p be some irreducible factor of x.'
Hint: The 'Proof' does not use any properties of $\mathfrak{O}$ beyond the existence of irreducible factorization and the fact that not every element is a unit. Now $\mathbb{Q}_2$ has these properties...

Solution. If we take $\mathbb{Q}_2$ which have only one irreducible 2, then $1+2=3$, but 3 is a unit in $\mathbb{Q}_2$, so there is no irreducible q which divides 3 and is not associates to 3. (A unit can't be irreducible by definition of irreducible)

Exercise 4.19.
Give a correct proof of the statement in Exercise 4.18.

Solution. Since Exercise 4.18, the only problem is that $\alpha = 1 + p_1...p_n$ can be a unit. Let find another α which is irreducible, hence not a unit, and different of all p_i.

Let take $x = p_1...p_n$, $x \in \mathfrak{O}_K$, hence its minimum polynomial $P_x = X^n + a_{n-1}X^{n-1} + ... + a_1X + a_0$ have its coefficients in $\mathbb{Z}$ (Lemma 2.12). We assume $a_0 \neq 0$ because if not $P_x = X^n + a_{n-1}X^{n-1} + ... + a_1X = X(X^{n-1} + a_{n-1}X^{n-2} + ... + a_1)$ but $x \neq 0$ then $x^{n-1} + a_{n-1}x^{n-2} + ... + a_1 = 0$ which is impossible because P_x is the minimum polynomial. It follows that $0 \neq -a_0 = x^n + a_{n-1}x^{n-1} + ... + a_1x = x(x^{n-1} + a_{n-1}x^{n-2} + ... + a_1)$. Let $y = x^{n-1} + a_{n-1}x^{n-2} + ... + a_1$. Then $x.y = -a_0 \in \mathbb{Z}\backslash\{0\}$. Assume that $xy > 0$ (Take $-x.y$ if not). Now take $\alpha = 1 + xy \in \mathbb{Z}$, $N(\alpha) = N(1+xy) = (1+xy)^N > 1$ where N is the degree of K, because $1 + xy \in \mathbb{Z} \subset \mathbb{Q}$ (Exercise 2.11). So $N(\alpha) > 1$, then α can't be a unit (Proposition 4.9 (a)). And we finish the proof as the statement in the Exercise 4.18.

4.5 Ideals p.128

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: $\alpha\beta \subset \langle p \rangle$ implies $\alpha \subset \langle p \rangle$ or $\beta \subset \langle p \rangle$. 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 $\alpha\beta \subset \{0\}$, then $\alpha = \{0\}$ or $\beta = \{0\}$ (because if $a \in \alpha\backslash\{0\}$ and $b \in \beta\backslash\{0\}$, then $ab \in \alpha\beta \subset \{0\}$, so $ab = 0$ but it's impossible because D is a domain, $a \neq 0$ and $b \neq 0$), hence $\alpha \subset \{0\}$ or $\beta \subset \{0\}$. It follows that $\langle p \rangle$ is prime.

Suppose p is a prime and $\alpha\beta \subset \langle p \rangle$. If $\alpha \not\subset \langle p \rangle$, then it exists a in $\alpha\backslash\langle p \rangle$. For all b in β, $ab \in \alpha\beta \subset \langle p \rangle$, 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 $\beta \subset \langle p \rangle$ 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 $p \mid b$.

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 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 5.2).

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 do 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 do 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 $\mathfrak{pr} = \langle 1-\sqrt{-5}\rangle$. $\mathfrak{pr} = \langle 6, 3(1+\sqrt{-5}), 2(1-\sqrt{-5}), (1+\sqrt{-5})(1-\sqrt{-5})\rangle = \langle (1+\sqrt{-5})(1-\sqrt{-5}), (-2+\sqrt{-5})(1-\sqrt{-5}), 2(1-\sqrt{-5})\rangle$ then we see that $\mathfrak{pr} \subset \langle 1-\sqrt{-5}\rangle$. For the other inclusion, we do assume that $1-\sqrt{-5}$ is in $\mathfrak{pr}$ (Indeed $1-\sqrt{-5} = (1+\sqrt{-5})(1-\sqrt{-5}) - (-2+\sqrt{-5})(1-\sqrt{-5}) - 2(1-\sqrt{-5})$), it follows that $\langle 1-\sqrt{-5}\rangle \subset \mathfrak{pr}$, hence $\langle 1-\sqrt{-5}\rangle = \mathfrak{pr}$.

Then we have $\langle 6\rangle = \mathfrak{p^2 qr}$ and if we consider $\langle 6\rangle = \mathfrak{p^2}.\mathfrak{qr} = \langle 2\rangle\langle 3\rangle$, we find $6 = 2.3$, and if we consider $\langle 6\rangle = \mathfrak{pq}.\mathfrak{pr} = \langle 1+\sqrt{-5}\rangle\langle 1-\sqrt{-5}\rangle$, we find $6 = (1+\sqrt{-5})(1-\sqrt{-5})$. So we understand the factorizations of 6 in the proof of Theorem 4.10.

