Algebraic Number Theory

Jeroen Sijsling

20 December 2016

Contents

0.1 Introduction

These are the notes for the 2012-2013 course on algebraic number theory at the University of Warwick, which also form the basis of the 2016 course at the Universität Ulm. They contain the material treated in the lectures, along with some extra remarks, added to clarify the main ideas behind the course.

I have rearranged the order of the results from the original order in the course. The meat of the notes is in a theoretical section and a more practically oriented section with lots of applications and calculations. I find this a logical way to present the subjects covered. The only drawback is that there is a large theoretical section to plod through before arriving at the nice examples that are the real motivation and heart of the subject. But presumably, if you downloaded these notes at all after following the course itself, then you will have faith enough to bear with me through the first part, which not only contains notions and proof techniques that are useful throughout mathematics but which hopefully also holdss some interest itself.

After the main section, the notes follow up with a brief discussion of further subjects. The notes conclude by giving the exercises used during the course, along with their full solutions.

These notes have very little in the way of originality. They can be considered as a personal reordering and simplification of the results in Bosman and Bouyer [1], Stein [4], and Stevenhagen [5]. Theorems and proofs are often copied outright and only modify to make things just a little more transparent.

Your thoughts or comments are very welcome! Please send them to `jeroen.sijsling@uni-ulm.de`. I owe many thanks to Guy Barwell, Alex Best, Duc Khoi Do, Daniel Parsons, Katherine Sroga, and Muhammad Haikal Yeo for helping me to bring the notes to their current improved form. Any remaining errors are solely due to me.

What the course is about

You will likely have seen and worked with the field of rational numbers $\mathbb{Q}$ and everyone's favourite subring of $\mathbb{Q}$, namely the ring of integer numbers $\mathbb{Z}$. The subring $\mathbb{Z}$ of $\mathbb{Q}$ is rather special, because one can factor every number in it as a product of prime numbers, which is extremely useful for answering questions about integers.

The goal of this course is to consider in how far similar statements hold for number fields. Number fields are field extensions of $\mathbb{Q}$ whose degree as a vector space over $\mathbb{Q}$ is finite. One can for example think of $\mathbb{Q}(i)$, which consists of the complex numbers $a + bi$ with $a, b \in \mathbb{Q}$. Other number fields are $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}[x]/(f)$ for irreducible polynomial f over $\mathbb{Q}$, such as $f = x^3 + x - 1$.

One can define analogues of the usual integers for a number field K, which leads one the consider the ring of integers $\mathcal{O}_K$ of K. This is the "right" generalization of the ordinary ring of integers $\mathbb{Z}$, and one could hope that a similar unique factorization of integral elements into prime elements holds.

Alas, this is not always true. The aim of the course is to analyse in how far the unique factorization property fails for the integers of general number fields. It turns out that it does not fail by too much: the obstruction to unique factorization is measured by a finite abelian group called the class group of $\mathcal{O}_K$. Analyzing this failure is interesting for many reasons. The most important one is that it leads one to prove unique factorization of ideals in $\mathcal{O}_K$ (instead of elements themselves), which is a procedure that can be emulated for more general rings called Dedekind rings.

Once the obstruction to unique factorization is known, one can once more attempt to solve problems about integers by using amended factorization techniques to get around the obstruction. These applications are important and much fun indeed. Moreover, my personal opinion is that after a course in algebraic number theory, one should be able to calculate with the notions above. By this I mean for example that if I give you a number field $K = \mathbb{Q}[x]/(f)$, then you can, at least in principle, find its ring of integers and its class group. At least for the case of quadratic and cubic number fields, we will do a lot of examples of these calculations. Being able to calculate like this is not only useful because number theory has practical applications and analogues (such as those mentioned below), but also because being forced to calculate concretely with ideals tends to lead to a better understanding of them.

Prerequisites

To understand this course, you need a basic understanding of groups, rings and fields. Further knowledge of Galois theory is useful but not required.

Why you should care

Dedekind rings have useful applications beyond number rings. We will not give examples in these notes, but one can think of trendy subjects such as cryptography (and its counterpart cryptanalysis) and codes. Both of these subjects can be explored by using algebraic curves over finite fields. To give an example in cryptography, it turns out that there is a rather non-trivial group structure on the solutions of an equation such as $y^2 = x^3 + x - 1$ modulo $10^7 + 19$, or indeed modulo a much bigger prime. The unpredictability of this group structure can be used to decently encrypt information. The study of curves such as these resembles algebraic number theory to a great extent, with the field of rational functions on it corresponding to a number field and the functions with prescribed pole orders in certain points of the curves taking the place of algebraic integers.

When restricting oneself to questions about integers, it is not unreasonable to doubt the usefulness of algebraic number theory at first. After all, why generalize to extensions of $\mathbb{Q}$ when all that one is interested in is ordinary integers? However, it does turn out that algebraic number theory in its general setting is very useful for these concrete questions as well. Consider another example coming from cryptanalysis, namely the decrypting of an RSA system. This question comes down to factoring a product of two large primes. The best factorization algorithm currently available is the number field sieve, which as the name suggest makes use of number fields larger than $\mathbb{Q}$. In other words, being interested in concrete problems gives you no excuse not to know algebraic number theory, and you should really turn the page now. . .

0.2 Notation

In this section, we summarize the notation used in these notes, and we indicate some alternative notation styles used in the literature.

$|$ A field extension; the notation $L\,|\,K$ indicated that K is a subfield of L. Elsewhere $L \mid K$ is usually denoted by L/K, but because of the possible confusion with quotients I prefer to avoid this.

$[\,:\,]$ The degree of a field extension. Elsewhere $[L : K]$ is sometimes denoted $\deg(L/K)$. Also denoted the index $[A : B]$ of an abelian group B in a larger abelian group A.

B A basis of a field L considered as an extension of a smaller field K. Typically used for number fields considered as extensions $K\,|\,\mathbb{Q}$.

d Usually a degree $[L : K]$ of an extension of fields. See $[\,:\,]$.

e See d.

f Usually an irreducible polynomial over a field, most often $\mathbb{Q}$.

$\overline{f}$ The reduction of a polynomial over $\mathbb{Z}$ modulo a prime.

g See f.

$\overline{g}$ See $\overline{f}$.

I An ideal.

I^{-1} The ideal inverse of the ideal I.

J See I.

K A number field.

$\overline{K}$ The algebraic closure of a field K.

$\overline{K}^L$ The algebraic closure of a field K in a larger field L.

$K(\alpha)$ The smallest field that contains both K and the element α.

$K(S)$ The smallest field that contains both K and the elements of the set S.

L A number field, typically an extension of a base number field K. See K. Sometimes a linear map, and later occasionally a lattice in a vector space or a logarithmic embedding map.

L_α The linear map $K \to K$ defined by the element α of a number field K.

Log A logarithmic map used in the section on the geometry of numbers.

nm The norm map of a finite extension of fields, which we have used in particular for number fields $K\,|\,\mathbb{Q}$.

$\mathcal{O}$ An order in a number field, or in other words a number ring.

$\mathcal{O}_K$ The maximal order of a number field K. Also called the ring of integers of that number field. Elsewhere the notation $\mathbb{Z}_K$ is sometimes employed instead.

$\mathfrak{p}$ A prime ideal.

P A parallelepiped.

$\mathfrak{q}$ See $\mathfrak{p}$.

$\mathbb{Q}(\alpha)$ See $K(\alpha)$.

R A ring.

$R[\alpha]$ The smallest ring that contains both R and the element α.

$R[S]$ The smallest ring that contains both R and the elements of the set S.

r	In the presence of an irreducible polynomial f over a number field K (usually $\mathbb{Q}$), this is the distinguished root $x+(f)$ of f in the field $\mathbb{Q}[x]/(f)$. Very often this notation is interchangeable with α; the difference is that r is typically not used for an element that does not generate the field under consideration, and that it is moreover only used in the presence of a specified irreducible polynomial. Later in the notes this is sometimes a ring element, or the number of distinct embeddings of a number field K into $\mathbb{R}$.
s	The number of embeddings of a number field K into $\mathbb{C}$ up to complex conjugation. But sometimes also used to denote an element of a ring.
tr	The trace map of a finite extension of fields, which we have used in particular for number fields $K\,\vert\,\mathbb{Q}$.
R	A ring, often a number ring.
$\mathbb{Z}[\alpha]$	See $R[\alpha]$.
α	An algebraic number.
β	See α.
$\Delta_B(K)$	The discriminant of a number field K with respect to a basis B.
$\Delta(\mathcal{O}_K)$	The discriminant of the number field $K=\mathrm{Frac}(\mathcal{O}_K)$ with respect to any integral basis of the order $\mathcal{O}_K$. Some writers also call this $\Delta(K)$.
$\Delta(f)$	The discriminant of an irreducible polynomial f of degree d. It equals $\Delta_B(K)$, where $K=\mathbb{Q}[x]/(f)$ and where $B=\left\{1,r,\ldots,r^{d-1}\right\}$.
π	An irreducible element of a ring.
φ	An embedding of a number field K into $\mathbb{C}$. Elsewhere these are sometimes denoted by ι.
ψ	See φ.
Φ	A cyclotomic polynomial. Later also used for the embedding $\Phi : K \to \mathbb{C}^d$ obtained by combining all embeddings of a number field K.
ζ	A root of unity.

Chapter 1

Theory

1.1 Algebraic numbers

Let L be a field containing another field K. Then L is called a field extension of K. By using scalar multiplication, we can consider L as a vector space over K.

Notation 1.1.1. A field extension $K \subset L$ is also denoted by $L \,|\, K$. The degree $[L : K]$ of the extension $L \,|\, K$ is the dimension of L when considered as a vector space over K.

Definition 1.1.2. The extension $L \,|\, K$ is called finite if $[L : K] < \infty$.

Definition 1.1.3. A number field is a field that is a finite extension of $\mathbb{Q}$.

Notation 1.1.4. Let $L \,|\, K$ be a field extension. Given a set $S = \{a_1, a_2, ..., a_n\}$, we denote by $K(S) = K(a_1, a_2, ..., a_n)$ the smallest subfield of L containing S.

Example 1.1.5. Let d be a non-square in $\mathbb{Q}$, and let $\sqrt{d}$ be the distinguished square root of the polynomial $x^2 - d$ in $\mathbb{C}$. So $\sqrt{d}$ equals the usual positive root of d when $d > 0$, and it equals $\sqrt{|d|}i$ when $d < 0$. We consider a field extension $L \,|\, K$ as above with $L = \mathbb{Q}(\sqrt{d})$ (considered as a subfield of $\mathbb{R}$) and $K = \mathbb{Q}$. We show that $[L : K] = [\mathbb{Q}(\sqrt{d}) : \mathbb{Q}]$ is finite, which will prove that the field $\mathbb{Q}(\sqrt{d})$ is a number field.

First of all $\sqrt{d} \notin \mathbb{Q}$. Therefore $[\mathbb{Q}(\sqrt{d}) : \mathbb{Q}] > 1$. I now claim that $\{1, \sqrt{d}\}$ is a vector space basis for the extension $\mathbb{Q}(\sqrt{d}) \mid \mathbb{Q}$. To prove this, it shows that the vector space spanned by these elements is indeed a field. Indeed, any field containing $\sqrt{d}$ must contain these two elements, so if the elements span a field themselves, then this is the smallest field containing $\sqrt{d}$.

So consider the vector space

$$V = \mathbb{Q} \oplus \mathbb{Q}\sqrt{d} = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\}. \tag{1.1.1}$$

Since V is a subset of the field $\mathbb{C}$, we only have to verify the following properties to show that it is a field.

(i) V is closed under addition. This is clear.

(ii) V is closed under multiplication. This follows because

$$(a_1 + b_1\sqrt{d})(a_2 + b_2\sqrt{d}) = (a_1a_2 + db_1b_2) + (a_1b_2 + b_1a_2)\sqrt{d} \tag{1.1.2}$$

(iii) Every non-zero element of V has an inverse. Since $\sqrt{d}$ is not in $\mathbb{Q}$, an element $a+b\sqrt{d}$ is non-zero if and only if a and b are not both zero. But in that case $a^2 - db^2$ is also non-zero (otherwise d would be a square in $\mathbb{Q}$). Now one verifies that the element $(a - b\sqrt{d})/(a^2 - db^2)$ is an inverse of $a + b\sqrt{d}$.

We have shown that $\mathbb{Q}(\sqrt{d})$ is a number field, and that

$$\mathbb{Q}(\sqrt{d}) = \left\{ a + b\sqrt{d} : a, b \in \mathbb{Q} \right\}. \tag{1.1.3}$$

The final step (iii) above is a trick that only works for quadratic fields. We now develop methods for more general fields.

Proposition 1.1.6. *Let $f \in K[x]$ be an irreducible polynomial of degree d. Let $L = K[x]/(f)$, and let α be the image of x in L. Then the extension $L \,|\, K$ is finite, and the set $B = 1, \alpha, ..., \alpha^{d-1}$ is a basis of L as a vector space over K. In particular L has degree d over K.*

Proof. We again let $V = \operatorname{span}(S)$, which a priori is a subspace of L. We claim that it is all of L. There are many slick ways to do this (proofs of a few lines certainly exist), but we stick with a calculatory approach, both because it is useful in practice and because we can exploit the ideas involved when we define trace and norm later. So let us verify the usual properties.

(i) V is closed under addition. OK!

(ii) V is closed under multiplication. First we show that V is closed under multiplication by α. Let $\sum_{i=0}^{d-1} c_i \alpha^i$ be in V, with $c_i \in \mathbb{Q}$. If we multiply this with α, we get $\sum_{i=0}^{d-1} c_i \alpha^{i+1}$. The first $d-1$ terms are certainly in V. It remains to deal with the term $c_{d-1}\alpha^d$. Suppose that $f = \sum_{i=0}^{d} a_i x^i$, with $a_i \in \mathbb{Q}$ and $a_d \neq 0$. Then we have $\alpha^d = (-1/a_d) \sum_{i=0}^{d-1} a_i \alpha^i$, so $c_{d-1}\alpha^d = \sum_{i=0}^{d-1} (-c_{d-1}/a_d) a_i \alpha^i$, which is again in V.

To deal with general elements of V, we can use induction, but we instead use a trick from linear algebra. We have just seen that multiplication by α defines a map from V to V. Because of the distributivity of multiplication (or alternatively, because of the explicit formula above), we see that it in fact defines a $\mathbb{Q}$-linear map

$$L_\alpha : V \to V. \tag{1.1.4}$$

(Here L_α stand for "linear" or "left multiplication", as you prefer.) Now let $v = \sum_{i=0}^{d-1} c_i \alpha^i$ be an arbitrary element of V. We get a $\mathbb{Q}$-linear map L_v from v as well. But by distributivity and associativity, we have

$$L_v = \sum_{i=0}^{d-1} c_i L_{\alpha^i} = \sum_{i=0}^{d-1} c_i L_\alpha^i. \tag{1.1.5}$$

This again maps V into V. We are done.

(iii) V is closed under inversion. Let $v \in V$ be the non-zero element to be inverted.

I claim that L_v is injective. Indeed, otherwise there would exist a non-zero v' such that $vv' = 0$ in the quotient L of $K[x]$. Choose representatives $\widetilde{v}$, $\widetilde{v'}$ in $K[x]$ for an equality of the form $\widetilde{v}\widetilde{v'} = gf$. We now use that f is irreducible and that polynomials $K[x]$ can be uniquely factored into irreducibles to see that f divides $\widetilde{v}$ or $\widetilde{v'}$. But this is nonsense, since these elements were non-zero in the quotient. Alternatively, dividing with remainder, one gets a polynomial of smaller degree than f that divides f, equally well a contradiction.

So $L_v : V \to V$ has trivial kernel. Count dimensions to see that L_v is surjective as well. This means that there exists a v' such that $vv' = 1$.

We have shown that L is a finite extension of K, and that

$$L = \left\{ \sum_{i=0}^{d-1} c_i \alpha^i : c_i \in \mathbb{Q} \right\} . \tag{1.1.6}$$

□

Using irreducible polynomials f in $\mathbb{Q}[x]$, this gives a large supply of number fields $K = \mathbb{Q}[x]/(f)$. These number field are also called Stammkörper in German. There are many everyday number fields that are not immediately given in this "principal" form, for example $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. However, we do get all number fields in this way:

Fact 1.1.7. *Every number field K is isomorphic to a number field $\mathbb{Q}[x]/(f)$ defined by a* single *irreducible polynomial f over $\mathbb{Q}$. More precisely, every element α of K outside a certain subset of codimension* 0 *has minimal polynomial f_α of degree $[K : \mathbb{Q}]$, and in this case we can take f to equal f_α.*

In Section 2.1, we will see how to find such an α in practice.

The following statement has a standard proof, which is left as an exercise.

Proposition 1.1.8 (Tower law). *Let $L \,|\, K$ and $M \,|\, L$ be field extensions. Then $[M : K] = [M : L][L : K]$. More precisely, if S is a basis of the extension $L \,|\, K$, and T a basis of $M \,|\, L$, then the extension $M \,|\, K$ has basis $ST = \{st : s \in S, t \in T\}$.*

Definition 1.1.9. Let $L \,|\, K$ be a field extension, and let α be an element of L. Then α is said to be algebraic over K if there exists a polynomial $f \in K[x]$ such that $f(\alpha) = 0$. If $K = \mathbb{Q}$, then we also say that α is an algebraic number. In that case, division with remainder in $K[x]$ shows that there exists a unique monic polynomial $f_\alpha \in K[x]$ whose degree is minimal. We call this the minimal polynomial of α.

Proposition 1.1.10. *Let $L \,|\, K$ be a field extension, and let α be an element of L. Then α is algebraic if and only if the extension $K(\alpha) \,|\, K$ is finite.*

Proof. For the "if"-part, consider the powers α^i of α. These are all in $K(\alpha)$ and therefore cannot all be independent over K. A dependence gives rise to a polynomial in $K[x]$ vanishing on α.

For the "only if"-part, let f be a polynomial of degree d vanishing on α. We can mimic the proof above to see that $K(\alpha)$ is spanned by the powers $\{1, \alpha, ..., \alpha^{d-1}\}$. These elements may not be independent, but that does not matter; the extension $K(\alpha) \,|\, K$ is still finite. □

The following two propositions are also proved in [1, Section 2.1]. Since we will revisit them in Section 1.3, we do not go into further detail. In fact, it is probably more useful to try and prove these results yourself after reading that section.

Theorem 1.1.11. *Let $L \,|\, K$ be a field extension. Then the subset*

$$\overline{K}^L = \{x \in L : x \text{ algebraic over } K\} \tag{1.1.7}$$

is a subfield of L.

Definition 1.1.12. The field $\overline{K}^L$ is called the algebraic closure of K in L. The fields that we obtain by choosing L to be algebraically closed are all isomorphic, so here the dependency on L is dropped from the notation. The resulting field $\overline{K}$ (or rather its isomorphism class) is simply called the algebraic closure of K.

Theorem 1.1.13. *Let $L \,|\, K$ be a field extension. Then the algebraic closure $\overline{K}^L$ of K in L is algebraically closed in L in the sense that every element of L that is algebraic over $\overline{K}^L$ is already algebraic over K, hence in $\overline{K}^L$ itself. In a formula:*

$$\overline{(\overline{K}^L)}^L = \overline{K}^L. \tag{1.1.8}$$

Example 1.1.14. Take $L = \mathbb{C}$ and $K = \mathbb{Q}$ to obtain the algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. By considering quadratic extensions of $\mathbb{Q}$, one can already show that $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$. So the extension $\overline{\mathbb{Q}} \,|\, \mathbb{Q}$ is infinite, but because all elements of $\overline{\mathbb{Q}}$ are algebraic over $\mathbb{Q}$, the extension $\mathbb{Q}(S)$ of $\mathbb{Q}$ is finite for every *finite* subset S of $\overline{\mathbb{Q}}$.

There is nothing particularly weird about this. Consider the countable infinite vector space $\mathbb{R}^{\mathbb{N}}$ over $\mathbb{R}$, which is spanned by the standard basis vectors $\{e_1, \dots, e_n, \dots\}$. Then by definition, every element of $\mathbb{R}^{\mathbb{N}}$ can be written as a finite sum in the e_i. In particular, any finite subset of $\mathbb{R}^{\mathbb{N}}$ generates a finite-dimensional subspace. But $\mathbb{R}^{\mathbb{N}}$ itself is infinite-dimensional over $\mathbb{R}$.

1.1.1 Complex embeddings

Let $K = \mathbb{Q}[x]/(f)$ be a number field defined by an irreducible polynomial $f \in \mathbb{Q}[x]$ of degree d, and let $r = x + (f)$ be the distinguished root of f in K. Usually r will be the only root of f in K. But in $\mathbb{C}$, we can find d roots, which are distinct because f is irreducible. (Proof: if f has multiple roots, then the non-trivial gcd of f and f' would divide f.)

Proposition 1.1.15. *Under the hypotheses above, there are d distinct embeddings $\varphi_1, \dots, \varphi_d : K \to \mathbb{C}$. Let $r_1 = \varphi_1(r), \dots, r_d = \varphi_d(r)$ be the images of r under these embeddings. Then if f is monic, we have*

$$f = \prod_{i=1}^{d} (x - r_i). \tag{1.1.9}$$

Proof. An embedding φ has to send r to a root of f in $\mathbb{C}$, and because an embedding is $\mathbb{Q}$-linear and K is spanned over $\mathbb{Q}$ by the powers of r, this completely determines the embedding. So at most d embeddings exist, and conversely we see that we can associate a well-defined embedding $K \to \mathbb{C}$ to a complex root z of $\mathbb{C}$ by factoring the homomorphism $\mathbb{Q}[x] \to \mathbb{C}$ given by

$$\sum_{i=0}^{d-1} c_i x^i \longmapsto \sum_{i=0}^{d-1} c_i z^i \tag{1.1.10}$$

(Note that this homomorphism vanishes on (f) by construction.) The final statement follows because the polynomials on both sides are monic and their roots coincide. □

Definition 1.1.16. Let α be an algebraic number, and let f_α be its minimal polynomial. Then the roots of f_α in $\mathbb{C}$ are called the conjugates of α. If $\varphi_1, \dots, \varphi_d$ are the embeddings of $\mathbb{Q}(\alpha)$ in $\mathbb{C}$, then the conjugates of α are $\alpha_1 = \varphi_1(\alpha), \dots, \alpha_d = \varphi_d(\alpha)$.

1.2 Norm, trace, discriminant

In this section we develop the linear-algebraic methods needed to relate the arithmetic of a number field to the arithmetic of the rational numbers.

Let $K = \mathbb{Q}[x]/(f)$ be a number field defined by an irreducible polynomial of degree d. Let α be an element of K. Then as before, we can consider the $\mathbb{Q}$-linear map $L_\alpha : K \to K$ given by multiplication by α. We can determine the matrix M_α with respect to a basis of K over $\mathbb{Q}$. The characteristic polynomial of this matrix, which does not depend on the chosen basis, is denoted by g_α. It is an element of $\mathbb{Q}[x]$, and we can therefore write

$$g_\alpha = g_0 + g_1 x + \cdots + g_{d-1}x^{d-1} + x^d \tag{1.2.1}$$

with g_i in $\mathbb{Q}$.

Definition 1.2.1. We define the trace of α by

$$\operatorname{tr}(\alpha) = \operatorname{tr}(M_\alpha) = -g_{d-1} \tag{1.2.2}$$

and the norm of α by

$$\operatorname{nm}(\alpha) = \det(M_\alpha) = (-1)^d g_0 = (-1)^d g_\alpha(0). \tag{1.2.3}$$

As coefficients of the characteristic polynomial, the trace and the norm are independent of the choice of basis. They also satisfy some pleasant algebraic properties:

Proposition 1.2.2. *The trace is additive, and the norm is multiplicative; for any α, β in K we have*

$$\operatorname{tr}(\alpha+\beta) = \operatorname{tr}(\alpha) + \operatorname{tr}(\beta),\ \operatorname{nm}(\alpha+\beta) = \operatorname{nm}(\alpha)\operatorname{nm}(\beta). \tag{1.2.4}$$

Proof. This follows immediately from the relations

$$L_{\alpha+\beta} = L_\alpha + L_\beta, L_{\alpha\beta} = L_\alpha L_\beta, \tag{1.2.5}$$

which are just translation of distributivity and associativity. □

Theorem 1.2.3. *Let α be an element of K. Let $\varphi_1, \ldots, \varphi_d$ be the embeddings of K into $\mathbb{C}$, and for $i = 1, \ldots, d$ let $\alpha_i = \varphi(\alpha)$. Then we have*

$$\begin{aligned}\operatorname{tr}(\alpha) &= \sum_{i=1}^{d} \alpha_i,\\ \operatorname{nm}(\alpha) &= \prod_{i=1}^{d} \alpha_i.\end{aligned} \tag{1.2.6}$$

Proof. First assume that we have $\mathbb{Q}(\alpha) = K$. Then the minimal polynomial f_α of α has degree d. Indeed, the degree cannot be larger because $\mathbb{Q}(\alpha)$ is contained in K, and if the degree were smaller, then we would have $[\mathbb{Q}(\alpha) : \mathbb{Q}] < [K : \mathbb{Q}]$ and hence $\mathbb{Q}(\alpha) \neq K$, contrary to our assumption.