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 Theorem 4, $\mathbb{Z}[\sqrt{-5}]/\langle 1+\sqrt{-5}\rangle = (\mathbb{Z}[X]/\langle X^2+5\rangle)/\langle\overline{1+\sqrt{-5}}\rangle = (\mathbb{Z}[X]/\langle X^2+5\rangle)/\langle 1+X\rangle = \mathbb{Z}[X]/\langle X^2+5, 1+X\rangle = (\mathbb{Z}[X]/\langle 1+X\rangle)/\langle\overline{X^2+5}\rangle = \mathbb{Z}/\langle 6\rangle = \mathbb{Z}/6\mathbb{Z}$ 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's 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 (Theorem 3). $\varphi_{X\to\sqrt{-5}}(X^2+5) = \sqrt{-5}^2 + 5 = 0$, 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 Theorem 3, $\mathbb{Z}[X]/\ \mathrm{Ker}(\varphi_{X\to\sqrt{-5}}) \simeq \mathbb{Z}[\sqrt{-5}]$. 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's surjective, and we want to prove that $\mathrm{Ker}(\varphi_{X\to -1}) = \langle X+1\rangle$, to use the first isomorphism theorem (Theorem 3). $\varphi_{X\to -1}(X+1) = -1+1 = 0$, 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 Theorem 3, $\mathbb{Z}[X]/\ \mathrm{Ker}(\varphi_{X\to -1}) \simeq \mathbb{Z}$. 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 $N(\mathfrak{r}) = |\mathbb{Z}[\sqrt{-5}]/\mathfrak{r}| = |\mathbb{Z}[\sqrt{-5}]/\langle 3, 1-\sqrt{-5}\rangle| = |(\mathbb{Z}/\langle 3, 6\rangle| = |\mathbb{Z}/3\mathbb{Z}| = 3$. (It's 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), $N(\mathfrak{qr}) = N(\langle 3\rangle) = N(3) = 9 = N(\mathfrak{q}).N(\mathfrak{r})$. $N(\mathfrak{pq}) = N(\langle 1+\sqrt{-5}\rangle) = N(1+\sqrt{-5}) =$

$1+5=6=N(\mathfrak{p}).N(\mathfrak{q})$, $N(\mathfrak{pr})=N(\langle 1-\sqrt{-5}\rangle)=N(1-\sqrt{-5})=1+5=6=N(\mathfrak{p}).N(\mathfrak{r})$, $N(\langle 6\rangle)=N(6)=6^2=36=2^2.3.3=N(\mathfrak{p}).N(\mathfrak{p}).N(\mathfrak{q}).N(\mathfrak{r})$.

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 5.9). But we see that $N(\mathfrak{p})=2$ in the Exercise 5.3 and $a^2+5b^2=2$ have no solution, since it implies $b=0$ and $a^2=2$ have no solution in $\mathbb{Z}$. For $\mathfrak{q}$ and $\mathfrak{r}$, use the same argue, because $a^2+5b^2=3$ have no solution, either.

Exercise 5.5.
Show the principal ideals $\langle 2\rangle$, $\langle 3\rangle$ in Exercise 5.2 are generated by irreducible elements but the ideals are not prime.

Solution. 2 and 3 are irreducible, just use the Exercise 3.10 to see that they don't have proper factor. 2 and 3 are not prime because in $\mathbb{Z}[\sqrt{-5}]$, $6=2.3=(1+\sqrt{-5})(1-\sqrt{-5})$ then 2 divides $(1+\sqrt{-5})(1-\sqrt{-5})$ but 2 doesn't divide neither $(1+\sqrt{-5})$ nor $(1-\sqrt{-5})$ (Exericse 3.10). Same thing for 3. Then use Exercise 5.1 (because $\mathbb{Z}[\sqrt{-5}]$ is an integral domain) to see that since 2 and 3 are not prime then $\langle 2\rangle$ and $\langle 3\rangle$ are not prime either.

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 idea 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 5.2).

We can do the same job 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 $\mathfrak{p_1^2 p_2^2} \subset \langle 6\rangle$. Conversely, $54 = -3.3.\sqrt{-6}.\sqrt{-6} \in \mathfrak{p_1^2 p_2^2}$ and $24 = -2.2.\sqrt{-6}\sqrt{-6} \in \mathfrak{p_1^2 p_2^2}$, then $54 - 2 \times 24 = 6 \in \mathfrak{p_1^2 p_2^2}$, it follows that $\langle 6\rangle \subset \mathfrak{p_1^2 p_2^2}$ and now $\langle 6\rangle = \mathfrak{p_1^2 p_2^2}$.

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 3.2) $14 = \sqrt{2}.\sqrt{2}.(\sqrt{2} + \sqrt{-5}).(\sqrt{2} - \sqrt{-5})$ is a factorization in $\mathbb{Z}[\sqrt{-5}, \sqrt{2}]$. Then we define $\mathfrak{p_1} = \mathfrak{I_1} \cap \mathbb{Z}[\sqrt{-10}] = \langle 2, \sqrt{-10}\rangle$ where $\mathfrak{I_1}$ is the principal ideal in $\mathbb{Z}[\sqrt{-5}, \sqrt{2}]$ generated by $\sqrt{2}$, $\mathfrak{p_2} = \mathfrak{I_2} \cap \mathbb{Z}[\sqrt{-10}] = \langle 2 + \sqrt{-10}, -5 + \sqrt{-10}\rangle$ where $\mathfrak{I_2}$ is the principal ideal in $\mathbb{Z}[\sqrt{-5}, \sqrt{2}]$ generated by $\sqrt{2} + \sqrt{-5}$ and $\mathfrak{p_3} = \mathfrak{I_3} \cap \mathbb{Z}[\sqrt{-10}] = \langle 2 - \sqrt{-10}, 5 + \sqrt{-10}\rangle$ where $\mathfrak{I_3}$ is the principal ideal in $\mathbb{Z}[\sqrt{-5}, \sqrt{2}]$ generated by $\sqrt{2} - \sqrt{-5}$. We assume that $\langle 14\rangle = \mathfrak{p_1^2 p_2 p_3}$.

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 $\langle 2 + \sqrt{-10}, -5 + \sqrt{-10}\rangle \subset \mathfrak{I_2} \cap \mathbb{Z}[\sqrt{-10}]$. 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 $\mathfrak{I_2} \cap \mathbb{Z}[\sqrt{-10}] \subset \langle 2 + \sqrt{-10}, -5 + \sqrt{-10}\rangle$. And we have the equality.

To prove that $\mathfrak{p_2}$ is prime, we use Theorem 5.11. 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 $\mathfrak{p_3}$, it's the same ideas.

Now we have to prove that $\langle 14\rangle = \mathfrak{p_1^2 p_2 p_3}$ since they are all primes. $\mathfrak{p_1^2} = \langle 4, -10, 2\sqrt{-10}\rangle$, $\mathfrak{p_2 p_3} = \langle 14, -35, 7\sqrt{-10}\rangle$ then $\mathfrak{p_1^2 p_2 p_3} = \langle 56, 140, 350, 28\sqrt{-10}, 70\sqrt{-10}\rangle$. But $14 = 350 - 2 \times 140 - 56$, it follows that $14 \in \mathfrak{p_1^2 p_2 p_3}$. 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 $N(\mathfrak{p_1^2 p_2 p_3}) = N(\mathfrak{p_1})^2 N(\mathfrak{p_2}) N(\mathfrak{p_3}) = 2^2.7.7 = 14^2$ (Theorem 5.10). And $N(\langle 14\rangle) = |N(14)| = 14^2$ (Corollary 5.9). It follows that $\langle 14\rangle = \mathfrak{p_1^2 p_2 p_3}$ because they have the same norm and we have an inclusion.

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

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 5.3, $\mathfrak{p}$ 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, $\mathfrak{p}+\mathfrak{q}=\mathfrak{O}$.

$\mathfrak{p}\mathfrak{q}\subset\mathfrak{p}\cap\mathfrak{q}$ because by definition of an ideal, for all $\alpha\in\mathfrak{p}\mathfrak{q}$, α is in $\mathfrak{p}$ and α is in $\mathfrak{q}$, then α is in $\mathfrak{p}\cap\mathfrak{q}$. We use the Chinese Remainder Theorem (Theorem 5) because $\mathfrak{p}+\mathfrak{q}=\mathfrak{O}$ then $\mathfrak{O}/\mathfrak{p}\cap\mathfrak{q}\simeq\mathfrak{O}/\mathfrak{p}\times\mathfrak{O}/\mathfrak{q}$. It follows that $N(\mathfrak{p}\cap\mathfrak{q})=|\mathfrak{O}/\mathfrak{p}\cap\mathfrak{q}|=|\mathfrak{O}/\mathfrak{p}\times\mathfrak{O}/\mathfrak{q}|=|\mathfrak{O}/\mathfrak{p}|.|\mathfrak{O}/\mathfrak{q}|=N(\mathfrak{p})N(\mathfrak{q})=N(\mathfrak{p}\mathfrak{q})$. Since we have the equality of the norm and an inclusion, we have $\mathfrak{p}\mathfrak{q}=\mathfrak{p}\cap\mathfrak{q}$.

Alternative proof for $\mathfrak{p}\mathfrak{q}=\mathfrak{p}\cap\mathfrak{q}$: we can use the Proposition 3.1.