Consider the linear map L_α. Then we have $g(L_\alpha) = 0$ by the Cayley-Hamilton theorem. But as we have seen in the proof of 1.1.6, we have

$$g(L_\alpha) = L_{g(\alpha)}. \tag{1.2.7}$$

So $L_{g(\alpha)} = 0$. On the other hand, an element β of a number field can be read off from the corresponding linear map L_β by taking the image of 1 under L_β. Therefore $g(\alpha) = 0$. However, g_α is of degree d, so since it is monic, it has to equal $f_\alpha = \prod_i (x - \alpha_i)$. We can then compare coefficients to conclude.

This deals with "almost all" α. To get the result in general, choose a generator r of the extension $K \,|\, \mathbb{Q}$, such as the distinguished root of f in K. Note that the result above shows that there exists an invertible matrix T over $\mathbb{Q}$ such that

$$M_r = T D_r T^{-1}, \tag{1.2.8}$$

where D_r is the diagonal matrix with entries $r_1 = \varphi_1(r), \ldots, r_d = \varphi_d(r)$. Now an arbitrary element α of K can be written in the form $\sum_i c_i r^i$, and using associativity and distributivity again, we get

$$\begin{aligned} M_\alpha &= \sum_{i=0}^{d-1} c_i M_r^i \\ &= \sum_{i=0}^{d-1} c_i (T D_r T^{-1})^i \\ &= T(\sum_{i=0}^{d-1} c_i D_r^i) T^{-1}. \end{aligned} \tag{1.2.9}$$

But since we have the equalities

$$\begin{aligned} \alpha_1 &= \varphi_1(\alpha) = \varphi_1(\sum c_i r^i) = c_i \sum r_1^i \\ &\vdots \\ \alpha_d &= \varphi_d(\alpha) = \varphi_d(\sum c_i r^i) = c_i \sum r_d^i \end{aligned} \tag{1.2.10}$$

the result once again follows by taking trace and determinant. □

Remark 1.2.4. While the elements $\varphi_i(\alpha)$ always run through the conjugates of α, they may coincide for different i if α does not generate K. In other words, the $\varphi_i(\alpha)$ are the conjugates of α with certain (uniform) multiplicities. In fact this implies that if α does not generate K, then g_α will be a power of f_α, but we will never need this.

We have considered $K \mid \mathbb{Q}$ as a vector space over $\mathbb{Q}$; scalar multiplication gave it a structure as a $\mathbb{Q}$-vector space. There is some more $\mathbb{Q}$-linear structure on K, which comes from a special $\mathbb{Q}$-bilinear form on K, namely

$$(\alpha, \beta) \longmapsto \operatorname{tr}(\alpha\beta). \tag{1.2.11}$$

We call this pairing the trace pairing.

Proposition 1.2.5. *The trace pairing is perfect: if α is an element of K, and* $\operatorname{tr}(\alpha\beta) = 0$ *for all $\beta \in K$, then $\alpha = 0$.*

Proof. If $\alpha \neq 0$, then $\operatorname{tr}(\alpha\alpha^{-1}) = d$. □

By choosing bases, we can relate the trace pairing with a matrix. So let $B = \{b_1, \ldots, b_d\}$ be a basis of $K \mid \mathbb{Q}$. This gives an isomorphism $i_B : K \to \mathbb{Q}^d$ that sends b_i to the i-th standard basis vector e_i. In terms of this basis, there exists a matrix T_B such that

$$\operatorname{tr}(\alpha\beta) = i_B(\alpha)^t T_B i_B(\beta), \tag{1.2.12}$$

and T_B is non-singular because of the proposition that we just proved. Tracing through the isomorphisms, we get

$$(T_B)_{i,j} = \operatorname{tr}(b_i b_j). \tag{1.2.13}$$

Definition 1.2.6. The discriminant $\Delta_B(K)$ of K relative to the basis B is the determinant of the matrix T_B.

This is not quite as nice as one would like, because T_B depends on the choice of B. More precisely, suppose that $B' = SB$ in the sense that

$$b_i' = \sum_{j=1}^{d} S_{i,j} b_j \tag{1.2.14}$$

for some invertible matrix $S = \{S_{i,j}\}_{i,j}$. Then $i_{B'}(b_i') = e_i$ and $i_B(b_i') = \sum S_{i,j} e_j$, so we have $i_B = S i_{B'}$ as linear maps. Moreover,

$$\begin{aligned} Tr(\alpha\beta) &= i_B(\alpha)^t T_B i_B(\beta) \\ &= i_B'(\alpha)^t S^t T_B S i_B'(\beta). \end{aligned} \tag{1.2.15}$$

so we get

$$T_B' = S^t T_B S \tag{1.2.16}$$

and

$$\Delta_{B'}(K) = \det(S)^2 \Delta_B(K). \tag{1.2.17}$$

We will get around this ambiguity after we have defined algebraic integers. For now, we state the following relations expressing determinants in terms of conjugates. Their proofs can be found in [1, Section 3.2].

Proposition 1.2.7. *Let $\varphi_1, \ldots, \varphi_d$ be the embeddings of K into $\mathbb{C}$. Then*

$$\Delta_B(K) = \det\left((\varphi_i(b_j))_{i,j=1}^d \right)^2. \tag{1.2.18}$$

Proposition 1.2.8. *Let $K = \mathbb{Q}[x]/(f)$, with $f \in \mathbb{Q}[x]$ an irreducible polynomial, and let r be the image of x in K. Consider the $\mathbb{Q}$-basis $B = \{1, r, \ldots, r^{d-1}\}$ of K . Then*

$$\Delta_B(K) = \prod_{i<j} (r_i - r_j)^2. \tag{1.2.19}$$

So the discriminant is related with the usual notion of the discriminant for polynomials. Therefore we employ the following notation.

Notation 1.2.9. Let f be an irreducible polynomial, let $K = \mathbb{Q}[x]/(f)$ be the corresponding number field, and let r be the image of x in K. Then we denote by $\Delta(f)$ the discriminant of K for the basis $B = \{1, r, \ldots, r^{d-1}\}$ of K associated to r.

1.3 Algebraic integers

Let K be an extension of $\mathbb{Q}$, and let α be an element of K. Then in Section 1.1 we have seen, either as a definition or as a result:

(A0) α is algebraic if and only if there is exists a monic polynomial over $\mathbb{Q}$ such that $f(\alpha) = 0$, in which case we can use the minimal polynomial f_α of α over $\mathbb{Q}$ (see Definition 1.1.9);

(A1) α is algebraic if and only if $K(\alpha)$ is a finite-dimensional vector space over $\mathbb{Q}$ (see Proposition 1.1.10).

(A2) The algebraic elements in K form a subfield $\overline{\mathbb{Q}}^K$ of K (see Theorem 1.1.11);

(A3) $\overline{\overline{\mathbb{Q}}^K}^K = \overline{\mathbb{Q}}^K$ (see Theorem 1.1.13).

We are going to define algebraic integers in such a way that these statements are true, but also in such a way that get the old integers back in the case $K = \mathbb{Q}$. We have to consider what is so intrinsically special about the elements of $\mathbb{Z}$ anyway.

Notation 1.3.1. Let S be a ring extension of a ring R, and let T be a subset of S. Then the smallest subring of S containing T is denoted by $R[T]$.

These rings are not hard to describe.

Proposition 1.3.2. *Let S be a ring extension of a ring R, and let T be a subset of S. Let*

$$M = \left\{ \prod_{i=1}^{N} t_i : N \in \mathbb{N}, t_i \in T \right\} \tag{1.3.1}$$

be the monomials in the elements of T. Then

$$R[T] = \left\{ \sum_{i=0}^{N} r_i m_i : N \in \mathbb{N}, r_i \in R, m_i \in M \right\}. \tag{1.3.2}$$

Proof. Formal multiplication shows that the right hand side is indeed a ring. But $R[T]$ certainly should contain M by multiplicativity. □

Example 1.3.3. Let $S = \mathbb{Q}(t)$ be the field of rational functions, which is both a ring extension and a field extension of $R = \mathbb{Q}$. Then

$$\mathbb{Q}[t^2] = \left\{ \sum_{i=0}^{N} a_i t^{2i} : a_i \in \mathbb{Q} \right\}. \tag{1.3.3}$$

while $\mathbb{Q}(t^2)$, the smallest sub*field* of S containing t^2, is given by

$$\mathbb{Q}(t^2) = \left\{ (\sum_{i=0}^{N} a_i t^{2i}) / (\sum_{i=0}^{M} b_j t^{2j}) : a_i, b_j \in \mathbb{Q} \right\}. \tag{1.3.4}$$

As an exercise, you can show that if $L|K$ is an extension, and S is a set of elements of L that are algebraic over K, then $K[S] = K(S)$.

The intrinsic property that distinguishes integers from general rational numbers is the following.

Proposition 1.3.4. *Let q be a rational number. Then q is an integer if and only if $\mathbb{Z}[q]$ is a finitely generated abelian group.*

Proof. If q is an integer, then $\mathbb{Z}[q] = \mathbb{Z}$, so one implication is clear. Now suppose that p is a prime occurring in the denominator of q. Suppose that $\{b_1, ..., b_n\}$ generates the abelian group $\mathbb{Z}[q]$. Let p^n be the maximal power of p occurring in the denominators of the b_i. Then every element of $\mathbb{Z}b_1 + \ldots + \mathbb{Z}b_n$ has at most a power p^n in its denominator. Which is a contradiction, since q^{n+1} is in $\mathbb{Z}[q]$. □

We can rephrase this in terms of polynomials.

Proposition 1.3.5. *Let q be a rational number. Then q is an integer it is a zero of a monic polynomial in $\mathbb{Z}[x]$.*

Proof. Suppose that q is the zero of a monic polynomial f in $\mathbb{Z}[x]$. We can now rerun the proof of Proposition 1.1.6. What makes everything work *over the integers* this time is that we do not have to divide by the leading coefficient a_d, so we do not move out of the integers. In the end, we see that $\mathbb{Z}[q]$ is generated as an abelian group by $\{1, q, \ldots, q^{d-1}\}$, and then we can apply the previous proposition. □

This motivates us to give the following definition.

Definition 1.3.6. An element α of a number field is called an algebraic integer if it is integral over $\mathbb{Z}$, which means by definition that there exists a *monic* polynomial $f \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$.

More generally, let $S|R$ be a ring extension, and let $s \in S$. Then s is called integral over R if there exists a monic polynomial f over R such that $f(s) = 0$. Finally, R is called integrally closed in S if the only elements of S that are integral over R are the elements of R itself. If R is a domain, then we say that R is integrally closed if it is integrally closed in its field of fractions.

We get by the essentially the same proof as that of Proposition 1.1.10:

Proposition 1.3.7. *An element α of a number field is integral if and only if the ring $\mathbb{Z}[\alpha]$ is a finitely generated abelian group.*

A more practical result, that makes it straightforward to check if an algebraic number is an integer, is the following. A nice proof is in [4, Lemma 2.3.4]; other proofs are much more indirect and make use of Gauss' Lemma to essentially nuke a mosquito.

Proposition 1.3.8. *An element α of a number field is integral if and only the minimal polynomial f_α has integral coefficients.*

We have found the correct analogue of (A0) and (A1). As for (A2):

Proposition 1.3.9. *The integers of a number field K form a subring of K.*

Proof. Suppose that α and β are integral elements of K. We have to show that $\alpha + \beta$, $\alpha - \beta$, and $\alpha\beta$ are integral as well. But these elements are all in the ring $\mathbb{Z}[\alpha, \beta]$. Let f be a monic polynomial of degree d such that $f(\alpha) = 0$, and let g be of degree e such that $g(\beta) = 0$. Then the usual reduction process shows that a *finite* amount of monomials in α and β suffice; we have

$$\mathbb{Z}[\alpha, \beta] = \left\{ \sum_{i=0}^{d-1} \sum_{j=0}^{e-1} a_i b_j \alpha^i \beta^j : a_i, b_j \in \mathbb{Z} \right\}. \tag{1.3.5}$$

In other words, as an abelian group $\mathbb{Z}[a, b]$ is finitely generated by $\{\alpha^i \beta^j : 0 \leq i \leq d - 1, 0 \leq j \leq e - 1\}$. Since subgroups of finitely generated abelian groups are again finitely generated, the rings $\mathbb{Z}[\alpha + \beta]$, $\mathbb{Z}[\alpha - \beta]$, and $\mathbb{Z}[\alpha\beta]$ are finitely generated, whence the result. □

Notation 1.3.10. Let K be a number field. Then the subring of K formed by the algebraic integers in K is called the ring of integers of K and denoted by $\mathcal{O}_K$.

We have the reassuring equality $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$. Finally, the analogue of (A3) is

Proposition 1.3.11. *Suppose that $\alpha \in K$ is integral over $\mathcal{O}_K$. Then $\alpha \in \mathcal{O}_K$.*

Proof. The idea is to reduce from the big ring $\mathcal{O}_K$ to a smaller ring generated by coefficients that we know to be finitely generated. In detail, suppose that $f \in \mathcal{O}_K[x]$ is a monic polynomial of degree d vanishing in α. Let $A = \{a_0, ..., a_{d-1}\}$ be the set of coefficients of f. Then the ring $\mathbb{Z}[A]$ is finitely generated; if a_i is the zero of a monic polynomial in $\mathbb{Z}[x]$ of degree e_i, then $\mathbb{Z}[A]$ is spanned by

$$\left\{a_0^{k_0} \cdots a_{d-1}^{k_{d-1}} : 0 \leq k_i \leq e_i - 1\right\}. \tag{1.3.6}$$

Consider the ring $\mathbb{Z}[\alpha]$. This is contained in the ring $\mathbb{Z}[A, \alpha]$. We will show that the latter ring is finitely generated as an abelian group. For this, note that because of the existence of f we have

$$\mathbb{Z}[A, \alpha] = \left\{\sum_{i=0}^{d-1} a_i \alpha^i : a_i \in \mathbb{Z}[A]\right\}. \tag{1.3.7}$$

(This is where the trick comes in; the coefficients of f are in a finitely generated abelian group, not merely in $\mathcal{O}_K$, about which we do not know a lot yet.) Our description of $\mathbb{Z}[A]$ above now yields.

$$\mathbb{Z}[A, \alpha] = \left\{\sum_{i=0}^{d-1} \sum_{k_1,\ldots,k_{d-1}=0}^{e_i-1} q_{i,k_1,\ldots,k_{d-1}} a_0^{k_0} \cdots a_{d-1}^{k_{d-1}} \alpha^i : q_{i,k_1,\ldots,k_{d-1}} \in \mathbb{Z}\right\}. \tag{1.3.8}$$

So $\mathbb{Z}[A, \alpha]$ is finitely generated by the elements.

$$\left\{a_0^{k_0} \cdots a_{d-1}^{k_{d-1}} \alpha^i : 0 \leq k_i \leq e_i - 1, 0 \leq i \leq d\right\}. \tag{1.3.9}$$

□

When given an integral element, all arithmetic information over $\mathbb{Q}$ associated to it tends to be integral as well. For example:

Proposition 1.3.12. *If α is integral, then* $\mathrm{tr}(\alpha)$ *and* $\mathrm{nm}(\alpha)$ *are in $\mathbb{Z}$.*

Proof. Along with α, all its conjugates are integers. So the values in question are algebraic integers, as they are the sum, respectively product, of algebraic integers. We have also seen that they are in $\mathbb{Q}$. Therefore they are in $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$. □

1.4 The ring $\mathcal{O}_K$

We now study the ring $\mathcal{O}_K$. We will later find effective methods to determine it explicitly, but right now we just try to see how big it is.

Proposition 1.4.1. *$\mathcal{O}_K$ contains an additive group isomorphic to $\mathbb{Z}^d$.*

Proof. Write $K = \mathbb{Q}[x]/(f)$ with f monic and irreducible of degree d, and let r be the image of x in K. Write $f = \sum_i a_i x^i \in \mathbb{Q}[x]$, and let N be the common denominator of the coefficients a_i. Then $Nf \in \mathbb{Z}[x]$ for some N, but of course in general this polynomial will not be monic. However,

$$\begin{aligned} 0 = \sum_{i=0}^{d-1} a_i r^i &= \sum_{i=0}^{d-1} (a_i N^{-i})(Nr)^i \\ &= \sum_{i=0}^{d-1} (a_i N^{d-i})(Nr)^i \end{aligned} \tag{1.4.1}$$

and the polynomial $\sum_{i=0}^{d-1}(a_i N^{d-i})(Nx)^i$ is monic and integral. So Nr is integral, and the ring $\mathbb{Z}[Nr]$ is finitely generated as an abelian group by the d elements $\{1, r, ..., r^{d-1}\}$. The map

$$\begin{aligned} \mathbb{Z}^d &\longrightarrow \mathbb{Z}[Nr], \\ (n_i)_{i=1}^d &\longmapsto \sum_{i=1}^d n_{i-1} r^i \end{aligned} \tag{1.4.2}$$

defines an isomorphism, since if it had a kernel, then there would be a rational polynomial of smaller degree vanishing in r. □

Proposition 1.4.2. *$\mathcal{O}_K$ is contained in an additive group isomorphic to $\mathbb{Z}^d$.*

Proof. Using the notation of the previous proof, consider the elements $\alpha_1 = 1, \alpha_2 = r, \ldots, \alpha_d = r^{d-1}$. Because the matrix defining the trace pairing is non-singular, there exist unique $\beta_1, \ldots, \beta_d$ in K such that

$$\mathrm{tr}(\alpha_i \beta_j) = \delta_{i,j} \tag{1.4.3}$$

(Kronecker delta). As such,

$$\mathbb{Z}\beta_1 + \ldots + \mathbb{Z}\beta_d = \{\beta \in K : \mathrm{tr}(\alpha_i \beta) \in \mathbb{Z} \text{ for all } i\} \tag{1.4.4}$$

But if β is integral, then the property on the right hand side holds by Proposition 1.3.12, since then the $\alpha_i \beta$ are all integral again. So

$$\mathcal{O}_K \subseteq \mathbb{Z}\beta_1 + \ldots + \mathbb{Z}\beta_d. \tag{1.4.5}$$

□

Definition 1.4.3. Let K be a number field of degree d. An order of K is a subring R of K that is isomorphic to $\mathbb{Z}^d$ as abelian group.

In particular, K is then the fraction field of R.

Theorem 1.4.4. *Let K be a number field. Then the ring of integers $\mathcal{O}_K$ of K is an order of K.*

Proof. Use the previous results and the structure theorem for finitely generated abelian groups. □

Because of the previous theorem, the ring of integers of K is often also called the maximal order of K.

One can show (try it!) that $\mathbb{Z}$ is the only order of $\mathbb{Q}$. On the other hand, every other number field contains infinitely many distinct orders. These orders can have a difficult structure. For example, if $K = \mathbb{Q}[x]/(f)$ with $f = x^3 + x^2 - 2x + 8$, then there does not exist any $\alpha \in K$ such that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. However, this phenomenon is not typical for fields of small degree. The structure of $\mathcal{O}_K$ in fact implies that all orders in quadratic fields are generated by a single element.

Definition 1.4.5. A number ring is an order in some number field. It need not be maximal!

1.4.1 Discriminants revisited

Using algebraic integers, we can finally attach a *unique* discriminant to a field K. Recall that we defined discriminants $\Delta_B(K)$ by using a basis, and that a change of basis affected $\Delta_B(K)$ by multiplying by the square of a determinant. It turns out that if we restrict to bases B that generate $\mathcal{O}_K$, then $\Delta_B(K)$ no longer depends on choices. This is for the following crucial reason.

Proposition 1.4.6. *Let $\mathbb{Z}^d \to \mathbb{Z}^d$ be a linear map given by a matrix A. Then A is invertible over $\mathbb{Z}$ if and only if $\det(A) \in \{\pm 1\}$.*

Proof. Use Cramer's rule for the non-trivial implication. □

Corollary 1.4.7. *Let B and B' be two $\mathbb{Z}$-bases of $\mathcal{O}_K$. Then $\Delta_B(K) = \Delta'_B(K)$.*

Proof. Because the elements of B' are in the abelian group generated by B, we have $B' = SB$ for some integral matrix S that is invertible over $\mathbb{Z}$. So $\det(S)^2 = 1$, and it now suffices to apply the general result $\Delta'_B(K) = \det(S)^2 \Delta_B(K)$ along with Proposition 1.4.6. □

Definition 1.4.8. Let K be a number field. We define the discriminant $\Delta(\mathcal{O}_K)$ of $\mathcal{O}_K$ to be the determinant of the matrix describing the trace pairing on some basis $b_1, \ldots, b_d$ of $\mathcal{O}_K$. In other words, we have

$$\Delta(\mathcal{O}_K) = (\mathrm{tr}(b_i b_j))_{i,j=1}^d \tag{1.4.6}$$

Since tr takes integral values on $\mathcal{O}_K$, the discriminant $\Delta(K)$ is integral. It gives us necessary criterion to determine whether we have found a $\mathbb{Z}$-basis of $\mathcal{O}_K$:

Proposition 1.4.9. *Let B', B be bases of K over $\mathbb{Q}$. Let*

$$L' = \mathbb{Z}b'_1 + \ldots + \mathbb{Z}b'_d, L = \mathbb{Z}b_1 + \ldots + \mathbb{Z}b_d. \tag{1.4.7}$$

Suppose that $L' < L$. Then $\Delta_{B'}(K) = [L : L']^2 \Delta_B(K)$, where $[L : L']$ is the subgroup index of L' in L.

Proof. Since the values of Δ_B are invariant under invertible integral transformations, we may use the Smith normal form to suppose that $b'_i = n_i b_i$, in which case the result is obvious:

$$\begin{aligned}\Delta'_B(K) &= \det(S)^2 \Delta_B(K) \\ &= (\prod_{i=1}^d n_i)^2 \Delta_B(K)\end{aligned} \tag{1.4.8}$$

while $[L : L'] = \prod_i n_i$. □

Corollary 1.4.10. *Let B be a subset of integral elements of K. If $\Delta_B(K)$ is squarefree, then $\mathcal{O}_K = \mathbb{Z}b_1 + ... + \mathbb{Z}b_n$.*

Finally, we give an important bit of intuition.

Proposition 1.4.11. *Let $f \in \mathbb{Z}[x]$ be a monic irreducible polynomial of degree d over $\mathbb{Q}$, let $K = \mathbb{Q}[x]/(f)$ be the corresponding number field, and let r be the image of x in K. Let $B = \{1, r, \ldots, r^{d-1}\}$. Then the primes dividing $\Delta_B(K)$ are exactly the primes modulo which f has a double root.*

Proof. Sketch : Use Proposition 1.2.8 along with the fact that the coefficients of both f and its reductions modulo p are symmetric expressions with integral expression in terms of the roots. □

1.5 Quadratic fields

This section classifies quadratic number fields and calculates their rings of integers. So let K be a quadratic extension of $\mathbb{Q}$, which means, by definition, that $[K : \mathbb{Q}] = 2$.

Proposition 1.5.1. *There exists a squarefree $d \in \mathbb{Z}$ such that $K = \mathbb{Q}(\sqrt{d}) = \mathbb{Q}[x]/(x^2-d)$. This d is uniquely determined by K.*

Proof. We will give a proof that is much too complicated involved, but the ideas in it are useful far beyond the case of quadratic fields.

There exists some element α of K that is not in $\mathbb{Q}$. Let $f = x^2 + ax + b$ be its minimal polynomial. Then $\beta = \alpha + (a/2)$ has minimal polynomial $x^2 - (b - (a^2/4))$. We let $d_0 = (b - (a^2/4))$. Replacing β by $N\beta$ transforms f into $x^2 - d_0 N^2$, and we can remove denominators and square factors from d_0 in this way to end up with a suitable d.

Now suppose that we have an isomorphism $\mathbb{Q}(\sqrt{d}) \cong \mathbb{Q}(\sqrt{d'})$ of quadratic fields obtained in this way. Then d' is a square in $\mathbb{Q}(\sqrt{d})$, so for some rational a and b, we have that $d' = (a + b\sqrt{d})^2 = (a^2 + db^2) + 2ab\sqrt{d}$. Since $\{1, \sqrt{d}\}$ is a basis of $\mathbb{Q}(\sqrt{d})$, we see that $ab = 0$. So either $d' = a^2$, which would mean that $\mathbb{Q}(\sqrt{d})$ is not a quadratic extension, or $d' = db^2$. Since d and d' are both squarefree and integral, this implies $d = d'$. □

We now determine the ring of integers $\mathcal{O}_K$. We know that $O_K \cap \mathbb{Q} = \mathbb{Z}$, because $\mathbb{Z}$ is the integral closure of $\mathbb{Z}$ in $\mathbb{Q}$. So let $\alpha = a + b\sqrt(d)$ with $b \neq 0$. We have to see what are the conditions on a and b for the minimal polynomial of α to be monic.

As for the minimal polynomial of α, we have $(\alpha - a)^2 = b^2 d$, so

$$f_\alpha = (x-a)^2 - b^2 d = x^2 - 2ax + (a^2 - b^2 d). \tag{1.5.1}$$

We see that $a \in \frac{1}{2}\mathbb{Z}$. Since $a^2 - b^2 d$ has to be integral, we see that no prime bigger than 2 can divide the denominator b_2 of $b = b_1/b_2$.