Exercise 5.9.
If $\mathfrak{O}$ is a principal ideal domain, prove that every fractional ideal is of the form $\{\alpha\phi|\alpha\in\mathfrak{O}\}$ for some $\phi\in K$. Does the converse hold ?

Solution. By definition of a principal ideal domain, every ideal of $\mathfrak{O}$ can be write $\{a\alpha\mid\alpha\in\mathfrak{O}\}$ where $a\in\mathfrak{O}$. By definition of fractional ideal (end of page 111), fractional ideal can be write as $c^{-1}\mathfrak{a}$ where $\mathfrak{a}$ is an ideal of the ring of integers we study and c a non-zero element of the ring of integers, then every fractional ideal of $\mathfrak{O}$ can be written $\{c^{-1}a\alpha\mid\alpha\in\mathfrak{O}\}$ and $c^{-1}\alpha\in K$ because K is a number **field**. So $\phi=c^{-1}a$ here. Conversely we use Lemma 2.10, if $\phi\in K$, there exists $c\in\mathbb{Z}\backslash\{0\}$ such that $c\phi\in\mathfrak{O}$. Then $\{c\phi\alpha\mid\alpha\in\mathfrak{O}\}$ is an ideal of $\mathfrak{O}$, it follows that $\{c^{-1}c\phi\alpha\mid\alpha\in\mathfrak{O}\}=\{\phi\alpha\mid\alpha\in\mathfrak{O}\}$ is a fractional ideal of $\mathfrak{O}$ since c is a non zero element of $\mathfrak{O}$ (we remind that $\mathbb{Z}\subset\mathfrak{O}$ because of Lemma 2.13.).

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 4.17) then they are principal ideal domain (Theorem 4.14). 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 ideal (end of page 111), fractional ideal can be write as $c^{-1}\mathfrak{a}$ where $\mathfrak{a}$ is an ideal of the ring of integers we study 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 $b\neq0$ (equivalent to $r\mathbb{Z}$ where $r\in\mathbb{Q}$ (Example page 112)). 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 $\beta\neq0$.

Exercise 5.11.
In $\mathbb{Z}[\sqrt{-5}]$, find a $\mathbb{Z}-$basis $\{\alpha_1, \alpha_2\}$ for the ideal $\langle 2, 1+\sqrt{-5}\rangle$. Check the formula

$$N(\langle 2, 1+\sqrt{-5}\rangle) = \left|\frac{\Delta[\alpha_1, \alpha_2]}{d}\right|^{1/2}$$

of Theorem 5.8.

Solution. If $\alpha \in \langle 2, 1+\sqrt{-5}\rangle$, we can write $\alpha = 2(a+b\sqrt{-5}) + (1+\sqrt{-5})(c+d\sqrt{-5}) = (2a+c-5d)+(2b+c+d)\sqrt{-5}$. Then $\{2, 2\sqrt{-5}, 1+\sqrt{-5}, -5+\sqrt{-5}\}$ generates $\langle 2, 1+\sqrt{-5}\rangle$ and we can reduce that in $B = \{2, 1+\sqrt{-5}\}$ because $-5+\sqrt{-5} = 1+\sqrt{-5}-2\times 3$ and $2\sqrt{-5} = 2(1+\sqrt{-5})-2$. Then B is a $\mathbb{Z}-$basis of $\langle 2, 1+\sqrt{-5}\rangle$. We know that $N(\langle 2, 1+\sqrt{-5}\rangle) = 2$ (Exercise 5.3). Calculate $\Delta[2, 1+\sqrt{-5}] = \begin{vmatrix} 2 & 1+\sqrt{-5} \\ 2 & 1-\sqrt{-5} \end{vmatrix}^2 = (2(1-\sqrt{-5}) - 2(1+\sqrt{-5}))^2 = (-4\sqrt{-5})^2 = -80$. Use Theorem 3.3 and the fact that $-5 \not\equiv 1$ [4] then $d = 4\times -5$. It follows that $\left|\frac{\Delta[\alpha_1, \alpha_2]}{d}\right|^{1/2} = \left|\frac{-80}{-20}\right|^{1/2} = 4^{1/2} = 2$. Then we check the formula of Theorem 5.8 in this particular case.

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

Solution. We will use Theorem 4, 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 $\mathbb{Z}[\sqrt{-5}]/\langle 6\rangle \simeq (\mathbb{Z}[X]/\langle X^2+5\rangle)/\overline{\langle 6\rangle} \simeq (\mathbb{Z}/6\mathbb{Z})[X]/\langle X^2+5\rangle \simeq (\mathbb{Z}/2\mathbb{Z})[X]/\overline{\langle X^2+5\rangle} \times (\mathbb{Z}/3\mathbb{Z})[X]/\overline{\langle X^2+5\rangle}$, by Chinese Remainder Theorem (Theorem 5) and the same idea of Exercise 5.3.