So we have to see which powers of 2 can divide b_2. Suppose that 2^n is the maximal power of 2 occurring in b_2. Then $2^2 n(a^2 - b^2 d)$ is a multiple of $2^2 n$. If $n > 1$, then $2^{2n}a^2 \equiv 0 \mod 4$, while by definition $2^2 n b^2 d \not\equiv 0 \mod 4$. So the difference of these two numbers cannot be a multiple of $2^2 n$. We conclude that as for a, we have $b \in \frac{1}{2}\mathbb{Z}$.

We certainly have $\mathbb{Z}[\sqrt{d}] \subseteq \mathcal{O}_K$. Suppose that it were bigger. Then because $a, b \in \frac{1}{2}\mathbb{Z}$, and because $\mathcal{O}_K$ is a ring, we could subtract appropriate elements in $\mathbb{Z}[\sqrt{d}]$ to end up with an integral element of the form

$$a_0 + b_0\sqrt{d} \tag{1.5.2}$$

with $a_0, b_0 \in \{0, 1/2\}$. Conversely, if we know which a_0, b_0 are possible, then the ring $\mathcal{O}_K$ can be obtained by adjoining these elements to $\mathbb{Z}[\sqrt{d}]$. We now check what is possible.

- The trivial case $a_0, b_0 = 0$ always occurs, but does not give anything new.

- The case $a_0 = 1/2, b_0 = 0$ gives the non-integer $1/2$, so this case does not occur.

- The case $a_0 = 0, b_0 = 1/2$ gives $1/2\sqrt{d}$. If this were integral, then so would its square be, which is $d^2/4$, in which case we obtain a contradiction with d being squarefree. So neither does this case occur.

- The case $a_0 = 1/2, b_0 = 1/2$ gives $(1 + \sqrt{d})/2$, which has minimal polynomial $x^2 - x + (1-d)/4$. This is integral if and only if $d \equiv 1 \mod 4$, in which case we have $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\sqrt{d} + \mathbb{Z}((1+\sqrt{d})/2) = \mathbb{Z} + \mathbb{Z}((1+\sqrt{d})/2)$ since $\sqrt{d} = 2((1+\sqrt{d})/2) - 1$.

We get

Theorem 1.5.2. *Let $d \neq 0, 1$ be a squarefree integer, and let K be the quadratic number field $\mathbb{Q}(\sqrt{d})$. Let $\alpha = \sqrt{d}$ if d is not congruent to 1 mod 4 and let $\alpha = (1+\sqrt{d})/2$ otherwise. Then $\mathcal{O}_K = \mathbb{Z}[\alpha]$.*

For a tremendous simplification of the proof of this theorem that shows the power of Kummer–Dedekind (Theorem 1.8.4), see Proposition 2.3.2.

1.6 Cyclotomic fields

Definition 1.6.1. Let n be a positive integer, and let K be a field. An n-th root of unity in K is an element ζ of K such that $\zeta^n = 1$. A primitive n-th root of unity in K is an element ζ of K such that $\zeta^n = 1$ and $\zeta^m \neq 1$ for $0 < m < n$. A cyclotomic field is a field that is generated over $\mathbb{Q}$ by a root of unity.

If we let $\zeta_n = \exp(2\pi/n) \in \mathbb{C}$, then ζ_n is a primitive n-th root of unity in $\mathbb{C}$.

Proposition 1.6.2. *The elements of $\mathbb{C}$ whose multiplicative order divides n are exactly the powers of ζ_n. Moreover, we have*

$$\prod_{i=0}^{n-1} (x - \zeta_n^i) = x^n - 1. \tag{1.6.1}$$

Proof. The given powers of ζ_n are distinct and all roots of $x^n - 1$, which as a polynomial of degree n admits at most n roots. □

Evaluating cleverly yields lots of identities for the n-th roots of unity. For example, we have

$$\prod_{i=1}^{n-1} (x - \zeta_n^i) = (x^n - 1)/(x - 1) = \sum_{i=0}^{n-1} x^i. \tag{1.6.2}$$

Evaluating at a non-trivial n-th root of 1, call it ζ, we get:

$$\sum_{i=0}^{n-1} \zeta^i = 0 \tag{1.6.3}$$

Evaluate at 0 for

$$\prod_{i=0}^{n-1} (-\zeta_n^i) = 1 \tag{1.6.4}$$

and at 1 for

$$\prod_{i=0}^{n-1} (1 - \zeta_n^i) = n. \tag{1.6.5}$$

We define the cyclotomic polynomial Φ_n be the result of removing from $x^n - 1$ the factors that already divide $x^m - 1$ for a proper divisor m of n. So

$$\Phi_n = \frac{x^n - 1}{\operatorname{lcm}\{x^m - 1 : m | n, m \neq n\}} = \prod_{(i,n)=1} (x - \zeta_n^i). \tag{1.6.6}$$

This is a polynomial with coefficients in $\mathbb{Q}$, whence in fact in $\mathbb{Z}$ because the ζ_n^i are algebraic integers. You can prove by using the inclusion-exclusion principle (or by ordering n-th roots of unity by their multiplicative order):

Proposition 1.6.3. *We have*

$$\Phi_n = \frac{x^n - 1}{\prod_{m|n} \Phi_m}, \tag{1.6.7}$$

and Φ_n has degree $\varphi(n) = (\mathbb{Z}/n\mathbb{Z})^*$.

We still have that ζ_n is a root of Φ_n, and since no obvious factors remain, we want to prove that Φ_n is irreducible. For this, we gather some information about the primes where its roots coincide.

Proposition 1.6.4. *Let $d = [\mathbb{Q}(\zeta_n) : \mathbb{Q}]$, and let B be the basis $\{1, \ldots, \zeta_n^{d-1}\}$ of $\mathbb{Q}(\zeta_n)$. Then $\Delta_B(\mathbb{Q}(\zeta_n))$ divides n^n.*

Proof. We have

$$\Delta_B(\mathbb{Q}(\zeta_n)) = \prod_S (\zeta_n^i - \zeta_n^j)^2 \tag{1.6.8}$$

for some some subset S of the pairs (i, j) with $0 \leq i, j \leq n - 1$ and $i < j$. But up to sign, we can use the relations derived above to see that the full product equals

$$\begin{aligned}\prod_{i<j} (\zeta_n^i - \zeta_n^j)^2 &= \prod_{i,j=0}^{n-1} (\zeta_n^i - \zeta_n^j) = \prod_{i=0}^{n-1} \zeta_n^i \prod_{j=0}^{n-1} (1 - \zeta_n^{j-i}) \\ &= \prod_{i=0}^{n-1} \zeta_n^i \prod_{j=0}^{n-1} (1 - \zeta_n^k) = \prod_{i=0}^{n-1} \zeta_n^i \prod_{j=0}^{n-1} n = n^n.\end{aligned} \tag{1.6.9}$$

So we have a division relation $\Delta_B(\mathbb{Q}(\zeta_n))|n^n$ in $\mathbb{Q}(\zeta_n)$. We should show that this gives a division relation in $\mathbb{Z}$. Fortunately it does. Indeed, the quotient of the two quantities is a product of factors $\zeta_n^i - \zeta_n^j$, and these elements are in $\mathcal{O}_{\mathbb{Q}(\zeta_n)}$. Therefore so is their product, which since it is in $\mathbb{Q}$ as well actually belongs to $\mathcal{O}_{\mathbb{Q}(\zeta_n)} \cap \mathbb{Q} = \mathbb{Z}$. □

Theorem 1.6.5. *Φ_n is irreducible. In particular, $\mathbb{Q}(\zeta_n)$ has degree $\varphi(n)$ over $\mathbb{Q}$.*

Proof. Again let f be the minimal polynomial of the algebraic integer ζ_n. Then f is monic and integral and $f|\Phi_n$ in $\mathbb{Q}[x]$.

The roots of Φ_n are exactly the ζ_n^k with $(k, n) = 1$. Then $k = \prod_i p_i^{n_i}$ with p_i primes such that $(p_i, n) = 1$. So by symmetry it suffices to show that if p is prime and $(p, n) = 1$, then ζ_n^p is again a root of f. If this were not the case, then for some subset I of $\{0, \ldots, n - 1\}$ we would have

$$0 \neq f(\zeta_n^p) = \prod_{i \in I} (\zeta_n^p - \zeta_n^i)|n^n. \tag{1.6.10}$$

However, we also know that $f(x^p) = f(x)^p$ modulo $p\mathbb{Z}[x]$, since (miraculously enough) this is true for any polynomial modulo p. Evaluating, we get $f(\zeta_n^p) = f(\zeta_n) = 0$ modulo $p\mathbb{Z}[\zeta_n]$. But this would imply that p divides n^n in $\mathbb{Z}[\zeta_n]$. Taking norms, we get that a power of p divides a power of n^n, but by unique factorization in $\mathbb{Z}$, this is impossible from our assumption that p did not divide n. □

The following result is true in general. A beautiful proof for $n = p$ prime is given in [1, Theorem 4.3].

Theorem 1.6.6. *We have $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$.*

Why consider cyclotomic fields at all? The first motivation is that along with quadratic fields, cyclotomic fields have the property that their ring of integers is easy to determine. This is far from being true for general fields. Moreover, certain special number fields (those with abelian Galois group) embed into cyclotomic fields, and one can use the friendliness of cyclotomic fields to get a grip on these number fields. As an example, we show that every quadratic field can be embedded into a cyclotomic field.

Theorem 1.6.7. *Using the Legendre symbol $(\cdot/p)$, let*

$$S = \sum_{n=0}^{p-1} (n/p)\zeta_p^n. \tag{1.6.11}$$

Then $S^2 = (-1/p)p$.

Proof. See [2]. □

Corollary 1.6.8. *Every quadratic field can be embedded into a cyclotomic field.*

Proof. This is Exercise 4 of Assignment 3 in the exercise section. □

For a typical fields of degree 3 or higher, such an embedding does not exist, because it implies that the Galois group is abelian.

1.7 Unique factorization of ideals

We have seen that usually number rings do not admit unique factorization. Examples of this are in the practice section of the notes, and also in the exercises. Or goal in this section is to show that if the number ring we are considering is the *full* ring of integers of a number field, then we can still save the situation by considering factorizations of *ideals* instead of *elements* of a number ring. This even makes the statement of the unique factorization property much more natural, since units are no longer involved.

Ideals will be familiar to you from previous courses on rings and groups. Basically, everything that can be done multiplicatively with elements of a ring, and all interesting notions involved, such as gcds and lcms, can be defined on the level of ideals (also see the exercises for this). The fact that ideals can be manipulated so naturally and that they manage to correct the problem so wonderfully will hopefully convince you that they are much more logical objects to consider than irreducible elements, and that being a UFD is more a fortunate property than an essential one in algebraic number theory.

We can without any further problems show that unique factorization holds in a generalization of the ring of integers of a number field called a Dedekind domain. For this, we need a slightly technical preamble first.

1.7.1 Noetherian rings and Noetherian induction

Definition 1.7.1. Let R be a ring. Then R is called Noetherian if any chain of inclusions of ideals

$$I_1 \subseteq I_2 \ldots \subseteq I_n \subseteq \ldots \tag{1.7.1}$$

stabilizes at some point, in the sense that there exists an integer N such that for all $n > N$ we have $I_{n+1} = I_n$.

This is a notion that should actually be defined on the level of modules, but that is a subject matter for a course on commutative algebra.

Proposition 1.7.2. *A ring R is Noetherian if and only if every ideal of R is finitely generated.*

Proof. Suppose first that every ideal is finitely generated. Consider a chain of inclusions $I_1 \subseteq I_2 \subseteq \dots$ and construct the set $I = \cup_{i=1}^{\infty}$. This is an R-ideal, hence finitely generated. Take $a_1, \dots, a_n$ of I. Then for every i, there exists an N_i such that $a_i \in I_{N_i}$. Taking the maximum N of the N_i, we see that all the a_i are in I_N. Hence $I = I_N$, and the chain stops at N.

Conversely, suppose that R is Noetherian, and let I be an ideal of R. We first give a proof that is wrong in general, to show the subtlety of the argument.

Choose generators $a_1, a_2, \dots$ of I and let $I_n = (a_1, \dots, a_n)$. We get an ascending chain of ideals. Let N is such that $I_N = I_{N+1} = \dots$. Then $I = I_N = (a_1, ..., a_N)$, so I is finitely generated.

This argument works for number rings, but not for general rings, because it assumes that I is countably generated. We are instead going to apply Zorn's lemma (so beware, oh ye haters of the axiom of choice).

Consider the set S consisting of the ideals J of R such that J is finitely generated and $J \subseteq I$. Then every subset of S has an upper bound, because if not, we would get an infinite properly ascending chain of ideals, which contradicts the fact that R is Noetherian. So by Zorn's lemma, there exists a maximal element K of S. We want that $K = I$. If not, then take $r \in I \backslash K$. Then the ideal generated by K and r is also in S, but strictly larger than K. Contradiction. □

The technique at the end of the previous proof is called Noetherian induction. It is extremely useful, and we will see it recur lots of times.

1.7.2 Dedekind domains

Now we can give the following definition.

Definition 1.7.3. Let R be a ring. Then R is called a Dedekind domain if

(D0) R is an integral domain;

(D1) R is Noetherian;

(D2) R is integrally closed in its field of fractions;

(D3) Every non-zero prime ideal of R is maximal.

Proposition 1.7.4. *Let K be a field. Then K is a Dedekind domain.*

Proof. (D0) and (D2) are trivial. As for (D1) and (D3), these are implied by the fact that every non-zero ideal is all of K. □

Proposition 1.7.5. *Let K be a number field, and let $\mathcal{O}_K$ be the ring of integers of K. Then $\mathcal{O}_K$ is a Dedekind domain.*

Proof. (D0) : $\mathcal{O}_K$ is a subring of a field.

(D1) : I_1 be a non-zero ideal of $\mathcal{O}_K$. Then the exercises show that $I_1 \cap \mathbb{Z}$ contains a non-zero element. Say that $n \in I_1 \cap \mathbb{Z}$. Then $(n) = n\mathcal{O}_K \subseteq I_1$, So $\mathcal{O}_K / I_1$ is a quotient of $\mathcal{O}_K / n\mathcal{O}_K$. This is a finite ring. Hence there are finitely many ideals between I_1 and R, and no infinite ascending chains starting with I_1 exist. Since I_1 was arbitrary, we are done.

(D2) : Exercise 6 of Assignment 1 in the exercise section shows that every element of K is of the form r/n, with $r \in \mathcal{O}_K$ and $n \in \mathbb{N} \subseteq \mathcal{O}_K$. So K is the field of fractions of $\mathcal{O}_K$, and we have seen in Proposition 1.3.11 that $\mathcal{O}_K$ is integrally closed in K.

(D3) : Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$. Then $\mathcal{O}_K/\mathfrak{p}$ is a finite integral domain. So if $r \in \mathcal{O}_K/\mathfrak{p}$ is non-zero, then multiplication with r is an injective map. It is therefore a bijection since $\mathcal{O}_K/\mathfrak{p}$ is finite. Hence r admits an inverse, $\mathcal{O}_K/\mathfrak{p}$ is a field, and $\mathfrak{p}$ is maximal. □

We have also proved:

Proposition 1.7.6. *Let R be a number ring. Then R satisfies the properties (D0),(D1),(D3).*

We now give some counterexamples to the properties (D0),(D1),(D2),(D3). Contrary to the univariate polynomial ring over $\mathbb{C}$, the ring $\mathbb{C}[x,y]$ in two variables satisfies (D0),(D1),(D2), but not (D3). The ring $\mathbb{Z}[\sqrt{19}]$ satisfies (D0),(D1),(D3), but not (D2). The integral closure $\overline{\mathbb{Z}}$ over $\mathbb{Z}$ in $\mathbb{C}$ satisfies (D0),(D2),(D3), but not (D1). Finally, the ring of infinitesimals $\mathbb{C}[x]/(x^2)$ satisfies (D1),(D2),(D3), but not (D0).

1.7.3 Inversion

As mentioned above, at least on the multiplicative level ideals can be manipulated like ordinary numbers. Given two ideals I and J, we can form their product IJ, their sum $I + J$ (which actually corresponds to their gcd, see Exercise 2 of Assignment 3 in the exercise section), and their intersection $I \cap J$ (which is actually an lcm). One can also define inverses for ideals, to which we turn now. The miracle is that for Dedekind domains these inverses do exactly what we want.

Let I be an ideal of R. Then an inverse of J should be an ideal J such that $IJ = R$. Since $IJ \subseteq I$, if we work with ideals of R itself, then only the unit ideal $(1) = R$ is invertible. We need to generalize our notion of ideal.

Definition 1.7.7. Let R be an integral domain with fraction field K. A fractional ideal of R is a subset I of K such that

(i) I is an abelian group under addition;

(ii) $RI = \{ri : r \in R, i \in I\} = I$;

(iii) There exists a non-zero $x \in R$ such that $xI \subseteq R$.

The final condition prevents I from being too exotic. For number fields, this statement can be made precise in the following sense.

Proposition 1.7.8. *Suppose that R is a number ring with field of fractions K. Let I be a subset of K. Then I is a fractional ideal of R if and only if*

(i) I is an abelian group under addition;

(ii) $RI = \{ri : r \in R, i \in I\} = I$;

(iii) I is finitely generated as an abelian group.

Proof. If there exists an $\alpha \in K$ such that $\alpha I \subseteq R$ then αI is finitely generated as an abelian group because it is a subgroup R, and R is finitely generated as an abelian group. Indeed, it is a subgroup of the abelian group $\mathcal{O}_K$, which is finitely generated by Theorem 1.4.4. Hence $I = \alpha^{-1}(\alpha I)$ is also finitely generated.

Conversely, if I is finitely generated as an abelian group, then choose generators $q_1, \ldots, q_k$ with $q_i \in K$. We have seen that there exist integers n_i such that $n_i q_i \in R$. Let n be the product of the n_i. Then nq_i is in R for all i, so $nI \subseteq R$. □

The fundamental and motivating example of a fractional ideal is the following.

Example 1.7.9. Let $a \in R$ be an element of a domain R. Then the subset $(a^{-1}) := a^{-1}R$ of K is a fractional ideal of R.

Example 1.7.10. Let R be a domain, and let $I = (a)$ be a principal ideal of R. Then if we let $J = (a^{-1})$, we have $IJ = aRa^{-1}R = aa^{-1}RR = R$. This has the important consequence that we can characterize J intrinsically as $J = \{\alpha \in K : \alpha I \subseteq R\}$.

Indeed, if $c \in J$, then $c = a^{-1}r$ for some $r \in R$, and if $b \in I$ then $b = as$ for some $s \in R$, so $bc = rs$ is an element of R. Conversely, suppose that $\alpha \in K$ is such that $\alpha I \subseteq R$. Then $\alpha a = r \in R$, and $\alpha = a^{-1}r$, which is in J.

This motivates

Notation 1.7.11. Let I be a fractional ideal of a domain R. Then we define the inverse ideal I^{-1} of I by

$$I^{-1} = \{\alpha \in K : \alpha I \subseteq R\}. \tag{1.7.2}$$

Example 1.7.12. Let R be a Dedekind ring, and let $I = (a)$ be a principal ideal of R. Then we just saw that $I^{-1} = (a^{-1})$. The same is true if $a \in K$, in which case $(a) = aR \subset K$ is a fractional ideal.

Proposition 1.7.13. *Let R be a Dedekind domain. Then if I is a non-zero fractional ideal of R, so is I^{-1}.*

Proof. It suffices to verify property (iii). Choose $a \in I$ non-zero. Then $(a) \subseteq (I)$, so (check this yourself!) $I^{-1} \subseteq (a)^{-1} = (a^{-1})$. Then $aI^{-1} \subset R$. □

If any decent inverse for an ideal I exists, then it has to be the I^{-1} that we just defined:

Proposition 1.7.14. *Let I be a fractional ideal of R. If there exists an ideal J such that $IJ = R$, then $J = I^{-1}$.*

Proof. Certainly $J \subseteq I^{-1}$. So suppose that $\alpha \in I^{-1}$. There exist elements i_k of I and j_k of J such that $\sum_k i_k j_k = 1$. Then $\alpha = \sum_k (i_k j_k)\alpha = \sum_k (\alpha i_k) j_k \in J$. □

Definition 1.7.15. Let I be a fractional ideal of a domain R. Then I is called invertible if $II^{-1} = I^{-1}I = R$. By the above, this is the case if and only if $IJ = JI = R$ for *some* fractional ideal J of R.

Right now, we only know that $II^{-1} = I^{-1}I = R$ for principal ideals I. So far we therefore only know these ideals to be invertible.

1.7.4 Group structure

We now prove that for Dedekind rings, inverses do the job they are supposed to do, and that they make the monoid of fractional ideals into a group. We need the following lemma.

Lemma 1.7.16. *Let I be an ideal of a Noetherian ring R. Then there exist prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ of R (not necessarily distinct) such that $\mathfrak{p}_1 \cdots \mathfrak{p}_n \subseteq I$.*

Proof. Suppose that I is maximal as an exception. Then I is not prime. So suppose that a, b are not in I but ab is. Let $J_a = I + (a)$ and let $J_b = I + (b)$. These ideals properly contain I. So $\mathfrak{p}_1 \cdots \mathfrak{p}_n \subseteq J_a$ and $\mathfrak{q}_1 \cdots \mathfrak{q}_m \subseteq J_b$ for certain prime ideals $\mathfrak{p}_i$ and $\mathfrak{q}_j$. Then $\mathfrak{p}_1 \cdots \mathfrak{p}_n \mathfrak{q}_1 \cdots \mathfrak{q}_m$ is contained in $J_a J_b = (I + (a))(I + (b)) = I^2 + aI + bI + (ab) \subseteq I$, and we are done.

Assuming, of course, that such an I exists. Here we use Noetherian induction. Indeed, if there were no maximal exception I, then we would get an infinite ascending chain of ideals. □

We can now show that inverse do what they are supposed to do.

Theorem 1.7.17. *Let R be a Dedekind ring. Then the set of fractional ideals* $\mathrm{Id}(R)$ *of R forms an abelian group, with multiplication given by $(I, J) \mapsto IJ$ and inversion given by $I \mapsto I^{-1}$.*

Proof. We follow Stein's wonderful proof in [4, Theorem 3.1.6]. First we show that inversion works for prime ideals $\mathfrak{p}$ of R. Note that $\mathfrak{p}^{-1} \supseteq R$ for such a prime ideal. We try to find more about the fractional ideal $\mathfrak{p}^{-1}$.

(i) $\mathfrak{p}^{-1}$ strictly contains R. To show this, let a be an element of $\mathfrak{p}$, and using the Lemma above (and hence invoking (D1)) choose $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ such that $\mathfrak{q}_1 \cdots \mathfrak{q}_n \subseteq (a) \subseteq \mathfrak{p}$. Suppose that the n is minimal among all such expressions. Then one of the $\mathfrak{q}_i$, say $\mathfrak{q}_1$, is contained in $\mathfrak{p}$. (If not, then we could construct $a_i \in \mathfrak{q}_i \backslash \mathfrak{p}$ for all i, in which case $a_1, \ldots, a_n$ are not in $\mathfrak{p}$, but their product is, a contradiction to $\mathfrak{p}$ being prime.) We now know that $\mathfrak{q}_1 = \mathfrak{p}$ by (D3). By the minimality of the expression, we can find a b in $\mathfrak{q}_2 ... \mathfrak{q}_n$ that is not in (a). Then $\mathfrak{q}_1(b) \subseteq (a)$, so $\mathfrak{p}(b) \subseteq (a)$. Let $\alpha = b/a$ (which implicitly uses (D0)). Then α is the requested element of $\mathfrak{p}^{-1} \backslash R$. Indeed, α is in $\mathfrak{p}^{-1}$ because $\alpha\mathfrak{p} = a^{-1} b \mathfrak{p} \subseteq a^{-1}(a) = R$, and it is not in $\mathcal{O}_K$ because then b would be in (a).

(ii) $\mathfrak{p}^{-1}\mathfrak{p}$ is either $\mathfrak{p}$ or R. Indeed, by definition $\mathfrak{p}^{-1}\mathfrak{p} \subseteq R$. Also $\mathfrak{p} \subseteq \mathfrak{p}^{-1}\mathfrak{p}$ since $R \subseteq \mathfrak{p}^{-1}$. So if $\mathfrak{p}^{-1}\mathfrak{p}$ does not equal R, then it equals $\mathfrak{p}$ by (D3).

(iii) $\mathfrak{p}^{-1}\mathfrak{p}$ does not equal $\mathfrak{p}$. Because if it did, then consider our $\alpha \in \mathfrak{p}^{-1} \backslash R$. Then α maps P to itself under multiplication. If $R = \mathcal{O}_K$ for a number field K, then $\mathfrak{p}$ is a subgroup the finitely generated abelian group $\mathcal{O}_K$, so choosing a $\mathbb{Z}$-basis for $\mathfrak{p}$ we can represent (multiplication by) α by a matrix with integral coefficients. The characteristic polynomial of this matrix vanishes in α, so α would be in $\mathcal{O}_K$ because of (D2). For more general R, essentially the same proof works, except that one takes a set of generators of $\mathfrak{p}$ as an R-module. This is slightly trickier because $\mathfrak{p}$ may not be a free module, but the result still goes through.

Now we can show that inversion works for ideals I of R. Choose a prime $\mathfrak{p}$ containing I. Then $I \subseteq \mathfrak{p}^{-1} I \subseteq \mathfrak{p}^{-1}\mathfrak{p} = \mathcal{O}_K$. We cannot have $I = \mathfrak{p}^{-1} I$ (use δ as before). Now we use Noetherian induction. Suppose that I is a maximal exception. Then $J = \mathfrak{p}^{-1} I$ does have an inverse J^{-1}. We now have $(J^{-1}\mathfrak{p}^{-1})I = (J^{-1}\mathfrak{p}^{-1})RI = (J^{-1}P^{-1})\mathfrak{p}(\mathfrak{p}^{-1}I) = (J^{-1}\mathfrak{p}^{-1})\mathfrak{p}J = J^{-1}(\mathfrak{p}^{-1}\mathfrak{p})J = J^{-1}J = R$, so by Proposition 1.7.14 $I^{-1} = J^{-1}\mathfrak{p}^{-1}$ and $I^{-1}I = R$.

Finally, let I be a fractional ideal of R, and choose $x \in K$ such that $xI = I_0 \subseteq R$. Then I_0 is an ideal of R. We can repeat the uniqueness argument to see that I is invertible, with inverse xI_0^{-1}. □

The hard work is now done, and the rest of the section is just wrapping up.

1.7.5 The main theorem, at last

Theorem 1.7.18 (Unique factorization of ideals)**.** *Let R be a Dedekind ring, and let I be a non-zero ideal of R. Then there exist distinct prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ of R and exponents $e_i \in \mathbb{Z}_{\geq 1}$ such that*

$$I = \prod \mathfrak{p}_i^{e_i}. \tag{1.7.3}$$

The ideals $\mathfrak{p}_i$ are uniquely determined up to permuting the indices.

Proof. First we show the existence of such a factorization by using Noetherian induction. Let I be a maximal exception. Then I is not prime. We can choose a prime $\mathfrak{p}$ containing I. Now $I\mathfrak{p}^{-1} \subseteq \mathfrak{p}\mathfrak{p}^{-1} = R$, and $I\mathfrak{p}^{-1}$ does not equal I because then we could cancel under the group law and obtain $\mathfrak{p}^{-1} = R$. So $J = I\mathfrak{p}^{-1}$ strictly contains I. Write $J = \mathfrak{q}_1 \cdots \mathfrak{q}_m$, then we have $I = \mathfrak{p}J = \mathfrak{p}\mathfrak{q}_1 \cdots \mathfrak{q}_m$, and by gathering the factors we get our factorization

Now for the uniqueness. Suppose that we have an equality

$$\mathfrak{p}_1 \cdots \mathfrak{p}_m = \mathfrak{q}_1 \cdots \mathfrak{q}_m \tag{1.7.4}$$

for prime ideals $\mathfrak{p}_i$ and $\mathfrak{q}_j$. Then $\mathfrak{p}_1 \subseteq \mathfrak{q}_1$ because otherwise we could again find $a_i \in \mathfrak{p}_i \backslash \mathfrak{q}_1$ whose product is in $\prod_i \mathfrak{p}_i = \prod_j \mathfrak{q}_j \subseteq \mathfrak{q}_1$. But then $\mathfrak{p}_1 = \mathfrak{q}_1$ by (D3). We can then cancel and conclude by induction. □

Corollary 1.7.19. *Let I and J be ideals of a Dedekind ring R. Then I divides J in the abelian group* $\mathrm{Id}(R)$ *if and only if I contains J. More precisely, we have that I contains J if and only if there exists another ideal K of R such that $J = IK$.*

Proof. This is a useful exercise. □

Theorem 1.7.20. *Let R be a Dedekind ring, and let I be a fractional ideal of R. Then there exist distinct prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ of R and exponents $e_i \in \mathbb{Z}$ such that*

$$I = \prod \mathfrak{p}_i^{e_i}. \tag{1.7.5}$$

The ideals $\mathfrak{p}_i$ are uniquely determined up to permuting the indices.

Proof. This is a useful exercise! □

This all works because ideals in Dedekind rings are all invertible, which is a very special property indeed. In fact, we will show the the following in Section 3.1.

Fact 1.7.21. *Let R be a proper subring of the ring of integers $\mathcal{O}_K$ of a number field K. Then R contains non-invertible prime ideals.*

1.8 The Kummer–Dedekind theorem

We return to the rings of integers $\mathcal{O}_K$ of number fields K. So far, we have not indicated how to contruct interesting non-principal ideals. And after our unique factorization result, we are of course particularly interested in explicitly obtaining prime ideals, which for all we know may not be principal.

So let us consider a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$. Then the exercises show that $\mathfrak{p} \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$, hence generated by a rational prime p. We say that $\mathfrak{p}$ lies over p. So $\mathfrak{p}$ corresponds to a prime ideal of $\mathcal{O}_K/p\mathcal{O}_K$. We can get our hands on the prime ideals of $\mathcal{O}_K$ by

(i) Running over the integral primes p and then

(ii) For fixed p, determine the prime ideals of $\mathcal{O}_K/p\mathcal{O}_K$.

So let p be fixed. The ring $\mathcal{O}_K/p\mathcal{O}_K$ may seem difficult to describe if the ring of integers is not of the form $\mathbb{Z}[\alpha]$. But we can often exploit these subring to determine the structure of $\mathcal{O}_K/p\mathcal{O}_K$. Recall that by using the discriminant, we can find out which primes can divide the index $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$. The following result is therefore useful.

Proposition 1.8.1. *Let $\mathbb{Z}[\alpha]$ be an order of K defined by an integral generator of the extension $K|\mathbb{Q}$. Suppose that $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$ is coprime with p, and let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be the primes of $\mathbb{Z}[\alpha]$ over p. Then $\mathfrak{p}_1\mathcal{O}_K, \ldots, \mathfrak{p}_n\mathcal{O}_K$ are the primes of $\mathcal{O}_K$ over p.*

Proof. Choose a $\mathbb{Z}$-basis B for $\mathbb{Z}[\alpha]$ and another $\mathbb{Z}$-basis B' for $\mathcal{O}_K$. Then the elements of B can be expressed in terms of those of B'. This gives rise to a matrix M with entries in $\mathbb{Z}$ such that $B = MB'$. The determinant of M equals $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$, as we have seen using the Smith normal form. Under the hypothesis of the proposition, M will be invertible modulo p. Therefore the inclusion $\mathbb{Z}[\alpha] \to \mathcal{O}_K$ factors to a bijection an isomorphism $\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] \cong \mathcal{O}_K/p\mathcal{O}_K$. Now use the correspondences between ideals containing p and ideals of the quotients. □

Note that if we find generators for the primes $\mathfrak{p}_i \subseteq \mathbb{Z}[\alpha]$, then the primes $\mathfrak{p}_i\mathcal{O}_K$ of $\mathcal{O}_K$ are generated by the same elements. Now it turns out that for order of the form $\mathbb{Z}[\alpha]$, the primes over p are simple to describe.

Proposition 1.8.2. *Let $\mathbb{Z}[\alpha]$ be as before, and let f be the minimal polynomial of α. Then the ideals of $\mathbb{Z}[\alpha]$ containing p are in bijective correspondence with the irreducible factors of the reduction $\overline{f} \in (\mathbb{Z}/p\mathbb{Z})[x]$ of f modulo p. To such a factor $\overline{g}$ corresponds the ideal $(p, g(\alpha))$, where $g \in \mathbb{Z}[x]$ is a lift of $\overline{g}$ in the sense that it reduces to $\overline{g}$ modulo p.*

Proof. We have to determine the prime ideals of $\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] = \mathbb{Z}[x]/(p, f) = (\mathbb{Z}/p\mathbb{Z})[x]/(\overline{f})$. Since $\mathbb{Z}/p\mathbb{Z}$ is a field, the ring $(\mathbb{Z}/p\mathbb{Z})[x]$ is a UFD. It is also a PID, as one shows using division with remainder. And every prime is maximal, because as we saw a finite integral domain is a field. The prime ideals in $(\mathbb{Z}/p\mathbb{Z})[x]$ therefore correspond to irreducibles, and the prime ideals containing $\overline{f}$ to the irreducible factors of $\overline{f}$. Tracing through the correspondences between ideals of $(\mathbb{Z}/p\mathbb{Z})[x]/(\overline{f})$ and ideals of $\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha]$, we obtain the proposition. □

Combining this result with the previous result, we see that for all but finitely many primes p, the prime ideals of $\mathcal{O}_K$ above p are generated by two elements. This turns out to be true for *any* ideal of $\mathcal{O}_K$, and can be proved using the Chinese remainder theorem. We do not concern ourselves with these and refer to Stein [4].

Another way to look at this theorem is as follows. Any prime ideal $\mathfrak{p}$ of $\mathbb{Z}[\alpha]$ is the kernel of the corresponding projection $\mathbb{Z}[\alpha] \to \mathbb{Z}[\alpha]/\mathfrak{p}$. The theorem explicitly describes what this evaluation morphism is: it sends α to $x \bmod \overline{g}$. In the simple case where $\overline{g} = x - r$ for some $r \in \mathbb{Z}/p\mathbb{Z}$, the prime is therefore nothing but the kernel of the map $\mathbb{Z}[\alpha] \to \mathbb{Z}/p\mathbb{Z}$ that sends α to r. The fact is very useful when trying to calculate with prime ideals, as we will see in Chapter 2.

The behavior of f modulo p gives important information about invertibility of the primes involved. Before giving the main theorem of Kummer–Dedekind, which contains all information that one could desire in this regard, we do a simple case first.

Proposition 1.8.3. *Let $\mathbb{Z}[\alpha]$ be an order of K defined by an integral generator of the extension $K|\mathbb{Q}$, and let f the minimal polynomial of α. Let $\mathfrak{p}$ be an ideal of $\mathbb{Z}[\alpha]$ lying over the rational prime p. Suppose that p does not divide $\Delta(f)$. Then $\mathfrak{p}$ is invertible in $\mathbb{Z}[\alpha]$, and $\mathfrak{p}\mathcal{O}_K$ is invertible in $\mathcal{O}_K$.*

Proof. By Proposition 1.4.11, the fact that p does not divide $\Delta(f) = \prod_i(\alpha_i - \alpha_j)^2$ means that the roots of f remain distinct mod p. That is, $\overline{f}$ does not have multiple factors. So let g be a lift of an arbitrary irreducible factor $\overline{g}$ of $\overline{f}$. Write $f = gh + pr$, with $g, r \in \mathbb{Z}[x]$. I claim that the ideal $\mathfrak{p} = (p, g(\alpha))$ of $\mathbb{Z}[\alpha]$ has inverse $(p^{-1}h(\alpha), 1)$. Indeed, we have $p^{-1}h(\alpha)p = h(\alpha)$, $p^{-1}h(\alpha)g(\alpha) = -r(\alpha)$ because $f(\alpha) = 0$, and $1 \cdot p = p$, $1 \cdot g(\alpha) = g(\alpha)$, so the product is contained in $\mathbb{Z}[\alpha]$. Its elements generate $\mathbb{Z}[\alpha] = \mathbb{Z}[x]/(f)$, because $p, g(\alpha), h(\alpha)$ do; the image of $\overline{g}$ and $\overline{h}$ of $g(\alpha)$ and $h(\alpha)$ under the isomorphism $\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] \cong (\mathbb{Z}/p\mathbb{Z})[x]/(f)$ are coprime by hypothesis, so they generate the unit ideal of $(\mathbb{Z}/p\mathbb{Z})[x]/(f)$.

Extending these ideals to $\mathcal{O}_K$, their product is still contained in $\mathcal{O}_K$ and still contains 1, so the statement is also true for these extensions. □

The big theorem in this context, and perhaps the most useful tool for calculations, is the following.

Theorem 1.8.4 (Kummer–Dedekind)**.** *Let K be a number field with ring of integers $\mathcal{O}_K$. Let $\mathbb{Z}[\alpha]$ be an order of K defined by an integral generator of the extension $K|\mathbb{Q}$. Let f be the minimal polynomial of α, let p be a rational prime, and let $\overline{f}$ be the reduction of f modulo p. Let*

$$\overline{f} = \prod_{i=1}^{n} \overline{g}_i^{e_i} \tag{1.8.1}$$

be the factorization of $\overline{f}$ into powers of distinct irreducibles $\overline{g}_i \in (\mathbb{Z}/p\mathbb{Z})[x]$.

(0) The prime ideals of $\mathbb{Z}[\alpha]$ over p are in one-to-one correspondence with the irreducible factors $\overline{g}_i$ of $\overline{f}$. To a factor $\overline{g}_i$ corresponds to prime ideal $(p, g_i(\alpha))$ of $\mathbb{Z}[\alpha]$, where $g_i \in \mathbb{Z}[x]$ is a lift of $\overline{g}_i$.

(1) Let $\overline{g}_i$ be a factor of $\overline{f}$, with associated monic lift g_i. Write $f = q_i g_i + r_i$ with q_i, r_i in $\mathbb{Z}[x]$, and let $\mathfrak{p}_i = (p, g_i(\alpha))$ be the prime ideal of $\mathbb{Z}[\alpha]$ corresponding to $\overline{g}_i$. Then $\mathfrak{p}_i$ is invertible unless both the following statements hold:

(i) $e_i > 1$, and

(ii) $r_i \in p^2\mathbb{Z}[x]$.

(2) We have an inclusion

$$(p) \supseteq \prod_{i=1}^{n} \mathfrak{p}_i^{e_i}, \tag{1.8.2}$$

with equality occurring if and only if all the $\mathfrak{p}_i = (p, g_i(\alpha))$ above p are invertible. If this is the case, then the ideals of $\mathcal{O}_K$ over p are the extensions $\mathfrak{p}_i\mathcal{O}_K$, and the prime p does not divide the index $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$. Moreover, the norm of the ideal $\mathfrak{p}_i$, that is, the index of abelian groups $[\mathcal{O}_K : \mathfrak{p}_i]$, equals $p^{\deg(g_i)}$.

(3) If one of the $\mathfrak{p}_i$ is not invertible, then let $\beta_i = q_i(\alpha)/p$. Then $\beta_i \in \mathcal{O}_K \backslash \mathbb{Z}[\alpha]$.

We have proved part (0) of the theorem, and we postpone the proof of parts (1) and (2) to Section 3.1. We prove (3) here. To show that β_i is in $\mathcal{O}_K$, it suffices to show that β_i maps the finitely generated abelian group $\mathfrak{p}_i\mathcal{O}_K$ to itself, because then β_i is a zero of its integral characteristic polynomial for this action. (Alternatively, we will have $(\beta_i)\mathfrak{p}_i\mathcal{O}_K = \mathfrak{p}_i\mathcal{O}_K$, so $\beta_i \in \mathcal{O}_K$ after cancelling $\mathfrak{p}_i\mathcal{O}_K$ on both sides, which is possible because $\mathcal{O}_K$ is a Dedekind ring.)

For this, it in turn suffices to show that β_i maps the generators of $\mathfrak{p}$ into itself. First consider $\beta_i p = q_i(\alpha)$. After reducing modulo p, the element $q_i(\alpha)$ corresponds to the polynomial $\overline{f}/\overline{g}_i$. The property (1)(i) shows that this polynomial still contains a factor $\overline{g}_i$. In other words, the reduction modulo p of the element $q_i(\alpha)$ is a multiple of the reduction modulo p of the element $g_i(\alpha)$. But this means that $q_i(\alpha)$ is in the ideal generated by p and $g_i(\alpha)$.

Now consider $\beta_i g_i(\alpha)$. By evaluating the equality $f = q_i g_i + r_i$ at α, we see that $q_i(\alpha)g_i(\alpha)$ equals $-r_i(\alpha)$. So $\beta_i = (q_i(\alpha)g_i(\alpha))/p$ equals $-r_i(\alpha)$, which by (1)(ii) is a multiple of p. We are done.

We see that the theorem shows how we can enlarge the ring of integers of we started out with a small subring. We will do this systematically in Section 2.3.

1.9 UFDs, PIDs, and Euclidean domains

This section considers the situation in which there is no obstruction to unique factorization of elements. We show that for Dedekind domains, such as the ring of integers in a number field, this property, being a unique factorization domain (UFD) is equivalent to an a priori much stronger notion, namely that of being a principal ideal domain (PID). We then briefly consider Euclidean domains, a special subclass of PIDs.

1.9.1 UFDs

Definition 1.9.1. Let R be a ring, and let a be a non-zero element of R that is also not a unit. Then a is called irreducible if for any product decomposition $a = rs$ in R we either have $r \in R^*$ or $s \in R^*$. The element a is called prime if it generates a prime ideal.

Example 1.9.2. Let $R = \mathbb{Z}[\sqrt{-19}]$, and let $a = 2$. Then a is irreducible because $\mathrm{nm}(a) = 4$ and no element of norm 2 exists in R, since $\mathrm{nm}(x + y\sqrt{-19}) = x^2 - 19y^2$ never equals 2. But a is not prime because $1 + \sqrt{-19}$ and $1 - \sqrt{-19}$ are not multiples of 2 in R, and $(1 + \sqrt{-19})(1 - \sqrt{-19}) = 2 \cdot 10$.

Example 1.9.3. Let $R = \mathbb{Z}/6\mathbb{Z}$, and let $a = 2$. Then a is not irreducible because of the decomposition $a = 2 \cdot 4$. But a is prime, because $R/(a) = (\mathbb{Z}/6\mathbb{Z})/(2\mathbb{Z}/6\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$.

The final example is a bit contrived, as the following result shows.

Proposition 1.9.4. *Let R be an integral domain. Then any prime element of R is irreducible.*

Proof. If not, then write $a = rs$. Then one of r, s, say r, is in (a). Write $r = at$. Then $a = ats$. So $(1 - ts)a = 0$, so $(1 - ts) = 0$ because R is a domain. We see that s is a unit. □

Definition 1.9.5. A unique factorization domain (UFD) is an integral domain R with the property that for any non-zero $r \in R$ there exist a unit u and irreducible elements $\pi_1, \ldots, \pi_n$ such that

$$r = u\pi_1 \ldots \pi_n \tag{1.9.1}$$

and such that any such decomposition is unique up to rearrangement of the irreducibles and changes by units $u \mapsto vu$ and $\pi_i \mapsto v_i \pi_i$.

You will certainly have seen examples of UFDs, such as $\mathbb{Z}$ or polynomial rings over fields.

Lemma 1.9.6. *In a UFD every irreducible element is prime.*

Proof. Let π be an irreducible element of a UFD R. Let a and b be such that ab is divisible by π. Then by the uniqueness of the factorization in R, either π divides a or π divides b. □

1.9.2 PIDs

We now define an even more special type of ring.

Definition 1.9.7. A principal ideal domain (PID) is an integral domain R in which every ideal I is principal, so of the form $I = (a)$ for some $a \in R$.

We prove a fact that we already know to be true for UFDs. This time we actually have to work for it, though.

Lemma 1.9.8. *In a PID every irreducible element is prime.*

Proof. Let π be an irreducible element of a PID R. Suppose that π divides ab but not a. We show that π divides b. Consider the ideal $I = (\pi, a)$ and choose a generator c of I. Then there exist r, s in R such that $c = r\pi + sa$. On the other hand we also have $\pi = cd$ and $a = ce$ for some d, e in R. Now there are two possibilities. If d is a unit, then we have $a = ce = d^{-1}e\pi$, but this is in contradiction with our assumption that π does not divide a.

So suppose that c is unit. Then we can multiply for $bc = br\pi + sab$ and therefore $b = c^{-1}br\pi + c^{-1}sab$, which is divisible by π, proving what we want. □

Proposition 1.9.9. *A PID is a UFD.*

Proof. This Exercise 1 of Assigment 3. □

1.9.3 Relation with Dedekind domains

There certainly exist UFD that are not PIDs, for example the multivariate polynomial ring $k[x, y]$ over a field k. But for Dedekind rings, we have the following strong result.

Theorem 1.9.10. *A Dedekind ring a is a UFD if and only if it is a PID.*

Proof. Suppose that R is a Dedekind ring that is a UFD. By unique factorization of ideals, it suffices to show that every prime ideal is principal. Let $\mathfrak{p}$ be a prime ideal of R. Choose $a \in \mathfrak{p}$. Then we have an essentially unique decomposition into irreducibles $a = u\pi_1 \dots \pi_m$, and by uniqe factorization of ideals in Dedekind rings also an essentially unique factorization $(a) = \mathfrak{p}_1 \dots \mathfrak{p}_n$.

Since $\mathfrak{p}$ contains a, it contains the ideal (a), so by Corollary 1.7.19, $\mathfrak{p}$ occurs in the decomposition of (a), and we may suppose that $\mathfrak{p} = \mathfrak{p}_1$.

Since a is in $\mathfrak{p}_1$, the π_i can not all be outside $\mathfrak{p}_1$, since this is a prime ideal. So we suppose that π_1 is in $\mathfrak{p}_1 = \mathfrak{p}$.

Now (π_1) is prime because π_1 is irreducible. It is contained in $\mathfrak{p}$, so it equals $\mathfrak{p}$ by (D3). So indeed $\mathfrak{p}$ is principal. □

This means that we can measure the obstruction to R being a UFD as follows.

Definition 1.9.11. Let R be a Dedekind ring with field of fractions K. Let $I(R)$ be the group of fractional ideals of R, and let $P(R)$ be the group of principal fractional ideals of R. The class group $\mathrm{Cl}(R)$ of R is the quotient $I(R)/P(R)$. Given an ideal I of R, we call the image of I in $\mathrm{Cl}(R)$ the class of I. It will be denoted by $[I]$.

Note that $\mathrm{Cl}(R)$ is well-defined because both $I(R)$ and $P(R)$ are abelian groups. We have the following simple result

Corollary 1.9.12. *Let R be a Dedekind ring. Then R is a UFD if and only if the group $\mathrm{Cl}(R)$ is trivial.*

1.9.4 Euclidean domains

A special type of PID is furnished by rings of the following type.

Definition 1.9.13. Let R be a ring. Then R is a Euclidean domain if it admits a Euclidean function $f : R\backslash\{0\} \to \mathbb{N}$, that is a function such that for all a, b in R there exists an expression ("division with remainder") $a = qb + r$ with q, r in R such that either $r = 0$ or $f(r) < f(b)$.

For example, $\mathbb{Z}$ with the absolute value is a Euclidean domain. And so is the univariate polynomial ring $k[x]$ over a field k if we take f to be the degree function. Other examples are given by p-adic numbers, if you know about those (and also if not). We conclude with a slightly more involved example.

Example 1.9.14. The ring $R = \mathbb{Z}[i]$, equipped with the absolute value, is a Euclidean domain. Here we have to show that given a and b in $\mathbb{Z}[i]$, we can find a $q \in \mathbb{Z}[i]$ such that $a/b = q + r/b$ and $|r/b| < 1$. But this is certainly possible, since the discs of radius 1 around the elements of $\mathbb{Z}[i]$ cover the complex plane.

Proposition 1.9.15. *A Euclidean domain is a PID.*

Proof. Let I be an ideal of a Euclidean domain R. Choose $b \in I$ non-zero such that $f(b)$ is minimal among the values that f attains on the elements of I. Let a be an element of I. Then a is a multiple of b, for otherwise we write $r = a - qb$ with $f(r) < f(b)$, which yields a contradiction because r is again in I. □

1.10 Norms of ideals

The nature of ideals is too multiplicative for us to be able to define traces. But it turns out that we can still define norms of ideals, and that these satisfy the multiplicativity property that we would want them to have.

Definition 1.10.1. Let $R = \mathcal{O}_K$ be the ring of integers of a number field K, and let I be an ideal R. Then we define the norm of I as

$$\mathrm{nm}(I) = [\mathcal{O}_K : I]. \tag{1.10.1}$$

Note that this index of abelian groups is well-defined, since the exercises show that I contains some non-zero integer n.

Theorem 1.10.2. *Let $\mathcal{O}_K$ be the ring of integers of a number field K, let I be an ideal R, and let a be an element of R. Then we have* $\mathrm{nm}(aI) = |\,\mathrm{nm}(a)|\,\mathrm{nm}(I)$. *In particular, we have* $\mathrm{nm}((a)) = |\,\mathrm{nm}(a)|$.

Proof. We know that $[\mathcal{O}_K : aI] = [\mathcal{O}_K : I][I : aI]$. Multiplication by a maps I onto aI. Choose a $\mathbb{Z}$-basis $B = \{b_1, \dots, b_e\}$ of I as a free abelian group and write multiplication by a with respect to this basis. We get a matrix M_a in $M_d(\mathbb{Z})$, the absolute values of whose determinant equals the index $[I : aI]$ (use the Smith normal form trick). Since B is also a $\mathbb{Q}$-basis for the extension $K|\mathbb{Q}$, this determinant equals $\mathrm{nm}(a)$. (Recall that $\mathrm{nm}(a)$ does not depend on the choice of $\mathbb{Q}$-basis for the extension $K|\mathbb{Q}$.) □

Theorem 1.10.3. *Let $\mathcal{O}_K$ be the ring of integers of a number field K. Then the norm is multiplicative on ideals of $\mathcal{O}_K$, in the sense that if I and J are two ideals of R, then we have* $\mathrm{nm}(IJ) = \mathrm{nm}(I)\,\mathrm{nm}(J)$.