Study $(\mathbb{Z}/2\mathbb{Z})[X]/\overline{\langle X^2+5\rangle}$. $(\mathbb{Z}/2\mathbb{Z})[X]/\overline{\langle X^2+5\rangle} \simeq (\mathbb{Z}/2\mathbb{Z})[X]/\langle X^2+1\rangle \simeq (\mathbb{Z}/2\mathbb{Z})[X]/\langle (X+1)^2\rangle \simeq (\mathbb{Z}/2\mathbb{Z})[Y]/\langle Y^2\rangle$ 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 $(\mathbb{Z}/3\mathbb{Z})[X]/\overline{\langle X^2+5\rangle}$. $(\mathbb{Z}/3\mathbb{Z})[X]/\langle X^2+2\rangle \simeq (\mathbb{Z}/3\mathbb{Z})[X]/\langle (X+1)(X+2)\rangle$ and while using Chinese Remainder Theorem (Theorem 5) (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 $\mathfrak{p} = \langle 2, 1+\sqrt{-5}\rangle$, $\mathfrak{q} = \langle 3, 1+\sqrt{-5}\rangle$, $\mathfrak{r} = \langle 3, 1-\sqrt{-5}\rangle$.

Exercise 5.13.
Find all the ideals in $\mathbb{Z}[\sqrt{2}]$ with norm 18.

Solution. Use Theorem 3.3 to see that $\mathbb{Z}[\sqrt{2}]$ is the ring of integers of $\mathbb{Q}[\sqrt{2}]$ and Theorem 4.20 to see that $\mathbb{Z}[\sqrt{2}]$ is norm-Euclidean. Then by Theorem 4.14, $\mathbb{Z}[\sqrt{2}]$ is principal, so all ideals of $\mathbb{Z}[\sqrt{2}]$ can we written $\langle\alpha\rangle$ with $\alpha \in \mathbb{Z}[\sqrt{2}]$. Use Corollary 5.9, and for all ideals $\langle u+v\sqrt{2}\rangle$ of $\mathbb{Z}[\sqrt{2}]$ where $u, v \in \mathbb{Z}$, $N(\langle u+v\sqrt{2}\rangle) = |N(u+v\sqrt{2})| = |u^2-2v^2|$. We looking for the ideals of norm 18, hence we want the solutions of $u^2-2v^2 = \pm 18$.

Use the reference [6] to solve $a^2-2b^2 = 1$, the fundamental solution is $a = 3$ and $b = 2$. then let $z_0 = 3+2\sqrt{2}$, all the solutions (a_n, b_n) are such that $a_n+b_n\sqrt{2} = z_0^n$ (Theorem 2 of reference [6]). For $a^2-2b^2 = -1$, use Theorem 4 of reference [6], to see that all solutions are (a_n, b_n) such that $a_n+b_n\sqrt{2} = (1+\sqrt{2})^n$ where n is odd, and for n even we find the solution of $a^2-2b^2 = 1$, because $(1+\sqrt{2})^2 = 3+2\sqrt{2}$.

We have all the solutions of $a^2-2b^2 = \pm 1$, let find the solutions of $u^2-2v^2 = \pm 18$. Take a solution (a, b) of $a^2-2b^2 = \pm 1$, let $u = 6(a+b)$ and $v = 3(a+2b)$, then $u^2-2v^2 = 6^2(a+b)^2-2.3^2(a+2b)^2 = 36(a^2+2ab+b^2)-18(a^2+4ab+4b^2) = 18(a^2-2b^2) = \pm 18$. Conversely, let (u, v) be a solution of $u^2-2v^2 = \pm 18$. In $\mathbb{Z}/3\mathbb{Z}$, we have $u^2+v^2 \equiv 0$ [3], but $1^2 \equiv 1$ [3] and $2^2 \equiv 1$ [3] so the only possibility is to have $u = 3k$ and $v = 3q$. So we want to solve $(3k)^2-2.(3q)^2 = \pm 18$ which is equivalent to $k^2-2q^2 = \pm 2$. In $\mathbb{Z}/2\mathbb{Z}$ we have $k^2 \equiv 0$ [2], hence $k = 2p$. It follows that we want to solve $(2p)^2-2q^2 = \pm 2$ which is equivalent to $q^2-2p^2 = \pm 1$. We have all solutions of $a^2-2b^2 = \pm 1$, hence we have also all the solutions for $u^2-2v^2 = \pm 18$.

Then all ideals of norm 18 are $\langle u+v\sqrt{2}\rangle$ with (u, v) solution of $u^2-2v^2 = \pm 18$.

Exercise 5.14.
If K is a number field of degree n with integers $\mathfrak{O}$, show that if $m \in \mathbb{Z}$ and $\langle m\rangle$ is the ideal in $\mathfrak{O}$ generated by m, then $N(\langle m\rangle) = |m|^n$.

Solution. We use Exercise 2.11, since $m \in \mathbb{Z} \subset \mathbb{Q}$, $N(m) = m^n$. And the Corollary 5.9 gives us that $N(\langle m\rangle) = |N(m)| = |m|^n$.