Proof. If I and J are coprime, then the Chinese remainder theorem for rings shows that $\mathcal{O}_K/IJ$ is isomorphic with $\mathcal{O}_K/I \times \mathcal{O}_K/J$, which immediately yields the result. So we can reduce to the case where $I = \mathfrak{p}^m$ and $J = \mathfrak{p}^n$ are powers of a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$. We can then write

$$[\mathcal{O}_K : IJ] = [\mathcal{O}_K : \mathfrak{p}][\mathfrak{p} : \mathfrak{p}^2] \cdots [\mathfrak{p}^{m+n-1} : \mathfrak{p}^{m+n}] \tag{1.10.2}$$

and

$$[\mathcal{O}_K : I][\mathcal{O}_K : J] = [\mathcal{O}_K : \mathfrak{p}] \cdots [\mathfrak{p}^{m-1} : \mathfrak{p}^m][\mathcal{O}_K : \mathfrak{p}] \cdots [\mathfrak{p}^{n-1} : \mathfrak{p}^n]. \tag{1.10.3}$$

It therefore suffices to show that $[\mathfrak{p}^i : \mathfrak{p}^{i+1}] = [\mathcal{O}_K : \mathfrak{p}]$ for all i.

Given i, choose $b \in \mathfrak{p}^i \backslash \mathfrak{p}^{i+1}$. Define a function $f : \mathcal{O}_K/\mathfrak{p} \to \mathfrak{p}^i/\mathfrak{p}^{i+1}$ by sending $x \in \mathcal{O}_K$ to bx. First of all f is injective:, because if bx is in $\mathfrak{p}^{i+1}$, then $\mathfrak{p}^{i+1}$ contains $(bx) = (b)(x)$. So since i is the exponent of $\mathfrak{p}$ in the factorization of (b), the factorization of (x) contains a factor $\mathfrak{p}$, which is exactly the same (why?) as saying that $x \in \mathfrak{p}$.

Surjectivity of f is harder to prove. But let I be the ideal $\mathfrak{p}^{-i}(b)$. This is an integral ideal that is coprime with $\mathfrak{p}$ because of our hypothesis on b (see also the exercises for a rephrasing of coprimality in the context of Dedekind rings). Therefore I and coprime with $\mathfrak{p}^i$ and $\mathfrak{p}^{i+1}$ as well.

Let $y \in \mathfrak{p}^i$ be a representative of a class in $\mathfrak{p}^i/\mathfrak{p}^{i+1}$. Since $\mathfrak{p}^{i+1}$ and I are coprime, the Chinese remainder theorem shows that there exists c in $\mathcal{O}_K$ such that both $c = y$ modulo $\mathfrak{p}^{i+1}$ and $c = 0$ modulo I. Now $\mathfrak{p}^i$ divides (c), because $\mathfrak{p}^i$ divides y by hypothesis and $c = y$ modulo $\mathfrak{p}^{i+1}$. And I divides (c) as well. Since these ideals are coprime, their product divides (c) as well because of unique factorization of ideals, but this product is (b) because of how we constructed I. We see that the ideal (b) divides (c), which is nothing but saying that (b) contains (c), which in turn is the same as saying that c is a multiple of b. We see that c/b is in $\mathcal{O}_K$. This allows us to calculate $f(c/b) = (c/b)b = c = y$ in $\mathfrak{p}^i/\mathfrak{p}^{i+1}$. □

Remark 1.10.4. Caution! This multiplicativity property fails for number rings that are not full rings of integers. We refer to Exercise 1 of Assignment 4 for a counterexample. However, it still goes through for invertible ideals.

1.11 Geometry of numbers

This section will study the complex embeddings of a number field K and deduce two fundamental results for its ring of integers $\mathcal{O}_K$, namely the finiteness of the class group and the structure of the unit group. The ideas involved are useful for further study of algebraic number theory, but for the applications that we have in mind, it suffices to know the end results. Therefore, you can choose how much detail of the proofs you wish to absorb.

So let K be a number field of degree d, write $K = \mathbb{Q}[x]/(f)$ with f an irreducible polynomial of degree d, and let r be the image of x in K. We saw that f has distinct roots in $r_1, \ldots, r_d$ in $\mathbb{C}$; indeed, a double root would be a root of f' as well, and then f would not be irreducible. From this, we obtain d embeddings $\varphi_i : K \to \mathbb{C}$ that send an element α of K to $\alpha_i = \varphi_i(\alpha)$. Choosing an order for the embeddings, we can combine them for a map

$$\begin{aligned} \Phi : K &\longrightarrow \mathbb{C}^d \\ \alpha &\longmapsto (\varphi_1(\alpha), \ldots, \varphi_d(\alpha)). \end{aligned} \tag{1.11.1}$$

If you know tensor products, then you will recognize this as the canonical embedding $K \to K \otimes \mathbb{C}$ (up to a non-canonical choice of basis).

Now we choose a $\mathbb{Q}$-basis B of the extension $K|\mathbb{Q}$. Recall from Proposition 1.2.7 that $0 \neq \Delta_B(K) = (\det(\varphi_i(b_j))_{i,j})^2$.

Proposition 1.11.1. *The image of K under Φ spans $\mathbb{C}^d$.*

Proof. This follows from the fact that $0 \neq (\det(\varphi_i(b_j))_{i,j})^2$. □

Now we consider the map $\mathcal{O}_K \to \mathbb{C}^d$ obtained by restricting Φ to $\mathcal{O}_K$. Pick a $\mathbb{Z}$-basis B of $\mathcal{O}_K$. We again get a matrix $T_{i,j} = (\varphi_i(b_j))_{i,j}$. Its determinant need not be an integer or even rational.

Example 1.11.2. Take $K = \mathbb{Q}(i)$, so that $\mathcal{O}_K = \mathbb{Z}[i]$, and let $B = \{1, i\}$. Then $T = \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}$, with determinant $2i$.

Proposition 1.11.3. *The absolute value $|\det(\varphi_i(b_j))_{i,j})|$ does not depend on the choice of $B = \{b_1, \ldots, b_d\}$.*

Proof. This follows because we showed that $|\Delta_B(K)^2| = |\det((\varphi_i(b_j))_{i,j})|^2$ is independent of the choice of B. □

Our goal is to relate the quantity $C = |\det((\varphi_i(b_j))_{i,j})|$ with the volume of a parallelepiped that admits an easy description in terms of $\mathcal{O}_K$. For this, we try to distill a real vector space out of the complex vector space above.

Let $K_{\mathbb{R}}$ be the subspace of $\mathbb{C}^d$ spanned over $\mathbb{R}$ by the $\varphi(b_j)$. So

$$K_{\mathbb{R}} = \mathbb{R}\varphi(b_1) + \ldots + \mathbb{R}\varphi(b_d). \tag{1.11.2}$$

The image $\Phi(\mathcal{O}_K)$ of $\mathcal{O}_K$ under the injective map Φ is again a free abelian group isomorphic with $\mathbb{Z}^d$, and it is contained in $K_{\mathbb{R}}$

Proposition 1.11.4. *The image $\Phi(\mathcal{O}_K)$ is a* lattice *in $K_{\mathbb{R}}$. That is to say, it is an abelian subgroup $K_{\mathbb{R}}$ whose $\mathbb{Z}$-basis B is also an $\mathbb{R}$-basis for $K_{\mathbb{R}}$.*

Proof. It is immediate from the definition of $K_{\mathbb{R}}$ that B spans $K_{\mathbb{R}}$. If we had a dependence between the $\varphi(b_i)$ over $\mathbb{R}$, then we would also have one $\mathbb{C}$, which is a contradiction with our previous result that the $\varphi(b_i)$ span $\mathbb{C}^d$. □

Corollary 1.11.5. *As a topological subspace, the image $\varphi(\mathcal{O}_K)$ is discrete in $K_{\mathbb{R}}$.*

Proof. Consider the bijective linear map (hence homeomorphism)

$$\begin{aligned} \mathbb{R}^d &\longrightarrow K_{\mathbb{R}} \\ e_i &\longmapsto \varphi(b_i) \end{aligned} \tag{1.11.3}$$

Take the image S of the real ball with radius $1/2$ around 0. Then $S \subseteq K_{\mathbb{R}}$ has the property that $B \cap \varphi(O_K) = \{0\}$, because the sphere of radius $1/2$ around 0 intersects $\mathbb{Z}^d$ in 0 only. By translating, we can find similar balls around arbitrary elements of $\Phi(\mathcal{O}_K)$. □

So the set

$$P_B = \{x_1\varphi(b_1) + \ldots + x_d\varphi(b_d) | \ 0 \leq x_i \leq 1 \ \} \tag{1.11.4}$$

is a parallelepiped in $K_{\mathbb{R}}$. It has finite volume, which we call the covolume of $\Phi(\mathcal{O}_K)$. Morally, this covolume should be the the quantity $C = |\det((\varphi_i(b_j))_{i,j})|$. We need to be a bit more precise to obtain this result. After all, volumes depend on a choice of Euclidean metric, or more down-to-earth, a choice of basis. (If not, then volumes would be invariant under arbitrary linear bijections of vector space, and that is certainly not the case!) So we need to consider which basis of $K_{\mathbb{R}}$ is a natural one to work with.

1.11.1 Pairing up embeddings

The embeddings φ of K into $\mathbb{C}$ come in two flavours. Recall that φ is determined by the image of r. There are two possibilities. First of all, $\varphi(r)$ can be real. In that case, the conjugate embedding, $\overline{\varphi}$, which sends an element α of K to $\overline{\varphi(\alpha)}$, sends r to r again and hence equals φ. But $\varphi(\alpha)$ may also be complex, in which case $\overline{\varphi}$ does not equal φ.

So we can split the embeddings into groups. We let R be the set of real embeddings, and we let S be the set of pairs of conjugate non-real embeddings. Then if let $\#R = r$ and $\#S = s$, we have $r + 2s = d$.

Let $\varphi_1, \ldots, \varphi_r$ be the real embeddings of K, and choose representative $\psi_1, \ldots, \psi_s$ of the elements of S. Then we can order the embeddings of K into $\mathbb{C}$ as

$$\varphi_1, \ldots, \varphi_r, \psi_1, \ldots, \psi_s, \psi'_1, \ldots, \psi'_s, \tag{1.11.5}$$

where ψ'_i is the conjugate embeddings $\overline{\psi_i}$. We get

$$\begin{aligned} \Phi : K &\longrightarrow \mathbb{C}^d \\ \alpha &\longmapsto (\varphi_1(\alpha), \ldots, \varphi_r(\alpha), \psi_1(\alpha), \ldots, \psi_s(\alpha), \psi'_1(\alpha), \ldots, \psi'_s(\alpha)). \end{aligned} \tag{1.11.6}$$

with corresponding basis vectors $e_1, \ldots e_r, f_1, \ldots, f_s, f'_1, \ldots, f'_s$. We can now give a different description of $K_{\mathbb{R}}$.

Proposition 1.11.6. *In terms of the basis vectors $e_1, \ldots e_r, f_1, \ldots, f_s, f'_1, \ldots, f'_s$, we have*

$$K_{\mathbb{R}} = \left\{ \sum_{i=1}^{r} a_i e_1 + \sum_{i=1}^{s} b_j f_j + \sum_{i=1}^{s} b'_j f'_j \mid a_i \in \mathbb{R}, b'_j = \overline{b_j} \right\}. \tag{1.11.7}$$

Proof. The discussion on pairs of embeddings shows that $K_{\mathbb{R}}$ lies in the space on the right hand side. Conversely, this space is of full $\mathbb{R}$-dimension $r + 2s$: it has a basis given by $e_1, \ldots e_r, g_1, \ldots, g_s, g'_1, \ldots, g'_s$, where $g_j = f_j + f'_j$ and $g'_j = if_j - if'_j$. □

So now once more consider the parallellepiped

$$P_B = \{x_1\varphi(b_1) + \ldots + x_d\varphi(b_d) | \ 0 \leq x_i \leq 1 \ \} \tag{1.11.8}$$

in $K_{\mathbb{R}}$. We want that $C = |\det((\varphi_i(b_j))_{i,j})|$ becomes the volume of P_B. To make this happen, we should find a basis of $K_{\mathbb{R}}$ such that the matrix T expressing the elements $\varphi(b_j)$ with respect to that basis has $\det(T) = C$. Note that he matrix $T_0 = (\varphi_i(b_j))$, whose determinant has correct absolute value, expresses the $\varphi(b_j)$ in terms of the basis the basis $e_1, \ldots e_r, f_1, \ldots, f_s, f'_1, \ldots, f'_s$ of $\mathbb{C}^n$, but these vectors are not all in $K_{\mathbb{R}}$, except of course when $s = 0$. So we have to adapt our construction a little.

We can use the matrix with respect to the new basis $e_1, \ldots e_r$, $g_1, \ldots, g_s$, $g'_1, \ldots, g'_s$. The slight problem is that the base change from $e_1, \ldots e_r$, $f_1, \ldots, f_s$, $f'_1, \ldots, f'_s$ to $e_1, \ldots e_r$, $g_1, \ldots, g_s$, $g'_1, \ldots, g'_s$ has determinant of absolute value 2^s, because for fixed j between 1 and s the base change from f_j, f'_j to g_j, g'_j has determinant $-2i$, which has absolute value 2. This will puff up our nice covolume, so we just cheat and modify the basis again by putting $h_j = g_j/\sqrt{2}$ and $h'_j = g'_j/\sqrt{2}$. Now we finally have

Proposition 1.11.7. *With respect to the basis $e_1, \ldots e_r, h_1, \ldots, h_s, h'_1, \ldots, h'_s$, the parallelepiped P_B has volume $\sqrt{\Delta(K)}$, and therefore $\Phi(\mathcal{O}_K)$ has covolume $\sqrt{\Delta(K)}$.*

Proof. This follows because the determinant of the transformation from the standard basis of $\mathbb{C}^d$ to $e_1, \ldots e_r, h_1, \ldots, h_s, h'_1, \ldots, h'_s$ has absolute value 1, and the determinant T of the φ_j with respect to the standard basis of $\mathbb{C}^d$ has correct absolute value. □

So to summarize, we now have a way of

(i) Embedding K via Φ into a "canonical" real vector space $K_{\mathbb{R}}$ associated with K;

(ii) Providing $K_{\mathbb{R}}$ with a "canonical" $\mathbb{R}$-basis $e_1, \ldots e_r, h_1, \ldots, h_s, h'_1, \ldots, h'_s$ so that we have a notion of volume;

(iii) Embedding $\mathcal{O}_K$ via Φ into $K_{\mathbb{R}}$ as a lattice;

(iv) Constructing the parallelepiped associated with this lattice of volume $C = \sqrt{|\Delta_K|}$.

We will exploit these tools to the full in the next subsections.

1.11.2 An additive embedding; structure of the class group and Minkowski's Theorem

First we are going to use Φ and a lemma that is usually attributed to Minkowski but, as Stein point out, actually due to Blichfeld to show that ideals in number fields contain elements of rather small norm with respect to $\mathrm{nm}(I)$. This will be applied to prove that the class group $\mathrm{Cl}(\mathcal{O}_K)$ is finite.

Proposition 1.11.8. *Let I be an ideal of $\mathcal{O}_K$. Embed I into $K_{\mathbb{R}}$ by Φ. Then the lattice $\Phi(I)$ has covolume $\mathrm{nm}(I)\sqrt{|\Delta_K|}$ in $K_{\mathbb{R}}$.*

Proof. Note that $\Phi(I)$ is a lattice, because it is of finite index in the lattice $\Phi(\mathcal{O}_K)$. Let $B' = \{b'_1, \ldots, b'_n\}$ be a basis for I, and let $B = \{b_1, \ldots, b_n\}$ be a basis for $\mathcal{O}_K$. With respect to the basis $e_1, \ldots, e_r, f_1, \ldots, f_s, f'_1, \ldots, f'_s$, which differs from the basis $e_1, \ldots, e_r, h_1, \ldots, h_s, h'_1, \ldots, h'_s$ by a transformation whose determinant has absolute value 1, the usual trick with the Smith normal form shows that

$$(|\det(\varphi_i(b'_j))_{i,j}|)^2 = [\mathcal{O}_K : I]^2 (|\det(\varphi_i(b_j))_{i,j}|)^2. \tag{1.11.9}$$

Taking square roots, By definition of covolumes, that means $\mathrm{Covol}(I) = [\mathcal{O}_K : I]\,\mathrm{Covol}(\mathcal{O}_K)$. But by the definition of the norm of an ideal, the latter quantity equals $[\mathcal{O}_K : I]\sqrt{|(\Delta_K)|}$. □

So under Φ, ideals in $\mathcal{O}_K$ become sublattices whose index and covolume are known. The idea of proving finiteness is as follows.

(i) We use our knowledge of the covolume of I and a lemma by Blichfeld to find a non-zero element $\alpha \in I$ that is small, in the sense that it is not too far from the origin under the embedding Φ, or alternatively, in the sense that its norm is small.

(ii) More uniformly: we prove that there exists an explicit constant μ such that for every ideal I there exists a non-zero element in I whose norm is at most $\mu \operatorname{nm}(I)$.

(iii) Now $(\alpha) \subseteq I$, so $(\alpha)I^{-1} \subseteq II^{-1} = \mathcal{O}_K$. Therefore $(\alpha)I^{-1}$ is an integral ideal that represents the same in $\operatorname{Cl}(\mathcal{O}_K)$, and its norm equals $\operatorname{nm}(a)\operatorname{nm}(I^{-1}) \leq \mu$.

(iv) One then shows that there are only finitely many ideals in $\mathcal{O}_K$ of bounded norm to conclude. Indeed, the preceding steps show that by inverting and modifying by a principal ideal, every ideal can be reduced to a set of finite cardinality.

Time to get to work! We go looking for small elements in the lattice $\Phi(I)$.

Lemma 1.11.9 (Blichfeld). *Let L be a lattice in $\mathbb{R}^d$, with volumes being taken with respect to the standard basis. Let $S \subseteq \mathbb{R}^d$ be a subset that is closed, convex and symmetric around 0. (In other words, suppose that S is closed, that if $x \in S$, then also $-x \in S$, and that $x, y \in S$, then so are the elements $\lambda x + \mu y$ with $0 \leq \lambda, \mu \leq 1$ and $\lambda + \mu = 1$.) Then if $\operatorname{Vol}(S) \geq 2^d \operatorname{Covol}(L)$, the set S contains a non-zero element if L.*

Proof. Suppose first that we have strict inequality $\operatorname{Vol}(S) \geq 2^d \operatorname{Covol}(L)$. There is a map $\frac{1}{2}S \to \mathbb{R}^d/L$. The elements of the quotient can be represented by the points of the parallellepiped P_L associated to L. We now use volumes to see that the map above is not injective:

$$\operatorname{Vol}(\frac{1}{2}S) = \left(\frac{1}{2}\right)^d \operatorname{Vol}(S) > \operatorname{Covol}(L) = \operatorname{Vol}(P_L). \tag{1.11.10}$$

Choose P_1, P_2 in $\frac{1}{2}S$ distinct but with the same image, so that $P_1 - P_2$ is in L. We have $-P_2 \in \frac{1}{2}S$ by symmetry. So by convexity $\frac{1}{2}P_1 - \frac{1}{2}P_2 = \frac{1}{2}(P_1 - P_2)$ is in $\frac{1}{2}S$. So $P_1 - P_2$ is in S, and it is by construction a non-zero element of L as well.

In the case of equality: Taking ε small, we get elements in $(1+\varepsilon)S$. There are finitely many elements that work by discreteness of L, so we can extract an element that works for all such ε and hence for $\varepsilon = 0$ as well. □

We prove a weak version of an upcoming theorem due to Minkowski, to illustrate the ideas involved.

Proposition 1.11.10. *Let K be a number field with ring of integers $\mathcal{O}_K$, and let s be the number of non-real complex embeddings of K up to conjugacy. Let $\mu = (\frac{2}{\pi})^s \sqrt{|\Delta(K)|}$, and let I be an ideal of $\mathcal{O}_K$. Then I contains an element α whose norm is at most $\mu \operatorname{nm}(I)$.*

Proof. We let X_t be the subset

$$\left\{ \sum_{i=1}^{r} a_i e_1 + \sum_{i=1}^{s} b_j f_j + \sum_{i=1}^{s} b'_j f'_j \mid |a_i|, |b_j|, |b'_j| < t \right\} \tag{1.11.11}$$

of $K_{\mathbb{R}}$. In the canonical basis of $K_{\mathbb{R}}$, this set transforms into

$$\left\{ \sum_{i=1}^{r} a_i e_1 + \sum_{j=1}^{s} c_j h_j + \sum_{j=1}^{s} b'_j h'_j \mid |a_i| < t, |(c_j)^2 + (c'_j)^2| < \sqrt{2} t \right\} \tag{1.11.12}$$

which has volume $2^r(\pi\sqrt{2}^2)^s t^d = 2^{r+s}\pi^s t^{r+2s}$.

The factor $\sqrt{2}$ is due to the fact that c_j and c_j' can be read off as the real and imaginary part of b_j, along with the fact that the modification $g_j \mapsto h_j = g_j/\sqrt{2}, g_j' \mapsto h_j' = g_j'/\sqrt{2}$ that we made corresponds to a dilation by $\sqrt{2}$.

We could take a set whose image is better behaved, but the advantage of working with X_t is that it has such a nice relation with the norm on K, which can after all be described as the product over all complex embeddings.

Let t be such that $\mathrm{Vol}(X_t) = 2^d \,\mathrm{nm}(I)\sqrt{|\Delta(K)|}$. Then since X_t is closed, convex and symmetric, $\Phi(I)$ contains a non-zero element of X_t. So there is a non-zero $\alpha \in K$ such that $\Phi(\alpha)$ is in X_t. Then by construction of the set X_t we have $\mathrm{nm}(\alpha) = \prod_i \varphi_i(\alpha) \leq t^d$, which equals $(2^d \,\mathrm{nm}(I)\sqrt{|\Delta(K)|})/(2^{r+s}\pi^s) = C$. □

We do not prove the following sharper version, but it really pays off to memorize the constant involved.

Theorem 1.11.11 (Minkowski)**.** *Let K be a number field of degree d with ring of integers $\mathcal{O}_K$, and let s be the number of non-real complex embeddings of K up to conjugacy. Consider the Minkowski constant*

$$\mu_K = \left(\frac{4}{\pi}\right)^s \frac{d!}{d^d}\sqrt{|\Delta(K)|}. \tag{1.11.13}$$

Let I be an ideal of $\mathcal{O}_K$. Then I contains a non-zero element α whose norm is at most $\mu_K \,\mathrm{nm}(I)$.

Now consider a class in $\mathrm{Cl}(\mathcal{O}_K) = I(\mathcal{O}_K)/P(\mathcal{O}_K)$, represented by the inverse I^{-1} of an integral ideal I. (It is a very useful exercise to prove yourself that every ideal can be represented in this way.)

Choose α for I as in the theorem above. Then (α) is contained in I, so $J = (\alpha)I^{-1} \subseteq II^{-1} = \mathcal{O}_K$. But $\mathrm{nm}(J) = \mathrm{nm}(\alpha)\,\mathrm{nm}(I^{-1}) \leq \mu_K$. We obtain:

Corollary 1.11.12 (Minkowski)**.** *Every ideal class is represented by an integral ideal $I \subseteq \mathcal{O}_K$ whose norm is at most μ_K.*

Proposition 1.11.13. *Let $B \geq 0$. Then there are only finitely many prime ideals of $\mathcal{O}_K$ whose norm is bounded by B.*

Proof. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$, and let $\mathfrak{p} \cap \mathbb{Z}$ be generated by the rational prime p, Then we have seen that $\mathcal{O}_K/\mathfrak{p}$ contains $\mathbb{Z}/p\mathbb{Z}$.

So $p < B$. And if p is fixed, then there are finitely many ideals containing p : indeed, these correspond to ideals of the quotient $\mathcal{O}_K/p\mathcal{O}_K$, which is isomorphic to the finite abelian group $(\mathbb{Z}/p\mathbb{Z})^d$. □

Theorem 1.11.14. *Let K be a number field with ring of integers $\mathcal{O}_K$. Then the class group $\mathrm{Cl}(\mathcal{O}_K)$ is finite.*

Proof. Use the two proceeding two results in combination with unique factorization for ideals. □

1.11.3 A logarithmic embedding; structure of the unit group and Dirichlet's Unit Theorem

We have constructed a map

$$\begin{aligned}\Phi : \mathcal{O}_K &\longrightarrow \mathbb{C}^d \\ \alpha &\longmapsto (\varphi_1(\alpha), \ldots, \varphi_r(\alpha), \psi_1(\alpha), \ldots, \psi_s(\alpha), \psi_1'(\alpha), \ldots, \psi_s'(\alpha)).\end{aligned} \tag{1.11.14}$$

whose image spanned a real vector space of dimension $d = [K : \mathbb{Q}]$, inside of which $\Phi(\mathcal{O}_K)$ sits as a lattice. Studying properties of this lattice with resect to the norm allowed us to prove finiteness of the ideal class group.

We are going to try something similar for the group of units $\mathcal{O}_K^*$. So we try to make it into a lattice under a suitable map.

Proposition 1.11.15. *Let $\alpha \in \mathcal{O}_K$. Then α is a unit if and only if* $\operatorname{nm}(\alpha) \in \{\pm 1\}$.

Proof. If α is a unit, then $\alpha\beta = 1$ for some $\beta \in \mathcal{O}_K$. But then $\operatorname{nm}(\alpha)\operatorname{nm}(\beta) = 1$, so $\operatorname{nm}(\alpha)$ and $\operatorname{nm}(\beta)$ are both integral and multiply to 1. This shows that $\operatorname{nm}(\alpha) \in \{\pm 1\}$. Conversely, if $\operatorname{nm}(\alpha) \in \{\pm 1\}$. Then choosing a basis B for $\mathcal{O}_K$, we see that the fact that $\operatorname{nm}(\alpha)$ is a unit in $\mathbb{Z}$ implies that the map $\mathcal{O}_K \to \mathcal{O}_K$ given by multiplication by α is bijective. So since $1 \in \mathcal{O}_K$, there exists a β in $\mathcal{O}_K$ such that $\alpha\beta = 1$. □

The multiplicative property of the norm function therefore suggests that we can study units by transforming multiplication into addition. Everyone's favorite way to do this is to apply the log function. So here goes our first try. We consider the map

$$\begin{aligned}\mathcal{O}_K^* &\longrightarrow \mathbb{C}^d \\ \alpha &\longmapsto (\log\varphi_1(\alpha), \ldots, \log\varphi_r(\alpha), \log\psi_1(\alpha), \ldots, \log\psi_s(\alpha), \log\psi_1'(\alpha), \ldots, \log\psi_s'(\alpha)).\end{aligned} \tag{1.11.15}$$

This does not work as well as we may like. For one, we do not land inside a real vector space. Worse, the log function is not well-defined on $\mathbb{C}$ because $e^{2\pi i} = 1$. A way around this problem is to take absolute values first. So our second attempt is the map

$$\begin{aligned}\mathcal{O}_K^* &\longrightarrow \mathbb{R}^d \\ \alpha &\longmapsto (\log|\varphi_1(\alpha)|, \ldots, \log|\varphi_r(\alpha)|, \log|\psi_1(\alpha)|, \ldots, \log|\psi_s(\alpha)|, \log|\psi_1'(\alpha)|, \ldots, \log|\psi_s'(\alpha)|).\end{aligned} \tag{1.11.16}$$

But there is redundant information here. Since ψ_i and ψ_i' are conjugate embeddings, the corresponding entries are equal. We may as well take

$$\begin{aligned}\mathcal{O}_K^* &\longrightarrow \mathbb{R}^{r+s} \\ \alpha &\longmapsto (\log|\varphi_1(\alpha)|, \ldots, \log|\varphi_r(\alpha)|, \log|\psi_1(\alpha)|, \ldots, \log|\psi_s(\alpha)|).\end{aligned} \tag{1.11.17}$$

Call this map L (for log embedding). We will prove that

(U1) $\ker(L)$ is finite cyclic, and consists of the roots of unity in $\mathcal{O}_K^*$; and

(U2) $\operatorname{im}(L)$ is isomorphic to the free abelian group $\mathbb{Z}^{r+s-1}$.

From this, we obtain the following important result.

Theorem 1.11.16 (Dirichlet's Unit Theorem)**.** *Let K be a number field with ring of integers $\mathcal{O}_K$. Let r be the number of real embeddings of K, and let s be the number of pairs of non-real complex embeddings of K up to conjugation. The subgroup of $\mathcal{O}_K$ roots of unity is finite cyclic, say of order w, and there exists an isomorphism*

$$\mathcal{O}_K^* \cong \mathbb{Z}/w\mathbb{Z} \times \mathbb{Z}^{r+s-1}. \tag{1.11.18}$$

Proof. Using (U1) and (U2), choose representatives $r_1, \ldots, r_{r+s-1}$ in $\mathcal{O}_K^*$ of the inverse images of the standard basis vectors $e_1, \ldots, e_{r+s-1}$ of $\mathbb{Z}^{r+s-1} \cong \mathcal{O}_K^*/\ker(L)$, and also choose a generator ζ of $\ker(L)$. Define a map $f : \mathbb{Z}/w\mathbb{Z} \times \mathbb{Z}^{r+s-1} \to \mathcal{O}_K^*$ by $f(1,0) = \zeta$ $f(0,e_i) = r_i$. The map f is then well-defined becuase $\mathcal{O}_K^*$ is commutative.

First we show that f is injective. Suppose $f(n_1, v_1) = f(n_2, c_2)$. Then taking images under L, we see that $v_1 = v_2$ because the e_i are independent form a basis. Subtract to get $f(n_1, 0) = f(n_2, 0)$, which forces $n_1 = n_2$ because ζ is a generator of $\ker(L)$.

Now to show that f is surjective. Let $u \in \mathcal{O}_K^*$ be arbitary. Then let $v \in \mathbb{Z}^{r+s-1}$ correspond to the image of u in $\mathcal{O}_K^*/\ker(L)$. Then $uf(0,v)^{-1}$ is in $\ker(L)$, hence of the form $f(n,0)$ for some n. We then have $u = f(n,v)$. □

It now remains to prove (U1) and (U2). The first is relatively easy.

Theorem 1.11.17. $\ker(L)$ *is finite cyclic, and consists of the roots of unity in $\mathcal{O}_K$.*

Proof. We have

$$\ker(L) = \{\alpha : |\varphi_i(\alpha)| = 1 \text{ for } 1 \leq i \leq d\}. \tag{1.11.19}$$

The image of this set under Φ is contained in a compact set, so contains finitely many elements of $\mathcal{O}_K$ because $\Phi(\mathcal{O}_K)$ is a lattice. Indeed, the corresponding intersection is discrete because $\Phi(\mathcal{O}_K)$ is, and remains compact as a subset of $\Phi(\mathcal{O}_K)$. Therefore it is finite.

Since it is finite, all its elements have finite order, hence are roots of unity. Conversely, it certainly contains all the roots of unity (why?). That $\ker(L)$ is cyclic now follows from an exercise! □

Now we start trying to prove (U2). The following property (which explains the exponent $r + s - 1$) is quickly observed.

Proposition 1.11.18. $\operatorname{im}(L)$ *is contained in the hyperplane $H \subset \mathbb{R}^{r+s}$ defined by*

$$H = \{(x_1, \ldots, x_r, x_{r+1}, \ldots, x_{r+s}) : x_1 + \ldots x_r + 2x_{r+1} + \ldots + 2x_{r+s} = 0\}. \tag{1.11.20}$$

Proof. This follows because for a unit $u \in \mathcal{O}_K^**$ we have

$$1 = |\operatorname{nm}(u)| = \prod_{i=1}^{d} |\varphi_i(u)| = \prod_{i=1}^{r} |\varphi_i(u)| \prod_{j=1}^{s} |\psi_j(u)|^2. \tag{1.11.21}$$

□

We first prove two propositions that shows that the image $\operatorname{im}(L)$ is not too big:

Proposition 1.11.19. $\operatorname{im}(L)$ *is discrete in H.*

Proof. It suffices to show that there are at most finitely many α in $\mathcal{O}_K$ for which $\log|\varphi_1(\alpha)|| \leq 1, \ldots, \log|\varphi_r(\alpha)|| \leq 1, \log|\psi_1(\alpha)|| \leq 1, \ldots, \log|\psi_s(\alpha)|| \leq 1$, which in turn follows if we can show that there are finitely many α for which $|\varphi_1(\alpha)| \leq e, \ldots, |\varphi_r(\alpha)| \leq e, |\psi_1(\alpha)| \leq e, \ldots, |\psi_s(\alpha)| \leq e$, or equivalently $|\varphi_1(\alpha)| \leq e, \ldots, |\varphi_r(\alpha)| \leq e, |\psi_1(\alpha)| \leq e, \ldots, |\psi_s(\alpha)| \leq e, |\psi_1'(\alpha)| \leq e, \ldots, |\psi_s'(\alpha)| \leq e$. But this follows from the fact that $\Phi(\mathcal{O}_K)$ is a lattice. □

Proposition 1.11.20. $\mathrm{im}(L)$ *is isomorphic to a subgroup of* $\mathbb{Z}^{r+s-1}$.

Proof. Let W be the vector space spanned by $\mathrm{im}(L)$. Then W has dimension at most $r+s-1$, because W is contained in H. We now use the following Lemma to conclude. □

Lemma 1.11.21. *Let V be a vector space of dimension d over $\mathbb{R}$, and let M be an abelian group of V spanning V as a vector space. Then M is discrete if and only if M is isomorphic with $\mathbb{Z}^d$ as an abelian group.*

Proof. One implication is clear; if M is isomorphic with $\mathbb{Z}^d$, then a $\mathbb{Z}$-basis $B = \{b_1, \dots, b_d\}$ for M is also a basis for V, because of the spanning hypothesis. Consider the linear isomorphism (hence homeomorphism) $V \to \mathbb{R}^d$ that sends b_i to the i-th standard basis vector e_i. Then the image $\mathbb{Z}^d$ of M is discrete, hence so is M itself.

We have seen one implication. For the converse, again choose a subset $B = \{b_1, \dots, b_d\}$ of M that is a basis for W as an $\mathbb{R}$-vector space. Let $N = \mathbb{Z}^d$ be the subgroup of M generated by B. If M is not isomorphic to $\mathbb{Z}^d$, then the index $[M : N]$ is infinte. Once more consider the linear isomorphism (hence homeomorphism) $V \to \mathbb{R}^d$ that sends b_i to the i-th standard basis vector e_i. Every element of $\mathbb{R}^d/N$ has a representative in the compact set $C = \{(x_1, \dots, x_d : 0 \leq x_i \leq 1\}$. If $[M : N]$ were infinite, then we would get infinitely many distinct elements in $C \cap M$. But this set is discrete and compact, hence finite. Contradiction. □

Note that the proof essentially uses that $\mathbb{R}/\mathbb{Z}$ is compact (in showing that $C \cong (\mathbb{R}/\mathbb{Z})^d$ is compact). Also note that $\mathbb{C}/\mathbb{Z}$ is not. We now show that $\mathrm{im}(L)$ is big enough, by showing that it spans H. For this, we first prove the following lemma.

Lemma 1.11.22. *Let V be a vector space of dimension d over $\mathbb{R}$, and let W be a subspace of V for which there exists a bounded set B such that*

$$V = W + B = \{w + b : w \in W, b \in B\}. \tag{1.11.22}$$

Then $W = V$.

Proof. We may transform linearly in such a way that $V = \mathbb{R}^n$ and $W = \mathbb{R}^m$ is defined as the span of the first m basis vectors of $\mathbb{R}^n$. Let $p : \mathbb{R}^n \to \mathbb{R}$ be the projection onto the final component. If $W \neq V$, then $p(W + B) \subseteq p(B)$, which as the image of a bounded set is bounded, contradiction. □

Theorem 1.11.23. $\mathrm{im}(L)$ *spans the hyperplane* H.

Proof. We follow [1, Section 6.3] and exploit the additive result. Let D be the "dilating set"

$$D = \left\{ (x_1, \dots x_r, y_1, \dots, y_s, y'_1, \dots y'_s) \in K_{\mathbb{R}} : \prod_{i=1}^{r} |x_i| \prod_{j=1}^{s} |y_j| \prod_{j=1}^{s} |y'_j| \in \{\pm 1\} \right\}. \tag{1.11.23}$$

Then we have seen that $\Phi(\mathcal{O}_K^*)$ is a subset of D, and because $y'_j = \overline{y_j}$, we lose no information under projecting D onto its first $r + s$ coordinates. Let p be the corresponding projection, and let $D' \subset \mathbb{C}^{r+s}$ be the image of $p(D)$ under this projection. Let Log be the log map

$$\begin{aligned} \mathrm{Log} : D' &\longrightarrow \mathbb{R}^{r+s} \\ (x_1, \dots x_r, y_1, \dots, y_s) &\longmapsto (\log|x_1|, \dots \log|x_r|, \log|y_1|, \dots, \log|y_s|). \end{aligned} \tag{1.11.24}$$

Then $\mathrm{Log}(D') = H$.

The idea is that because one can construct many elements of the image $\mathrm{im}(L)$ by dividing by dividing elements that generate the same ideal, there exists a subset Y' of D' such that such that

(a) $\mathrm{Log}(Y')$ is bounded, and

(b) $H = L(\mathcal{O}_K^*) + \mathrm{Log}(Y')$, or alternatively

(b') $D' = p(\Phi(\mathcal{O}_K^*)) \cdot Y'$, which is implied by

(b") $D = \Phi(\mathcal{O}_K^*) \cdot Y$.

By the preceding lemma, this suffices to show what we want.

Again let

$$X_t = \left\{ \sum_{i=1}^{r} a_i e_1 + \sum_{i=1}^{s} b_j f_j + \sum_{i=1}^{s} b'_j f'_j \mid |a_i|, |b_j|, |b'_j| \leq t \right\}. \tag{1.11.25}$$

Choose t st $\mathrm{Vol}(X_t) = 2^d\sqrt{\Delta_K}$, and denote the corresponding X_t by X. Then by Blichfeld, X contains an element of $\Phi(\mathcal{O}_K)$.

Now let $d = (x_1, \ldots, x_r, y_1, \ldots, y_s, y'_1, \ldots, y'_s) \in D$ be a dilating element. Then

$$dX = \left\{ \sum_{i=1}^{r} a_i e_1 + \sum_{i=1}^{s} b_j f_j + \sum_{i=1}^{s} b'_j f'_j \mid |a_i| <\leq |x_i|t, |b_j| \leq |y_i|t, |b'_j| \leq |y'_i|t \right\}. \tag{1.11.26}$$

which by construction of D has the same volume as X and therefore also contains an element α_d of $\Phi(\mathcal{O}_K)$. This gives us a lot of dilated boxes to play with.

The norms of the ideals (α_d) are globally bounded, so we get finitely many ideals, given by $\{\alpha_1, \ldots, \alpha_N\}$ say. It is this paucity of ideals compared with the abundance of d that makes the proof work.

We let

$$Y = D \cap \bigcup_{i=1}^{N} \Phi(\alpha_i^{-1})X), \tag{1.11.27}$$

with $\Phi(a_i^{-1})$ dilating as an element of D, and we set $Y' = p(Y)$.

There is a global bound on the absolute values of the coordinates of the elements of Y. So since by definition Y is contained in D, we get a lower bound on the coordinates too. Therefore $\mathrm{Log}(Y')$ is a bounded, and we have proved (a).

To show (b'), let $d \in D$. There exists an α_d such that $\Phi(\alpha_d)$ is in $d^{-1}X$. Also, and crucially, there exists an α_i in the representing set such that α_i and α_d generate the same ideal So $\alpha_i \alpha_d^{-1} = u$ is an element of $\mathcal{O}_K^*$. So d is in $\Phi(\alpha^{-1})X = \Phi(u)\Phi(\alpha_i^{-1})X$. We are done. □

Corollary 1.11.24. $\mathrm{im}(L)$ *is isomorphic with* $\mathbb{Z}^{r+s-1}$.

Proof. This is now OK! □

The actual calculation of the unit group involves a technical tool called the regulator. In our simple examples in the practice section, we do not exploit this tool, but it is very useful and is described in more advanced texts on the subject, such as [5], where it is defined in Definition 5.15.

Chapter 2

Practice

2.1 Minimal polynomials and rewriting

As mentioned in Fact 1.1.7, every number field is isomorphic to one of the form $\mathbb{Q}[x]/(f)$, with $f \in \mathbb{Q}[x]$ irreducible. Here we indicate how to find an explicit representation of a number field in this form.

Example 2.1.1. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Then K is a degree 4 extension of $\mathbb{Q}$, since it is spanned by $\{1, \sqrt{2}, \sqrt{3}, \sqrt{2}\sqrt{3}\}$, and it contains two non-isomorphic quadratic subfields; if $[K : \mathbb{Q}]$ were to equal 2, then $\sqrt{2}$ would be in the quadratic field $\mathbb{Q}(\sqrt{3})$ and vice versa, and we know that this does not happen. We find an element α of K whose minimal polynomial f is a quartic. Then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$, so $K = \mathbb{Q}(\alpha)$ by the tower law (Proposition 1.1.8).

Any element that is not in a proper subfield of K in fact generates K. So we choose an element that seems to be unlikely to be in such a subfield, say $\alpha = \sqrt{2} + \sqrt{3}$. This works: writing the powers of α in terms of the basis $\{1, \sqrt{2}, \sqrt{3}, \sqrt{2}\sqrt{3}\}$, we get

$$\begin{array}{ccccccccc} \alpha^0 & = & 1 & + & 0 \cdot \sqrt{2} & + & 0 \cdot \sqrt{3} & + & 0 \cdot \sqrt{2}\sqrt{3}, \\ \alpha^1 & = & 0 & + & 1 \cdot \sqrt{2} & + & 1 \cdot \sqrt{3} & + & 0 \cdot \sqrt{2}\sqrt{3}, \\ \alpha^2 & = & 5 & + & 0 \cdot \sqrt{2} & + & 0 \cdot \sqrt{3} & + & 2 \cdot \sqrt{2}\sqrt{3}, \\ \alpha^3 & = & 0 & + & 11 \cdot \sqrt{2} & + & 9 \cdot \sqrt{3} & + & 0 \cdot \sqrt{2}\sqrt{3}, \\ \alpha^4 & = & 49 & + & 0 \cdot \sqrt{2} & + & 0 \cdot \sqrt{3} & + & 20 \cdot \sqrt{2}\sqrt{3}, \end{array} \tag{2.1.1}$$

The matrix formed by the first four equalities is non-singular, so the first dependence that we find in this way is of degree 4. It corresponds to the left kernel of the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 5 & 0 & 0 & 2 \\ 0 & 11 & 9 & 0 \\ 49 & 0 & 0 & 20 \end{pmatrix}. \tag{2.1.2}$$

Since this kernel is generated by the vector $(1, 0, -10, 0, 1)$, we have $f = x^4 - 10x^2 + 1$. Calculating an explicit isomorphism is again linear algebra; to get some familiarity with these calculations, try to determine $\mathbb{Q}$-linear expressions of $\sqrt{2}$ and $\sqrt{3}$ in terms of powers of α. For now, we conclude by showing how to calculate the inverse α^{-1} in terms of the powers of α.

In terms of the basis $\{1, \alpha, \alpha^2, \alpha^3\}$, multiplication by α takes an especially simple form, since the first three basis elements are map to the last three. In a matrix representation, we have

$$M_\alpha = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 10 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{2.1.3}$$

Since 1 corresponds to the first basis standard vector e_1, the inverse α^{-1} corresponds to the vector $M_\alpha^{-1}e_1$, which equals $(0, 10, 0, -1)$. We get $\alpha^{-1} = -\alpha^3 + 10\alpha$.

Example 2.1.2. Let $K = \mathbb{Q}[x]/(f)$ be the number field defined by the irreducible cubic polynomial $f = x^3 + 5x + 10$, and let r be the image of x in K. Consider the element $\alpha = (r^2 - r)/2$. We determine the minimal polynomial of α, and after that, we express r in terms of α.

First the minimal polynomial. As usual, we can use the minimal polynomial $x^3+5x+10$ of r to obtain the relation $r^3+5r+10$, which allows us to express every power of r beyond r^2 in terms of the basis $B = \{1, r, r^2\}$, as in the proof of Proposition 1.1.6. We represent the powers of α in the basis B until we spot a dependency. The zeroth power α^0 is easy and corresponds to the vector $(1, 0, 0)$. Also easy is α^1, which has the representation $(0, -1/2, 1/2)$. The second power α^2 equals $(r^2 - r)^2/4 = (r^4 - 2r^3 + r^2)/4$. So since $r^3 = -5r - 10$ and therefore $r^4 = -5r^2 - 10r$, we can indeed express α^2 just in terms of $1, r, r^2$. We have

$$\begin{aligned} \alpha^2 &= (r^4 - 2r^3 + r^2)/4 \\ &= (-5r^2 - 10r - 2(-5r - 10) + r^2)/4 \\ &= (-4r^2 + 20)/4 \\ &= -r^2 + 5. \end{aligned} \tag{2.1.4}$$

We get the vector $(5, 0, -1)$. The vectors obtained thus far are not dependent yet, but now we know that we will obtain a dependence at the next step, for reasons of degree. One calculates $\alpha^3 = 5r^2 - 5$ in the same way. So the successive powers of α up to α^3 give use the matrix

$$M = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1/2 & 1/2 \\ 5 & 0 & -1 \\ -5 & 0 & 5 \end{pmatrix}. \tag{2.1.5}$$

The minimal polynomial for α corresponds to a relation between the rows of M, that is, to an element in its one-dimensional left kernel. That kernel is spanned by $(-20, 0, 5, 1)$. So $\alpha^3 + 5\alpha^2 + 0\alpha^1 - 20\alpha^0 = 0$, and because we did not find dependencies of lower degree, the minimal polynomial of α is $g = x^3 + 5x^2 - 20$.

Now we express r in terms of α. This is again nothing but linear algebra; let

$$N = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1/2 & 1/2 \\ 5 & 0 & -1 \end{pmatrix}. \tag{2.1.6}$$

be the matrix formed by the first rows of M. This matrix gives us the linear transformation between the bases $\{1, r, r^2\}$ and $\{1, \alpha, \alpha^2\}$ of K. Since r has representation $(0, 1, 0)$ in terms of the basis $\{1, r, r^2\}$, and the rows of N give the representations of the powers of α, finding an expression $r = c_2\alpha^2 + c_1\alpha^1 + c_0\alpha^0$ for r in terms of α is nothing but finding the solution of the equation $(c_0, c_1, c_2)N = (0, 1, 0)$. This solution is $(5, -2, -1)$, so we have $r = -\alpha^2 - 2\alpha + 5$.

Example 2.1.3. The integral expressions for the coeffcients of the expression of α in terms of α were purely coincidental. Let $\beta = (\alpha^2 + 5\alpha)/2$. You can by now verify yourself that β has minimal polynomial $x^3 - 25x - 50$ and that $\alpha = (\beta^2 - 25)/5$.

2.2 Calculating traces, norms, and discriminants

Being able to calculate discriminants is essential for determining the rings of integers of number fields. In turn, determining a discriminant requires you to be able to calculate traces. This section explains how to do this effectively. First we calculate some traces and norms.

Example 2.2.1. Let $K = \mathbb{Q}(\sqrt{5})$, let $r = \sqrt{5}$, and let $\alpha = a + b\sqrt{5}$. We can choose the embeddings φ_1, φ_2 of K such that $\varphi_1(\alpha) = a + b\sqrt{5}$ and $\varphi_2(\alpha) = a - b\sqrt{5}$. Then by Theorem 1.2.3 we have that

$$\begin{aligned} \operatorname{tr}(\alpha) &= \varphi_1(\alpha) + \varphi_2(\alpha) = (a + b\sqrt{5}) + (a - b\sqrt{5}) = 2a, \\ \operatorname{nm}(\alpha) &= \varphi_1(\alpha) \cdot \varphi_2(\alpha) = (a + b\sqrt{5}) \cdot (a - b\sqrt{5}) = a^2 - 5b^2. \end{aligned} \tag{2.2.1}$$

We can also show this by a direct calculation, merely using Definition 1.2.1. This is actually much more feasible in higher degree than calculating the conjugates. In this particular case, in terms of the basis $\{1, r\}$, the matrix of the linear map L_r is given by

$$M_r = \begin{pmatrix} 0 & 5 \\ 1 & 0 \end{pmatrix}. \tag{2.2.2}$$

So

$$M_\alpha = a + bM_r = \begin{pmatrix} a & 5b \\ b & a \end{pmatrix}. \tag{2.2.3}$$

Taking traces and determinants, we recover the results above. Note that the characteristic polynomial g_q of L_q equals $(x - q)^2$ if $q \in \mathbb{Q}$, which is not minimal, but a power of the minimal polynomial, as remarked after Theorem 1.2.3.

Example 2.2.2. Let $K = \mathbb{Q}[x]/(x^3 - x + 1)$, let r be the image of x in K, and consider an element $\beta = a + br + cr^2$ of K. Then in the basis $B = \{1, r, r^2\}$, multiplication by r is represented by the matrix

$$M_r = \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}. \tag{2.2.4}$$

So

$$M_\beta = a + bM_r + cM_r^2 = \begin{pmatrix} a & -c & -b \\ b & a + c & b - c \\ c & b & a + c \end{pmatrix}. \tag{2.2.5}$$

We get

$$\begin{aligned} \operatorname{tr}(\beta) &= \operatorname{tr}(M_\beta) = 3a + 2c, \\ \operatorname{nm}(\beta) &= \det(M_\beta) = a^3 + 2a^2c - ab^2 + 3abc + ac^2 - b^3 + bc^2 + c^3. \end{aligned} \tag{2.2.6}$$

Example 2.2.3. We wrap up this section by calculating some discriminants. First let $K = \mathbb{Q}(\sqrt{5})$ once more. For this field, we can calculate the discriminant in two ways.

We first apply the method that always works, namely the direct application of the definition 1.2.6. Let $r = \sqrt{5}$, and consider the basis $B = \{1, r\}$ of K. Then with respect to B, the trace pairing has matrix

$$T_B = (\mathrm{tr}(b_i b_j))_{i,j=1}^2 = \left(\mathrm{tr}(r^{i-1} r^{j-1})\right)_{i,j=1}^2 = \begin{pmatrix} \mathrm{tr}(r^0) & \mathrm{tr}(r^1) \\ \mathrm{tr}(r^1) & \mathrm{tr}(r^2) \end{pmatrix} \tag{2.2.7}$$

We know $M_r = M_{\sqrt{5}}$ from the Example 2.2.1, so we can certainly calculate $\mathrm{tr}(r^i) = \mathrm{tr}(M_r^i)$. We get

$$T_B = \begin{pmatrix} 2 & 0 \\ 0 & 10 \end{pmatrix} \tag{2.2.8}$$

So $\Delta_B(K)$ equals $\det(T_B) = 20$.