Exercise 5.15.
(Version of the third edition because there were mistakes in the first edition)
In $\mathbb{Z}[\sqrt{-29}]$ we have $30 = 2.3.5 = (1+\sqrt{-29})(1-\sqrt{-29})$. Show $\langle 30\rangle \subseteq \langle 2, 1+\sqrt{-29}\rangle$ and verify $\mathfrak{p}_1 = \langle 2, 1+\sqrt{-29}\rangle$ has norm 2 and is thus prime. Check that $1-\sqrt{-29} \in \mathfrak{p}_1$ and deduce $\langle 30\rangle \subseteq \mathfrak{p}_1^2$. Find prime ideals $\mathfrak{p}_2$, $\mathfrak{p}'_2$, $\mathfrak{p}_3$, $\mathfrak{p}'_3$ with norms 3 or 5 such that $\langle 30\rangle \subseteq \mathfrak{p}_i\mathfrak{p}'_i$ for $i = 2,\ 3$. Deduce that $\mathfrak{p}_1^2\mathfrak{p}_2\mathfrak{p}'_2\mathfrak{p}_3\mathfrak{p}'_3 \mid \langle 30\rangle$ and by calculating norms, or otherwise, show $\langle 30\rangle = \mathfrak{p}_1^2\mathfrak{p}_2\mathfrak{p}'_2\mathfrak{p}_3\mathfrak{p}'_3$. Comment on how this relates to the two factorizations: $\langle 30\rangle = \langle 2\rangle\langle 3\rangle\langle 5\rangle$ and $\langle 30\rangle = \langle 1+\sqrt{-29}\rangle\langle 1-\sqrt{-29}\rangle$

Solution. $30 = (1+\sqrt{-29})(1-\sqrt{-29})$, hence $30 \in \langle 2, 1+\sqrt{-29}\rangle$ and then $\langle 30\rangle \subseteq \langle 2, 1+\sqrt{-29}\rangle$.We use the same ideas than Exercise 5.3, $N(\mathfrak{p}_1) = |\mathbb{Z}[\sqrt{-29}]/\langle 2, 1+\sqrt{-29}\rangle| = |((\mathbb{Z}[X]/\langle X^2+29\rangle)/\langle 1+X\rangle)/\langle 2\rangle| = |((\mathbb{Z}[X]/\langle 1+$

$X\rangle)/\langle(-1)^2+29\rangle)/\langle 2\rangle| = |(\mathbb{Z}/\langle 30\rangle)/\langle 2\rangle| = |\mathbb{Z}/\langle 2,30\rangle| = |\mathbb{Z}/\langle 2\rangle| = 2$. Then by Theorem 5.11, we have $\mathfrak{p_1}$ prime because 2 is prime in $\mathbb{Z}$.

We have $1-\sqrt{-29} = 2-(1+\sqrt{-29}) \in \mathfrak{p_1}$, hence $30 = (1+\sqrt{-29})(1-\sqrt{-29}) \in \mathfrak{p_1^2}$ and then $\langle 30\rangle \subseteq \mathfrak{p_1^2}$.

Let $\mathfrak{p_2} = \langle 3, 1+\sqrt{-29}\rangle$, $\mathfrak{p_2'} = \langle 3, 1-\sqrt{-29}\rangle$, $\mathfrak{p_3} = \langle 5, 1+\sqrt{-29}\rangle$ and $\mathfrak{p_3'} = \langle 5, 1-\sqrt{-29}\rangle$. It follows that $30 = (1+\sqrt{-29})(1-\sqrt{-29}) \in \mathfrak{p_2}\mathfrak{p_2'}$ and $30 = (1+\sqrt{-29})(1-\sqrt{-29}) \in \mathfrak{p_3}\mathfrak{p_3'}$ so we have $\langle 30\rangle \subseteq \mathfrak{p_2}\mathfrak{p_2'}$ and $\langle 30\rangle \subseteq \mathfrak{p_3}\mathfrak{p_3'}$. And as we already saw several times $N(\mathfrak{p_2}) = |\mathbb{Z}/\langle 30\rangle/\langle 3\rangle| = |\mathbb{Z}/\langle 3\rangle| = 3$, $N(\mathfrak{p_2'}) = |\mathbb{Z}/\langle 30\rangle/\langle 3\rangle| = |\mathbb{Z}/\langle 3\rangle| = 3$, $N(\mathfrak{p_3}) = |\mathbb{Z}/\langle 30\rangle/\langle 5\rangle| = |\mathbb{Z}/\langle 5\rangle| = 5$ and $N(\mathfrak{p_3'}) = |\mathbb{Z}/\langle 30\rangle/\langle 5\rangle| = |\mathbb{Z}/\langle 5\rangle| = 5$.