For quadratic fields (unlike for more general fields), it is also still feasible to use the formula

$$\Delta_B(K) = \det\left((\varphi_i(b_j))_{i,j=1}^d\right)^2. \tag{2.2.9}$$

from Proposition 1.2.7. We then first calculate the determinant of the matrix

$$(\varphi_i(b_j))_{i,j=1}^2 = \begin{pmatrix} 1 & r \\ 1 & -r \end{pmatrix}, \tag{2.2.10}$$

which equals $-2r$. The square of this determinant equals $(-2r)^2 = 20$.

This twice obtained discriminant is not squarefree, and considering Proposition 1.4.9, this is not surprising, since the $\mathbb{Z}$-span of B does not equal $\mathcal{O}_K$. The double factor 2 points to the extension of degree 2 that is needed to obtain $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\frac{1+\sqrt{5}}{2}$ from $\mathbb{Z} \oplus \mathbb{Z}\sqrt{5}$.

Example 2.2.4. Now consider $K = \mathbb{Q}[x]/(x^3 - x + 1)$ again, with the same basis B as before. Then with respect to B, the trace pairing has matrix

$$T_B = (\mathrm{tr}(b_i b_j))_{i,j=1}^3 = \left(\mathrm{tr}(r^{i-1} r^{j-1})\right)_{i,j=1}^3 = \begin{pmatrix} \mathrm{tr}(r^0) & \mathrm{tr}(r^1) & \mathrm{tr}(r^2) \\ \mathrm{tr}(r^1) & \mathrm{tr}(r^2) & \mathrm{tr}(r^3) \\ \mathrm{tr}(r^2) & \mathrm{tr}(r^3) & \mathrm{tr}(r^4) \end{pmatrix} \tag{2.2.11}$$

Calculating the necessary $\mathrm{tr}(r^i) = \mathrm{tr}(M_r^i)$, we find

$$T_B = \begin{pmatrix} 3 & 0 & 2 \\ 0 & 2 & -3 \\ 2 & -3 & 2 \end{pmatrix}. \tag{2.2.12}$$

The corresponding discriminant $\Delta_B(K) = -23$ is squarefree, so $\mathcal{O}_K = \mathbb{Z}[r]$ by Corollary 1.4.10.

2.3 Determining rings of integers

The determination of the ring of integers of a number field is one of the most important parts to understanding the arithmetic properties of this field. We will give lots of examples of this calculation in this section, and indeed also in later sections, where this calculation will often be an essential requirement to obtain results.

For some fields with an especially simple structure, on can determine the ring of integers in complete generality, as we have seen for quadratic fields and cyclotomic fields. These are also some examples of cubic fields whose ring of integers is easy to determine. For an excellent example, we refer to the proof in [1, Chapter 4] that $\mathcal{O}_{\mathbb{Q}(\sqrt[3]{2})} = \mathbb{Z}[\sqrt[3]{2}]$.

Here we treat treat techniques that work in general. A first step is to find a generator α of the number field as in Section 2.1 and determine its minimal polynomial f to write $K = \mathbb{Q}(\alpha) = \mathbb{Q}[x]/(f)$. In these notes, α and f were usually given in advance. After this, if α is not already integral, then one scales it by a sufficiently large integer N as in the proof of Proposition 1.4.1 so that it yields an integral element $\beta = N\alpha$. A first guess for the ring of integers of K is then the ring $\mathbb{Z}[\beta]$. One can use the determinant criterion in Proposition 1.4.9 or Corollary 1.4.10 to find out whether or not this guess is correct.

Example 2.3.1. Let $K = \mathbb{Q}[x]/(f)$, where $f = x^3 - (1/4)x + (1/8)$. Let α be the image of x in K. Then 2α has minimal polynomial $2^3 f(x/2) = x^3 - x + 1$. Let $\beta = 2\alpha$, and let $B = \{1, \beta, \beta^2\}$. Then $\Delta_B(K) = \Delta(f) = -23$ by the exercises. This is square-free, so $\mathcal{O}_K = \mathbb{Z}[\alpha]$ by Corollary 1.4.10.

However, we will often need to combine Proposition 1.4.9 and the Kummer–Dedekind Theorem 1.8.4 to do the job. The procedure is as follows:

(i) Find an integral element $\alpha \in K$ such that $K = \mathbb{Q}(\alpha)$. Then $\mathbb{Z}[\alpha]$ is an order in K, hence of finite index in $\mathcal{O}_K$.

(ii) Using Proposition 1.4.9, determine the set of rational primes S that may divide the index $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$.

(iii) For the primes $p \in S$, use part (3) of the Kummer–Dedekind theorem to either conclude (using parts (1) and (2)) that p does not divide $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$ or to construct (using part (3)) elements $\beta_p, \beta'_p, \ldots$ in $\mathcal{O}_K \backslash \mathbb{Z}[\alpha]$ and such that p occurs to a lower power in $[\mathcal{O}_K : \mathbb{Z}[\beta_p]], [\mathcal{O}_K : \mathbb{Z}[\beta'_p]], \ldots$.

(iv) Now consider the ring $\mathbb{Z}[\beta_p]$ and repeat the procedure to create rings $\mathbb{Z}[\gamma_p], \mathbb{Z}[\gamma'_p], \ldots, \mathbb{Z}[\delta_p], \mathbb{Z}[\delta'_p], \ldots$. Continue inductively in this way for $\beta'_p, \ldots$ as well. In the end you end up with a ring whose index in $\mathcal{O}_K$ is coprime with p.

(v) After this calculation is finished for all primes, let $R = \mathbb{Z}[\alpha, \{\beta_p, \beta'_p, \ldots, \gamma_p, \gamma'_p, \ldots, \delta_p, \delta'_p \ldots\}_{p \in S}]$. Then $\mathcal{O}_K = R$.

The final claim is easy to show, and we will exploit its proof often. It goes as follows. The index $[\mathcal{O}_K : R]$ divides the index $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$. As such, it is only divisible by the primes in S. But none of these primes can occur, because R also has subrings whose index in $\mathcal{O}_K$ is coprime with p.

This procedure does not look pleasant, and in general it is very far from being so. Fortunately, it is not that difficult in practice, and with some luck, you end up with a ring $\mathcal{O}_K$ that is again of the form $\mathbb{Z}[\gamma]$ for some integral element γ. Some examples are in order, the first of which is that of quadratic fields. You are invited to compare the following quick and easy proof with the horribly complicated one in Theorem 1.5.2. This is to show you how useful the Kummer–Dedekind theorem is; it downgrades theorems into propositions.

Proposition 2.3.2. *Let $d \neq 0, 1$ be a square-free integer, and let K be the quadratic number field $\mathbb{Q}(\sqrt{d})$. Let $\beta = \sqrt{d}$ if d is not congruent to 1 mod 4 and let $\beta = (1 + \sqrt{d})/2$ otherwise. Then $\mathcal{O}_K = \mathbb{Z}[\beta]$.*

Proof. Consider the integral element $\alpha = \sqrt{d}$. It has minimal polynomial $f = x^2 - d$. The discriminant of K with respect to the basis $\{1, \alpha\}$ equals $4d$, so only the prime 2 and the odd primes dividing d can divide $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$. The order $\mathbb{Z}[\alpha]$ is isomorphic with $\mathbb{Z}[x]/(f)$, so we analyse its primes by using the Kummer–Dedekind Theorem 1.8.4.

First consider an odd prime p dividing d. Then $\overline{f}$ equals x^2, which has the unique factor x. The remainder of f after division by the lift x equals d, which because d is square-free is not in $p^2\mathbb{Z}[x]$. Using Theorem 1.8.4(1)(ii), we conclude that the primes of $\mathbb{Z}[\alpha]$ over p are all invertible. Hence by Theorem 1.8.4(2) the prime p does not divide $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$.

Now let $p = 2$. Then $\overline{f}$ equals $x^2 - d$. If $d = 3 \bmod 4$, then $\overline{f} = (x-1)^2$, and upon dividing f with remainder by the corresponding lift $x - 1$, we get $f(1) = 1 - d$, which is 2 mod 4 and hence not in $2^2\mathbb{Z}[x]$. So in this case 2 does not divide $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$ either and $\mathcal{O}_K = \mathbb{Z}[\alpha]$. If $d \equiv 2 \bmod 4$, then $\overline{f} = x^2$, and upon dividing f with remainder by the corresponding lift x, we get $f(0) = -d$, which is 2 mod 4 and hence not in $2^2\mathbb{Z}[x]$. So in this case 2 again does not divide $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$ either and $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

If $d = 1 \bmod 4$, then $\overline{f} = (x-1)^2$, and upon dividing f with remainder by the corresponding lift $x - 1$, we get $f(1) = 1 - d$, which is 2 mod 4. Now Theorem 1.8.4(3) gives us a new integral element by writing $f = q(x-1) + r$. We see that $q = (x+1)$, so we get the element $\beta = q(\alpha)/2 = (1 + \sqrt{d})/2$.

We are in the fortunate situation that $\alpha = 2\beta - 1$ is in $\mathbb{Z}[\beta]$. So we have found a ring $\mathbb{Z}[\beta]$ containing $\mathbb{Z}[\alpha]$ as a subring of index 2. For this reason, the discriminant of K with respect that the basis $\{1, \alpha\}$ equals $4d/2^2$. The factor 2 occurs at most once in this discriminant, so 2 does not divide the index $[\mathcal{O}_K : \mathbb{Z}[\beta]]$ by Proposition 1.4.9. Since $\mathbb{Z}[\beta]$ contains $\mathbb{Z}[\alpha]$, neither does any other prime divide this index, and we therefore have $\mathcal{O}_K = \mathbb{Z}[\beta]$. □

Example 2.3.3. We now treat a more complicated example. Let $K = \mathbb{Q}[x]/(f)$ be the number field defined by the irreducible cubic polynomial $f = x^3 + 5x + 10$. Let α be the image of x in K. Then one calculates as in Section 2.2 that the discriminant of K with respect to the basis $\{1, \alpha, \alpha^2\}$ of $K|\mathbb{Q}$ equals $-2^7 5^2$. So in the light of Proposition 1.4.9, we have to apply Kummer–Dedekind modulo 5 and modulo 2.

Modulo 5, we have $\overline{f} = x^3$. we obtain $r = 10$ as remainder term upon division by x, which is not in $5^2\mathbb{Z}[x]$. Therefore 5 does not divide the index $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$ by Theorem 1.8.4(1)(ii) and (2).

Modulo 2, we have $\overline{f} = (x-1)^2 x$. We get two primes $(2, \alpha)$ and $(2, \alpha - 1)$ above 2. Since x is a single factor of $\overline{f}$, the prime $(2, \alpha)$ is invertible by Theorem 1.8.4(1)(i). For $(2, \alpha - 1)$, we have to find a quotient q and a remainder term r, both in $\mathbb{Z}[x]$, such that $f = q(x-1) + r$.

There are two ways to find such a remainder term. A method that always works is long division in the ring $\mathbb{Z}[x]$. However, for number fields of degree at most 3, there is a trick that speeds up the process. In this case, the only multiple factors that can occur are linear, say of the form $x - d$, and the remainder r in the division with remainder $f = q(x-d) + r$ will be a constant. One now simply evaluates both sides of the equality at $x = d$ to obtain $r = f(d)$.

In this particular case, we see that for the factor $x - 1$ of f, we end up with the remainder $f(1) = 16 \in 2^2\mathbb{Z}[x]$. By Theorem 1.8.4(1), this means that the prime $(2, \alpha - 1)$ is not invertible, and we can construct an element of $\mathcal{O}_K \backslash \mathbb{Z}[\alpha]$ by constructing the element β in Theorem 1.8.4(3).

We have $f = (x^2+x+6)(x+1)+16$, so we get $\beta = q(\alpha)/2 = (\alpha^2+\alpha+6)/2$. We see that $\mathcal{O}_K$ contains the order $\mathbb{Z}[\alpha, (\alpha^2 + \alpha + 6)/2] = \mathbb{Z}[\alpha, (\alpha^2 - \alpha)/2]$. If we let $\gamma = (\alpha^2 - \alpha)/2$, then in fact we will have $\mathbb{Z}[\alpha, (\alpha^2 - \alpha)/2] = \mathbb{Z}[\gamma]$ since $\alpha = -\gamma^2 - 2\gamma + 5$ (a calculation performed in Section 2.1).

So we are lucky and consider the subring $\mathbb{Z}[\gamma]$ of $\mathcal{O}_K$, which contains $\mathbb{Z}[\alpha]$ as a subring of finite order. As we saw in Section 2.1), the minimal polynomial of γ equals $g = x^3+5x^2-20$, so $\mathbb{Z}[\gamma] \cong \mathbb{Z}[x]/(g)$. We once more apply Kummer–Dedekind. Modulo 2, this polynomial factors as $x^2(x-1)$, so in the light of Theorem 1.8.4(1), we have to consider the prime $(2, \gamma)$. Dividing with remainder by the double factor x, we once more get $g(0) = -20 \in 2^2\mathbb{Z}[x]$, so this prime is again non-invertible by Theorem 1.8.4(1). We can write $f = (x^2+5x)x - 20$, so by Theorem 1.8.4(3) the new element $\delta = q(\gamma)/2 = (\gamma^2 + 5\gamma)/2$ is in $\mathcal{O}_K$. We have constructed a farily large subring $\mathbb{Z}[\gamma, \delta]$ of $\mathcal{O}_K$.

It is now more difficult to find a single generator of the ring $\mathbb{Z}[\gamma, \delta]$, because we saw in Section 2.1 that $\gamma = (\delta^2 - 25)/5$ is not in $\mathbb{Z}[\delta]$. But no matter; we just employ the proof technique above to show that $\mathcal{O}_K = \mathbb{Z}[\gamma, \delta]$!

Consider the minimal polynomial $h = x^3 - 25x - 50$ of ε. Modulo 2, it factors as $x(x-1)^2$. Dividing with remainder by the double factor $x-1$, we get remainder $h(1) = -74$, which is not a multiple of 4. By Theorem 1.8.4(1) and (2), the index $[\mathcal{O}_K : \mathbb{Z}[\delta]]$ is not divisible by 2. Hence neither is $[\mathcal{O}_K : \mathbb{Z}[\gamma, \delta]]$. On the other hand, because $\mathbb{Z}[\gamma, \delta]$ contains α, no odd primes can divide $[\mathcal{O}_K : \mathbb{Z}[\gamma, \delta]]$. Therefore in fact $\mathcal{O}_K = \mathbb{Z}[\gamma, \delta]$, and we are done.

It is too bad that we did not find an $\varepsilon \in \mathcal{O}_K$ such that $\mathcal{O}_K = \mathbb{Z}[\varepsilon]$, but such is life. Sometimes this is in fact unavoidable; see [4, Example 5.3.2].

As a final example, we give a general result. It is included in this section on practice because it is such an excellent illustration of the whole procedure.

Proposition 2.3.4. *Let $d \neq 0, 1$ be a cube-free integer. Let $\alpha = \sqrt[3]{d}$. Then the cubic field $K = \mathbb{Q}(\sqrt[3]{d})$ has ring of integers $\mathbb{Z}[\alpha, \beta_p, \beta_3]$, where for a prime $p \neq 3$ the element $\beta_p = \alpha^2/p$ is included if and only if p^2 divides d, and where β_3 is included if and only if $d \in \{-1, 0, 1\}$ mod 9. If $d = -1$ mod 9, then $\beta_3 = (\alpha^2 - \alpha + 1)/3$, if $d = 0$ mod 9, then $\beta_3 = \alpha^2/3$, and if $d = 1$ mod 9, then $\beta_3 = (\alpha^2 + \alpha + 1)/3$.*

Proof. By Exercise 3 of Assignment 2, the discriminant of K with respect to the basis $\{1, \alpha, \alpha^2\}$ equals $-27b^2$. This means that only $p = 3$ and the primes dividing d can possibly divide the index $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$.

First let $p \neq 3$ be a prime dividing d. Then we get $\overline{f} = x^3$, with remainder $f(0) = d$, which is in $p^2\mathbb{Z}[x]$ if and only if p^2 divides d. Should this happen, then we have $f = x^2 \cdot x - d$, so the element adjoined in Theorem 1.8.4(3) is $\beta_p = \alpha^2/p$. On the other hand β_p has minimal polynomial $x^3 - d^2/p^3$. Reducing and dividing with remainder, we get d^2/p, which contains a single factor p because d is cube-free. So the index $[\mathcal{O}_K : \mathbb{Z}[\beta_p]]$ is not divisible by 3 by Theorem 1.8.4(1) and (2).

Now look at the prime $p = 3$. First suppose that 3 divides d. Then we get $\overline{f} = x^3$. Proceeding as before, we see that we are done if d is not congruent to 0 mod 9. On the other hand, Theorem 1.8.4(3) yields the new integral element $\beta_3 = \alpha^2/3$ if $d = 0$ mod 9. The element β_3 has minimal polynomial $x^3 - (d^2/3^3)$, and once more division with remainder and applying Theorem 1.8.4(1) and (2) shows that $[\mathcal{O}_K : \mathbb{Z}[\beta_3]]$ is not divisible by 3.

Now suppose that $d = 1$ mod 3. Then $\overline{f} = x^3 - 1 = (x-1)^3$. Division with remainder gives remainder term $f(1) = 1 - d$, which is in $3^2\mathbb{Z}[x]$ if and only if $d = 1$ mod 9. In that case, Theorem 1.8.4(3) yields the new integral element $\beta_3 = (\alpha^2 + \alpha + 1)/3$. This gives an index 3 overring $\mathbb{Z}[\alpha, \beta_3]$ of $\mathbb{Z}[\alpha]$ whose discriminant equals $-27d^2/3^2$ by Proposition 1.4.9. By our hypothesis on d, this discriminant contains no square factor 3, so we see that we do not have to enlarge at 3.

Now suppose that $d = 2 \bmod 3$. Then $\overline{f} = x^3 + 1 = (x+1)^3$. Division with remainder gives remainder term $f(-1) = -1 - d$, which is in $3^2\mathbb{Z}[x]$ if and only if $d = -1 \bmod 9$. In that case, Theorem 1.8.4(3) yields the new integral element $\beta_3 = (\alpha^2 - \alpha + 1)/3$. This gives an index 3 overring $\mathbb{Z}[\alpha, \beta_3]$ of $\mathbb{Z}[\alpha]$ whose discriminant equals $-27d^2/3^2$ by Proposition 1.4.9. By our hypothesis on d, this discriminant contains no square factor 3, so we see that we do not have to enlarge at 3.

Let $R = \mathbb{Z}[\alpha, \beta_p, \beta_3]$. Then as before we see that no prime can divide the index $[\mathcal{O}_K : \mathbb{Z}[\alpha, \beta_p, \beta_3]]$. So indeed $\mathcal{O}_K = \mathbb{Z}[\alpha, \beta_p, \beta_3]$. □

2.4 Factoring ideals

This section consider how to actually factor ideals. After applying Kummer–Dedekind for factoring rational primes, we will give some tricks for factoring more general ideals.

2.4.1 Factoring rational primes

For orders of the form $\mathbb{Z}[\alpha]$, the exercises furnish lots of examples of this, using part (0) and (2) of the Kummer–Dedekind Theorem 1.8.4. Note that in general, there may not exist a monogenous subring $\mathbb{Z}[\alpha]$ of $\mathcal{O}_K$ whose index is coprime with a given prime p. But in fact one can show that given a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, there exists a subring $\mathbb{Z}[\alpha]$ such that $\mathfrak{p}$ corresponds to a factor of the minimal polynomial f of α that is either single or for which the remainder is not in $p^2\mathbb{Z}[x]$. Besides, in everyday calculations with number fields, the chances of this happening are simply too small to merit a full treatment here, interesting though it is. We again refer to [4, Example 5.3.2].

2.4.2 Factoring principal ideals

A useful trick involving principal ideals of the form $(n - \alpha)$ is the following observation:

Proposition 2.4.1. *Let K be a number field, and let $\alpha \in K$ be an element generating an order in K, and let $f \in \mathbb{Z}[x]$ be the minimal polynomial of α. Then we have* $\mathrm{nm}((n-\alpha)) = |f(n)|$.

Proof. We can reduce to the case $n = 0$ by the observation that $\alpha - n$ has minimal polynomial $f(x+n)$. And if $n = 0$, this is immediate from Definition 1.2.1 and Theorem 1.10.2; indeed, the characteristic polynomial g_α of α equals f because α generates the extension $K|\mathbb{Q}$. □

By the multiplicativity of the norm, shown in Theorem 1.10.3, along with the norm calculation in Theorem 1.8.4(2), this shows that the prime ideals of $\mathcal{O}_K$ that divide $(n-\alpha)$ are above the primes dividing $|f(n)|$. We then proceed as in the next subsection to determine the actual factorization. For now, note that this gives a useful way to construct principal ideals divisible by a prime over a given rational prime p; simply scan through a small list of values $f(n)$ and see if p divides $f(n)$. We will see that this is exceedingly useful for class group calculations.

2.4.3 Factoring general ideals

Suppose we are given a finite set $S \subset \mathcal{O}_K$. Can we then determine the factorization of the ideal I generated by S into primes?

Observe the following. If a prime ideal $\mathfrak{p}$ divides I, then it contains all the s_i in S. Let $(p) = \mathfrak{p} \cap \mathbb{Z}$. Then by the multiplicativity of the norm, we know that $\mathrm{nm}(\mathfrak{p})$, which is a power of p by Theorem 1.8.4(2), divides $\mathrm{nm}(s_i)$. This means that the primes of $\mathcal{O}_K$ dividing I are above the rational primes dividing the gcd of the $\mathrm{nm}(s_i)$.

This gives a finite amount of primes to try. To simplify further, suppose that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Factorize the possible $\mathfrak{p} = (p, g(\alpha))$. Then I is contained in $\mathfrak{p}$ if and only if all the elements s_i are in the ideal $(\overline{g})$ in $(\mathbb{Z}/p\mathbb{Z})[\alpha]$. This can be checked by evaluating the s_i under the homomorphism $\mathcal{O}_K \to (\mathbb{Z}/p\mathbb{Z})[\alpha]$ corresponding to $\mathfrak{p}$.

Finding multiplicities is more difficult, so we do not get into this. Usually a norm or uniqueness argument can be used to conclude matters. Running over all the possible $\mathfrak{p}$, we get our factorization.

Example 2.4.2. Let $K = \mathbb{Q}[x]/(f)$ be the cubic field defined by the irreducible polynomial $f = x^3 + x + 1$, and let α be the image of x in K. The discriminant of f equals the prime -31, so $\mathcal{O}_K = \mathbb{Z}[\alpha]$ by Corollary 1.4.10. Consider the ideal $I = (78\alpha^2 + 39\alpha + 39, 104\alpha^2 + 104\alpha + 91)$.

An obvious factor of I is (13), so we factorize the ideal (13) further into prime ideal. The polynomial f is not irreducible mod 13, since it admits -6 as a root. This already gives use a prime ideal $\mathfrak{p}_{13} = (13, \alpha + 6)$ of $\mathcal{O}_K$, which has norm 13 by Theorem 1.8.4(2). We factor out $(x + 6)$ from $\overline{f}$ using long division to get $\overline{f} = (x + 6)(x^2 - 6x - 2)$. The second factor is degree 2 and has no roots modulo 11; therefore it is irreducible, and it gives rise to an ideal $\mathfrak{q}_{169} = (13, \alpha^2 - 6\alpha - 2)$ of norm 13^2 of $\mathcal{O}_K$. By Theorem 1.8.4(2), we get the factorization $(13) = \mathfrak{p}_{13}\mathfrak{q}_{169}$ since both factors occur with multiplicity 1.

Now we are left to factor $J = (13)^{-1}I = (6\alpha^2 + 3\alpha + 3, 8\alpha^2 + 8\alpha + 7)$. We calculate $\mathrm{nm}((6\alpha^2 + 3\alpha + 3)) = 3^3 11$ and $\mathrm{nm}((8\alpha^2 + 8\alpha + 7)) = 3^2 1113$. So only primes above 3 and 11 can occur in the factorization of J.

Modulo 11, $\overline{f}$ has a single root 2 mod 11. We divide out the corresponding factor $x - 2$ to obtain the factorization $\overline{f} = (x - 2)(x^2 + 2x + 5)$. Again the second factor has no roots, so we get two ideals $\mathfrak{p}_{11} = (11, \alpha - 2)$ and $\mathfrak{q}_{121} = (11, \alpha^2 + 2\alpha + 5)$ of $\mathcal{O}_K$ of norm 11 and 11^2, respectively, along with the factorization $(11) = \mathfrak{p}_{11}\mathfrak{q}_{121}$ by Theorem 1.8.4(2).

Modulo 3, $\overline{f}$ factors as $(x - 1)(x^2 + x - 1)$. This gives two ideal $\mathfrak{p}_3 = (3, \alpha - 1)$ and $\mathfrak{q}_9 = (3, \alpha^2 + \alpha - 1)$ of norms 3 and 3^2, respectively.