$\mathfrak{p_1^2} = \langle 4, 2+2\sqrt{-29}, -28+2\sqrt{-29}\rangle$, hence $2 = -28+2\sqrt{-29} - (2+\sqrt{-29}) + 4\times 8 \in \mathfrak{p_1^2}$. Then $\mathfrak{p_2}\mathfrak{p_2'} = \langle 9, 3+3\sqrt{-29}, 3-3\sqrt{-29}, 30\rangle$, hence $3 = 30 - 9\times 3 \in \mathfrak{p_2}\mathfrak{p_2'}$. And $\mathfrak{p_3}\mathfrak{p_3'} = \langle 25, 5+5\sqrt{-29}, 5-5\sqrt{-29}, 30\rangle$, hence $5 = 30 - 25 \in \mathfrak{p_2}\mathfrak{p_2'}$. It follows that $30 = 2.3.5 \in \mathfrak{p_1^2}\mathfrak{p_2}\mathfrak{p_2'}\mathfrak{p_3}\mathfrak{p_3'}$. Then $\langle 30\rangle \subseteq \mathfrak{p_1^2}\mathfrak{p_2}\mathfrak{p_2'}\mathfrak{p_3}\mathfrak{p_3'}$. Moreover $N(\langle 30\rangle) = N(30) = 30^2$ (Corollary 5.9) and $N(\mathfrak{p_1^2}\mathfrak{p_2}\mathfrak{p_2'}\mathfrak{p_3}\mathfrak{p_3'}) = N(\mathfrak{p_1})^2 N(\mathfrak{p_2}) N(\mathfrak{p_2'}) N(\mathfrak{p_3}) N(\mathfrak{p_3'}) = 2^2.3^2.5^2 = 30^2$. So we have $\langle 30\rangle = \mathfrak{p_1^2}\mathfrak{p_2}\mathfrak{p_2'}\mathfrak{p_3}\mathfrak{p_3'}$

We have $\langle 30\rangle = \langle 2\rangle\langle 3\rangle\langle 5\rangle$ because $\langle 2\rangle \subseteq \mathfrak{p_1^2}$ (already saw above) and $N(\langle 2\rangle) = N(2) = 4 = 2^2 = N(\mathfrak{p_1^2})$, $\langle 3\rangle \subseteq \mathfrak{p_2}\mathfrak{p_2'}$ (already saw above) and $N(\langle 3\rangle) = N(3) = 9 = 3^2 = N(\mathfrak{p_2}\mathfrak{p_2'})$ and $\langle 5\rangle \subseteq \mathfrak{p_3}\mathfrak{p_3'}$ (already saw above) and $N(\langle 5\rangle) = N(5) = 25 = 5^2 = N(\mathfrak{p_3}\mathfrak{p_3'})$

We have $\langle 30\rangle = \langle 1+\sqrt{-29}\rangle\langle 1-\sqrt{-29}\rangle$ because $\langle 1+\sqrt{-29}\rangle = \mathfrak{p_1}\mathfrak{p_2}\mathfrak{p_3}$ and $\langle 1+\sqrt{-29}\rangle = \mathfrak{p_1}\mathfrak{p_2'}\mathfrak{p_3'}$, we use a norm argument and an inclusion as above. (Or we can do a similar proof of $\mathfrak{pq} = \langle 1+\sqrt{-5}\rangle$ of Exercise 5.2)

Exercise 5.16.
Find all ideals in $\mathbb{Z}[\sqrt{-29}]$ containing the element 30.

Solution. We will use Theorem 4, there is a bijection between ideals of $\mathbb{Z}[\sqrt{-29}]$ that contain 30 and the ideals of $\mathbb{Z}[\sqrt{-29}]/\langle 30\rangle$. Look at $\mathbb{Z}[\sqrt{-29}]/\langle 30\rangle \simeq (\mathbb{Z}[X]/\langle X^2+29\rangle)/\langle\overline{30}\rangle \simeq (\mathbb{Z}/30\mathbb{Z})[X]/\langle X^2+29\rangle \simeq (\mathbb{Z}/2\mathbb{Z})[X]/\langle\overline{X^2+29}\rangle \times (\mathbb{Z}/3\mathbb{Z})[X]/\langle\overline{X^2+29}\rangle \times (\mathbb{Z}/5\mathbb{Z})[X]/\langle\overline{X^2+29}\rangle$, by Chinese Remainder Theorem (Theorem 5) and the same idea of Exercise 5.3.

Study $(\mathbb{Z}/2\mathbb{Z})[X]/\langle\overline{X^2+29}\rangle$. $(\mathbb{Z}/2\mathbb{Z})[X]/\langle\overline{X^2+29}\rangle \simeq (\mathbb{Z}/2\mathbb{Z})[X]/\langle X^2+1\rangle \simeq (\mathbb{Z}/2\mathbb{Z})[X]/\langle(X+1)^2\rangle \simeq (\mathbb{Z}/2\mathbb{Z})[Y]/\langle Y^2\rangle$ 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 $(\mathbb{Z}/3\mathbb{Z})[X]/\langle\overline{X^2+29}\rangle$. $(\mathbb{Z}/3\mathbb{Z})[X]/\langle X^2+2\rangle \simeq (\mathbb{Z}/3\mathbb{Z})[X]/\langle(X+1)(X+2)\rangle$ and while using Chinese Remainder Theorem (Theorem 5) (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 $\langle 1\rangle$.

Study $(\mathbb{Z}/5\mathbb{Z})[X]/\langle\overline{X^2+29}\rangle$. $(\mathbb{Z}/5\mathbb{Z})[X]/\langle X^2-1\rangle \simeq (\mathbb{Z}/5\mathbb{Z})[X]/\langle(X+1)(X-1)\rangle$ and while using Chinese Remainder Theorem (Theorem 5) (because $5-2((X+1)-(X-1)) = 1$, then $\langle X+1\rangle + \langle X-1\rangle = \langle 1\rangle$ in $\mathbb{Z}/5\mathbb{Z}[X]$), we

have $(\mathbb{Z}/5\mathbb{Z})[X]/\langle(X+1)(X-1)\rangle \simeq (\mathbb{Z}/5\mathbb{Z})[X]/\langle X+1\rangle \times (\mathbb{Z}/5\mathbb{Z})[X]/\langle X-1\rangle \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ but $\mathbb{Z}/5\mathbb{Z}$ is a field so the only ideals are $\langle 0\rangle$ and $\langle 1\rangle$.

Then there are 48 ideals of $\mathbb{Z}[\sqrt{-29}]$ which contain the element 30. ($48 = 3.2.2.2.2$). We find it while using the prime ideals $\mathfrak{p} = \langle 2, 1+\sqrt{-29}\rangle$, $\mathfrak{q} = \langle 3, 1+\sqrt{-29}\rangle$, $\mathfrak{r} = \langle 3, 1-\sqrt{-29}\rangle$, $\mathfrak{s} = \langle 5, 1+\sqrt{-29}\rangle$, $\mathfrak{t} = \langle 5, 1-\sqrt{-29}\rangle$. We have $\mathbb{Z}[\sqrt{-29}]$, $\mathfrak{p} = \langle 2, 1+\sqrt{-29}\rangle$, $\mathfrak{q} = \langle 3, 1+\sqrt{-29}\rangle$, $\mathfrak{r} = \langle 3, 1-\sqrt{-29}\rangle$, $\mathfrak{s} = \langle 5, 1+\sqrt{-29}\rangle$, $\mathfrak{t} = \langle 5, 1-\sqrt{-29}\rangle$, $\mathfrak{p}^2 = \langle 2\rangle$, $\mathfrak{pq}$, $\mathfrak{pr}$, $\mathfrak{ps}$, $\mathfrak{pt}$, $\mathfrak{qr} = \langle 3\rangle$, $\mathfrak{qs}$, $\mathfrak{qt}$, $\mathfrak{rs}$, $\mathfrak{rt}$, $\mathfrak{st} = \langle 5\rangle$, $\mathfrak{p}^2\mathfrak{q}$, $\mathfrak{p}^2\mathfrak{r}$, $\mathfrak{p}^2\mathfrak{s}$, $\mathfrak{p}^2\mathfrak{t}$, $\mathfrak{pqr}$, $\mathfrak{pqs} = \langle 1+\sqrt{-29}\rangle$, $\mathfrak{pqt}$, $\mathfrak{prs}$, $\mathfrak{prt} = \langle 1-\sqrt{-29}\rangle$, $\mathfrak{pst}$, $\mathfrak{qrs}$, $\mathfrak{qrt}$, $\mathfrak{qst}$, $\mathfrak{rst}$, $\mathfrak{p}^2\mathfrak{qr}$, $\mathfrak{p}^2\mathfrak{qs}$, $\mathfrak{p}^2\mathfrak{qt}$, $\mathfrak{p}^2\mathfrak{rs}$, $\mathfrak{p}^2\mathfrak{rt}$, $\mathfrak{p}^2\mathfrak{st}$, $\mathfrak{pqrs}$, $\mathfrak{pqrt}$, $\mathfrak{pqst}$, $\mathfrak{prst}$, $\mathfrak{qrst}$, $\mathfrak{p}^2\mathfrak{qrs}$, $\mathfrak{p}^2\mathfrak{qrt}$, $\mathfrak{p}^2\mathfrak{qst}$, $\mathfrak{p}^2\mathfrak{rst}$, $\mathfrak{pqrst}$, $\mathfrak{p}^2\mathfrak{qrst} = \langle 30\rangle$.

5 References

[1] I.STEWART and D.TALL, *Algebraic Number Theory*, First Edition, Ed. 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] P. LE BARBENCHON, *Introduction of Algebraic Number Theory*, 2018

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

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

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