The ideal $\mathfrak{p}_3$ does not occur in the factorization of I, because $8\alpha^2 + 8\alpha + 7$ is not killed by the evaluation $\mathcal{O}_K \to \mathbb{Z}/3\mathbb{Z}$ sending α to 1 that corresponds to the prime ideal $\mathfrak{p}_3$. On the other hand, both $6\alpha^2 + 3\alpha + 3$ and $8\alpha^2 + 8\alpha + 7$ are annihilated by the evaluation $\mathcal{O}_K \to (\mathbb{Z}/3\mathbb{Z})[x]/(x^2 + x - 1)$ sending α to x that corresponds to the prime ideal $\mathfrak{q}_9$. We conclude that $\mathfrak{q}_9$ divides J, and by Theorem 1.10.3, we know that the integral ideal $J\mathfrak{q}_9^{-1}$ has norm 11. It is therefore the unique prime ideal $\mathfrak{p}_{11}$ of norm 11 above 11. (In passing, note that an ideal whose norm is prime is prime itself!) Putting everything together, we see that $I = \mathfrak{q}_9\mathfrak{p}_{11}\mathfrak{p}_{13}\mathfrak{q}_{169}$. This ideal is in fact principal.

2.5 Non-invertible ideals

Let $\mathbb{Z}[\alpha]$ be a monogenous suborder of $\mathcal{O}_K$. By Proposition 1.8.1 and Theorem 1.8.4(2), the only prime ideals of $\mathbb{Z}[\alpha]$ that can be non-invertible are those over the rational primes dividing the index $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$. We consider an example of this.

Example 2.5.1. Let $\alpha = \sqrt{5}$, and let $R = \mathbb{Z}[\alpha]$ be the number ring generated by α. Then there is a single prime ideal $\mathfrak{p}_2$ of R containing 2 by Proposition 1.8.2. This ideal corresponds to the unique ideal of $(\mathbb{Z}/2\mathbb{Z})[x]/(x^2 - 5) = (\mathbb{Z}/2\mathbb{Z})[x]/(x - 1)^2$, and is given by $\mathfrak{p}_2 = (2, \alpha - 1)$.

The ideal $\mathfrak{p}_2$ is not invertible. Indeed, let a, b be rational numbers. Then $a + b\alpha$ is in $\mathfrak{p}_2^{-1}$ if and only if $(a + b\alpha)2 = 2a + 2b\alpha$ and $(a + b\alpha)(\alpha - 1) = (5b - a) + (a - b)$ are both in R. Either $2a$ and $2b$ are both odd, or they are both even. So $\mathfrak{p}_2^{-1} = (1, (\alpha + 1)/2)$, and we have $\mathfrak{p}_2\mathfrak{p}_2^{-1} = (2, \alpha + 1, \alpha - 1, 2) = (2, \alpha - 1) = I$, which does not contain 1.

For another example, using different proof techniques, see Exercise 1 of Assignment 6.

2.6 Calculating class groups and unit groups

We give a few examples of how to calculate class groups and unit groups. The first examples of class groups will be relatively simple and can be calculated without knowledge of the unit group. This situation will become more complicated later.

2.6.1 Class groups

Example 2.6.1. Let K be the quadratic number field $\mathbb{Q}(\sqrt{35})$, let $\alpha = \sqrt{35}$, and let $\mathcal{O}_K = \mathbb{Z}[\alpha]$ be the ring of integers of K. The Minkowski contant μ_K from Corollary 1.11.12 equals $(4/\pi)^0(2!/2^2)\sqrt{|\Delta_K|} = (1/2)\sqrt{140} = \sqrt{35}$, so $\mathrm{Cl}(\mathcal{O}_K)$ is generated by the prime ideals of norm at most 5.

We proceed to factor the ideals $(2), (3), (5)$ using Theorem 1.8.4. Let $f = x^2 - 35$ be the minimal polynomial of α. Modulo 2, we have $\overline{f} = x^2 - 1 = (x - 1)^2$, so we get the single prime ideal $\mathfrak{p}_2 = (2, \alpha - 1)$ for which $\mathfrak{p}_2^2 = (2)$ by Kummer–Dedekind. Modulo 3, we have $\overline{f} = x^2 + 1$, which is irreducible. So (3) is a principal prime ideal of norm 9. Modulo 5, we have $\overline{f} = x^2$. We get the prime ideal $\mathfrak{p}_5 = (5, \alpha)$ for which $\mathfrak{p}_5^2$ equals the principal ideal (5).

Since the generators $\mathfrak{p}_2$ and $\mathfrak{p}_5$ have order 2, this already shows that the class group is at worst $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$. We try to find some more relations by factoring ideals of the form $(k - \alpha)$ where k is in $\mathbb{Z}$.

Recall that $\mathrm{nm}((k - r)) = |f(k)|$ from Proposition 2.4.1. We use this to find principal ideals of small norm, which we then factor for extra relations. The most interesting ones are of course those containing the factors 2 and 5 , since using these, we find relations between $\mathfrak{p}_2$ and $\mathfrak{p}_5$. There is one very good candidate now, namely $k - 5$, leading to the element $5 - r$ of norm -10. We obtain the factorization $(5 - \alpha) = \mathfrak{p}_2\mathfrak{p}_5$, which shows that $\mathrm{Cl}(\mathcal{O}_K)$ is generated by $\mathfrak{p}_2$. This ideal may still be trivial.

However, we do not end up with any more nice relations in this way. So we wish to prove that $\mathfrak{p}_2$ is *not* principal, so as to conclude that $\mathrm{Cl}(\mathcal{O}_K) \cong \mathbb{Z}/2\mathbb{Z}$.

To see this, it suffices to show that no elements of norm 2 or -2 exist in $\mathbb{Z}[\alpha]$. For this, consider the norm form $\mathrm{nm}(x + \alpha y) = x^2 - 35y^2$ modulo 5 to see that it cannot assume the value 2, and modulo 7 to see that it cannot assume the value -2.

This reduction step at the end is a trick that is only guaranteed to work for quadratic fields. For more general fields, we will later consider another method, which uses some knowledge of the unit group. For now, we treat one more simple example.

Example 2.6.2. Let K be the quadratic number field $\mathbb{Q}(\sqrt{-14})$, let $\alpha = \sqrt{-14}$ with minimal polynomial $x^2 - 14$ and let $\mathcal{O}_K = \mathbb{Z}[\alpha]$ be the ring of integers of K.

This time we have $\mu_K = (4/\pi)^1(2!/2^2)\sqrt{|\Delta_K|} = (4/\pi)^1\sqrt{14} < 5$. So we factor the integral primes 2 and 3 using Kummer–Dedekind.

Modulo 2, we get $\overline{f} = x^2$, whence a single prime ideal $\mathfrak{p}_2 = (2, \alpha)$ of square (2). Modulo 3, we get the factorization $\overline{f} = (x - 1)(x + 1)$, whence prime ideals $\mathfrak{p}_3 = (3, \alpha - 1)$ and $\mathfrak{q}_3 =$

$(3, \alpha+1)$ for which $(3) = \mathfrak{p}_3\mathfrak{q}_3$, which yields the relation $[\mathfrak{p}_3] + [\mathfrak{q}_3] = 0$ between the classes $[\mathfrak{p}_3]$ and $[\mathfrak{q}_3]$ of $\mathfrak{p}_3$ and $\mathfrak{q}_3$ in $\mathrm{Cl}(\mathcal{O}_K)$. (Recall the bracket notation from Definition 1.9.11.)

So $\mathrm{Cl}(\mathcal{O}_K)$ is generated by the ideals $\mathfrak{p}_2$ and $\mathfrak{p}_3$. We do not know yet what the order of $\mathfrak{p}_3$ is. But we have $f(-2) = 18$, which in light of Proposition 2.4.1 should give something interesting. The element $(-2-\alpha)$ is not sent to 0 under the evaluation $\alpha \mapsto -1$ corresponding to $\mathfrak{q}_3$. So necessarily we have $(-2-\alpha) = \mathfrak{p}_2\mathfrak{p}_3^2$, which implies that $[\mathfrak{p}_2] + 2[\mathfrak{p}_3] = 0$. We see that $\mathfrak{p}_3$ generates the class group, and that its order divides 4 (since $\mathfrak{p}_2^2$ is principal).

These ideals $\mathfrak{p}_3$ and $\mathfrak{p}_3^2$ are not principal because the norm form $x^2 + 14y^2$ takes values in $\{3, 9\}$ only for $x = \pm 3$, $y = 0$, and the corresponding elements 3 and -3 do not furnish generators for $\mathfrak{p}_3^2$ since they generate the ideal $\mathfrak{p}_3\mathfrak{q}_3$ instead. We obtain that $\mathrm{Cl}(\mathcal{O}_K)$ is cyclic of order 4, a generator being given by $[\mathfrak{p}_3]$.

As you may guess from this example, the class number of imaginary quadratic number fields grows much quicker than those of real number fields, since too few elements of small norms are available.

2.6.2 Unit groups

For quadratic fields, calculating unit groups is possible by relatively simple methods.

Example 2.6.3. Let $K = \mathbb{Q}(\sqrt{-14})$, and let $\mathcal{O}_K = \mathbb{Z}[\sqrt{-14}]$ be the ring of integers of K. Then $\mathcal{O}_K^* = \{\pm 1\}$ because the norm form $x^2 + 14y^2$ only assumes values in $\{\pm 1\}$ if $(x, y) = \pm(1, 0)$.

Example 2.6.4. Let $K = \mathbb{Q}(\sqrt{35})$, let $\alpha = \sqrt{35}$, and let $\mathcal{O}_K = \mathbb{Z}[\alpha]$ be the ring of integers of K. Since K admits an embedding into $\mathbb{R}$, the only roots of unity in $\mathbb{R}$ are $\{\pm 1\}$. By Dirichlet's Unit Theorem 1.11.16, there exists an isomorphism $\mathcal{O}_K^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$, so we try to find an additional generator of this group. In particular, we should find a neat way to produce units.

There are multiple ways to do this. The first naive way is to use Proposition 2.4.1 and check if $\mathrm{nm}(k - r) = f(k)$ is ever equal to ± 1, and in this example this actually happens; we thus obtain the unit $6 - \alpha$.

The other way is to find two different generators for the same ideal, whose quotient will then be a unit. For example, we know from the preceding subsection that $\mathfrak{p}_2\mathfrak{p}_5$ is an ideal of norm 10 whose square equals (10). This square is also generated by $(5+\alpha)^2 = 25 + 35 + 10\alpha = 60 + 10\alpha$. Now by taking the quotient of these generators, which is unit, we end up with $(6+\alpha) = (6-\alpha)^{-1}$.

So let $u = 6 + \alpha$. Because it is so small, the unit u is pretty likely to generate unit group $\mathcal{O}_K^*$ modulo the cyclic group of roots of unity generated by -1. We now prove this.

Suppose that u does not generate $\mathcal{O}_K^*/\langle -1 \rangle$. Then either u or $-u$ is a power u_0^k of another unit u_0. Changing u_0 to u_0^{-1} if necessary, we may suppose that u or $-u$ is a *strictly positive* power of u_0. We will derive a contradiction from this.

First suppose that $u = u_0^k$. Write $u_0 = a_0 + b_0\alpha$ with a, b in $\mathbb{Z}$. Then if a_0 and b_0 have different sign, so would the entries of u, so this does not happen. Neither can we have a_0, b_0 negative if k is odd, and if k is even, then we can always change u_0 to $-u_0$. So we may suppose that a_0 and b_0 are positive. But since the cases $a_0 = 0$ and $b_0 = 0$ are easily excluded, the coefficients of 1 and α in the powers of u_0 strictly grow with each powering, as you can easily prove using induction. We can therefore restrict our search to $1 \leq a_0, b_0 \leq 6$, and one checks that this does not give any suitable u_0.

Next, suppose that $u = -u_0^k$. Again we see that a and b have the same sign, and we may once more suppose that a and b are both positive. Choosing the embedding under which α is positive, we now immediately get a contradiction.

We conclude that $\mathcal{O}_K^* = \langle -1 \rangle \times \langle 6 + \alpha \rangle$.

As mentioned at the end of Section 1.11, calculating unit groups in general requires more technical tools. However, usually the information on $\mathcal{O}_K$ that you want to get your hands on is the class group, to determine this, one can do with less information, as will be shown in the next subsection.

2.6.3 Class groups and unit groups simultaneously

Usually, one has to calculate a weak version of the unit group to calculate the class group, as the following example illustrates.

Example 2.6.5. Let $K = \mathbb{Q}[x]/(f)$ be the cubic field defined by the polynomial $f = x^3 - 2x - 5$, and let α be the image of x in K. Then f has discriminant -643, which is prime, so $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

Plotting the graph, we see that f has a single real root. So in the usual notation, we have $r = s = 1$. Moreover, we have $\mu_K = (4/\pi)^1 (6/27)\sqrt{643} < 8$, so we have to factor the ideals up to 7. Skipping the details, we see that $(2) = (2, \alpha - 1)(2, \alpha^2 + \alpha + 1) = \mathfrak{p}_2\mathfrak{q}_4$, $(3) = (3, \alpha - 1)(3, \alpha^2 + \alpha + 2) = \mathfrak{p}_3\mathfrak{q}_9$, $(5) = (5, \alpha)(5, \alpha^2 - 2) = \mathfrak{p}_5\mathfrak{q}_{25}$, and $(7) = (7) = \mathfrak{p}_{343}$.

We have to find relations between $[\mathfrak{p}_2], [\mathfrak{q}_4], [\mathfrak{p}_3]$ and $[\mathfrak{p}_5]$. The factorizations above already show that $[\mathfrak{p}_2] + [\mathfrak{q}_4]$, and we factor ideals of the form $(k - \alpha)$ to obtain more. We evaluate f at small values and apply Proposition 2.4.1. This shows that $\text{nm}(\alpha) = 5$, so $\mathfrak{p}_5 = (\alpha)$ by uniqueness and therefore $[\mathfrak{p}_5]$ is trivial. Also, $\text{nm}(1 - \alpha) = -6$ so $[\mathfrak{p}_2] + [\mathfrak{p}_3]$ is trivial, showing that $\mathfrak{p}_2$ generates $\text{Cl}(\mathcal{O}_K)$. Finally, we have $\text{nm}(-1 - \alpha) = -4$. Evaluation shows that this element is in $\mathfrak{p}_2$, so it cannot be a generator of $\mathfrak{q}_4$. As such, we see that $\mathfrak{p}_2^2 = (-1 - \alpha)$, so $2[\mathfrak{p}_2] = 0$ in the class group.

We do not find any more relations. So we conjecture that $\text{Cl}(\mathcal{O}_K)$ is a cyclic group of order 2, generated by $[\mathfrak{p}_2]$. This is equivalent to proving that no element with norm 2 or -2 exists, but this time around this becomes difficult to verify because the norm form is huge for cubic fields.

We give up for now and try to determine the unit group of $\mathcal{O}_K$. Since K can be embedded into $\mathbb{R}$, there are no roots or unity in $\mathcal{O}_K$ beyond $\{\pm 1\}$. Dirichlet now tells us that $\mathcal{O}_K^* / < -1 >$ is isomorphic with $\mathbb{Z}^{r+s-1} = \mathbb{Z}$. We try to find a generator. Here we are lucky! Checking small values of f, we see that $\text{nm}(2 - \alpha) = -1$. This is so small that it simply has to be a fundamental unit.

Unfortunately, we cannot prove this here. This needs further study of the geometry of numbers. However, we are going to use a weaker statement, namely that -1 and $u = 2 - \alpha$ generate $\mathcal{O}_K^* / (\mathcal{O}_K^*)^2$. This is much easier: it suffices to find a prime modulo which u is not a square or -1 times a square. That is quickly done: use $\mathfrak{p}_5 = (5, \alpha)$. The corresponding evaluation $\alpha \mapsto 0$ sends u to 2 mod 5, which is not a square, and neither is -2 mod 5.

It turns out that this information about the unit group modulo the cardinality of the tentative class group suffices for our purposes of determining the class group. Indeed, if $\mathfrak{p}_2$ were principal, generated by $x \in \mathcal{O}_K$ say, then we would have $(x^2) = \mathfrak{p}_2^2 = (-1 - \alpha)$. So $x^2 = v(-1 - \alpha)$ for some unit v. Since we can incorporate squares of units into x, this would imply that one of the elements $(-1 - \alpha)$, $(1 + \alpha)$, $u(-1 - \alpha)$ or $u(1 + \alpha)$ would be a square.

You can check yourself that by evaluating modulo the prime $\mathfrak{p}_3 = (3, \alpha - 1)$, both $(1 + r)$ and $u(1 + \alpha)$ become non-squares, that modulo $\mathfrak{p}_5 = (5, \alpha)$ the element $u(-1 - r)$ becomes a non-square, and that modulo $\mathfrak{p}_{13} = (13, \alpha - 10)$, the element $(-1 - \alpha)$ becomes a non-square. Hence all of the aforementioned elements are non-squares, an indeed the class group is cyclic of order 2.

A similar procedure, first reducing the tentative class group as much as possible and then determining a weak version of the unit group to prove the correctness of this guess, works for general number fields.

We conclude with a final example.

Example 2.6.6. Let $K = \mathbb{Q}[x]/(f)$ be the cubic field defined by the polynomial $f = x^3 - 3x^2 - 8$, and let α be the image of x in K. We first determine the ring of integers $\mathcal{O}_K$.

The discriminant of f equals $-2^5 3^4$. So we only have to apply Kummer–Dedekind to the primes 2 and 3. You can check that the index $[\mathcal{O}_K : \mathbb{Z}[\alpha]$ is not divisible by 3. On the other hand, over the prime 2 we get a non-invertible ideal and a new element $\beta = (\alpha^2 - \alpha)/2$ of $\mathcal{O}_K$.

As in Section 2.1, we determine that the minimal polynomial of β equals $g = x^3 - 3x^2 - 6x - 10$, which has discriminant $-2^3 3^6$. We also obtain the relation $\alpha = (\beta^2 - 2\beta - 2)/3$. Using Kummer–Dedekind, we see that the index $[\mathcal{O}_K : \mathbb{Z}[\beta]$ is not divisible by 2, and we conclude that $\mathcal{O}_K = \mathbb{Z}[\alpha, \beta]$. This is slightly awkward because no single generator is in sight, but the goal of the example is to show how to proceed in this case.

As usual, we tabulate some small values, this time of both f and g:

n	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5	6
$f(n)$	-332	-208	-120	-62	-28	-12	-8	-10	-12	-8	8	42	100
$g(n)$	-298	-180	-98	-46	-18	-8	-10	-18	-26	-28	-18	10	62

(2.6.1)

The Minkowski bound μ_K is strictly smaller than 8, so we factor the rational primes up to 7 in $\mathcal{O}_K$. The key point is that by Proposition 1.8.1, these factorizations can all be performed in the ring $\mathbb{Z}[\alpha]$, except for the rational prime 2, for which we have to use $\mathbb{Z}[\beta]$. Conversely, the ring $\mathbb{Z}[\beta]$ can be used to factor all rational primes but 3, for which we have to use $\mathbb{Z}[\alpha]$.

Using the tables, these factorizations are easy. We obtain $(2) = \mathfrak{p}_2^2 \mathfrak{q}_2$ with $\mathfrak{p}_2 = (2, \beta)$ and $\mathfrak{q}_2 = (2, \beta - 1)$, $(3) = \mathfrak{p}_3^3$ with $\mathfrak{p}_3 = (2, \alpha + 1)$, $(5) = \mathfrak{p}_5 \mathfrak{q}_{25}$ with $\mathfrak{p}_5 = (5, \beta) = (5, \alpha - 1)$, and $(7) = \mathfrak{p}_7 \mathfrak{q}_{49}$ with $\mathfrak{p}_7 = (7, \beta - 3) = (7, \alpha + 2$.

We also use the tables to determine some relations. First of all, we have $(1 - \beta) = \mathfrak{q}_2 \mathfrak{p}_3^2$ by the uniqueness of the prime ideal $\mathfrak{p}_3$ above 3, because certainly $(1 - \beta) \in \mathfrak{q}_2$. So $[\mathfrak{q}_2] = -2[\mathfrak{p}_3]$. On the other hand, we already know that $[\mathfrak{q}_2] = -2[\mathfrak{p}_2]$, so because the order of $[\mathfrak{p}_3]$ divides 3, we conclude that $[\mathfrak{p}_2] = [\mathfrak{q}_3]$. So we can discard the ideals above 2 as generators of $\mathrm{Cl}(\mathcal{O}_K)$.

Factoring $(-\beta)$ and $(3 - \beta)$ allows us to discard the ideals $\mathfrak{p}_5$ and $\mathfrak{p}_7$ as well, so we see that $[\mathfrak{p}_3]$ generates the class group. We claim that this ideal is not principal, which will imply that $\mathrm{Cl}(\mathcal{O}_K) \cong \mathbb{Z}/3\mathbb{Z}$.

To show our claim, we construct a fundamental unit, of which we only prove that it generates $\mathcal{O}_K^*/(\mathcal{O}_K^*)^3$, an abelian group of order 3 by Dirichlet. Consider the ideals $(4 - \alpha)$ and $(-\alpha)$. The ideals $\mathfrak{p}_2$ and $\mathfrak{q}_2$ correspond to the evaluations $\mathbb{Z}[\beta] \to \mathbb{Z}/2\mathbb{Z}$ sending β to 0 and 1, respectively. These evaluations extend to $\mathcal{O}_K$ to send $\alpha = (\beta^2 - 2\beta - 2)/3$ to 0 and 1, respectively. Using this, we conclude that $(4 - \alpha)$ and $(-\alpha)$ generate the same ideal $\mathfrak{p}_2^3$. Taking the quotient, we get the fundamental unit $u = \alpha/(4 - \alpha) = 1 + \alpha + \beta$. Try yourself to find similar relations! We show that u generates $\mathcal{O}_K^*/(\mathcal{O}_K^*)^3$. This is not difficult; modulo the prime $\mathfrak{p}_7$, u is sent to 2, which is not a third power.

Now suppose that $\mathfrak{p}_3 = (x)$ were principal. Since $\mathfrak{p}_3^3 = (3)$, then we would have that either 3, $3u$ or $3u^{-1}$ is a third power in $\mathcal{O}_K$. The first possibility can be excluded using $\mathfrak{p}_7$ again. Consider the unique prime $\mathfrak{p}_{13} = (13, \beta - 2) = (13, \alpha + 5)$ of norm 13 above 13. Under the corresponding evaluation, u is sent to $1 - 5 + 2 = -2$, and now we note that $3u = -6$ is not a cube modulo 13. To exclude $3u^{-1}$, use the unique prime $\mathfrak{p}_{31} = (31, \beta - 6) = (31, \alpha + 3)$ of norm 31 above 31. Under the corresponding evaluation, u is sent to $1 - 3 + 6 = 4$, and $3u^{-1}$ to -7, which is not a cube modulo 31. This concludes our determination of $\mathrm{Cl}(\mathcal{O}_K) \cong \mathbb{Z}/3\mathbb{Z}$.

To conclude, we factor an ideal in $\mathcal{O}_K$. Let $I = (-\alpha^2 + 5\alpha + 18, 15\beta^2 + 28\beta + 8)$. The ideals generated by these elements have norm $2^6 3^1 7^2$ and $2^2 3^2 7^2 179$, respectively, so the only primes that can divide I are over 2, 3, and 7. By uniqueness of the prime ideal $\mathfrak{p}_3$ over 3, the factor $\mathfrak{p}_3$ occurs in the factorization of I with multiplicity 1.

Looking above 7, we see that neither of the generators of I is sent to 0 under the evaluation $\alpha \mapsto -2$, $\beta \mapsto 3$ corresponding to $\mathfrak{p}_7$. So $\mathfrak{q}_{49}$ divides both generators, hence I itself, and for reasons of norm, we see that it occurs in the factorization of I with multiplicity 1.

Looking above 2, we see that neither of the generators of I is sent to 0 under the evaluation $\alpha \mapsto 1$, $\beta \mapsto 1$ corresponding to $\mathfrak{q}_2$. So $\mathfrak{p}_2$ divides both generators, hence I itself, and for reasons of norm, we see that it occurs in the factorization of I with multiplicity 2. We have obtained the factorization $I = \mathfrak{p}_2^2 \mathfrak{p}_3 \mathfrak{p}_7$.

2.7 The Pell equation

Let $d \neq \{0, 1\}$ be squarefree. All our troubles allow us to find the solutions of the *Pell equation* $x^2 - dy^2 = \pm 1$. After our experience with number rings, we immediately recognize the left hand side as the norm form $\mathrm{nm}(x + y\sqrt{d})$ in the ring $\mathbb{Z}[\sqrt{d}]$. Even better, solving this equation comes down to finding the units in the ring $\mathbb{Z}[\sqrt{d}]$.

This makes it extremely simple to describe the solutions; they form an abelian group as in the Dirichlet unit theorem, and solving the equation is only difficult if $d > 0$, in which case it boils down to finding a generator of $\mathcal{O}_K^* / < -1 >$, otherwise known as a *fundamental unit*. In Example 2.6.4, we have therefore actually solved the Pell equation for $d = 35$ by finding the fundamental unit $6 - \sqrt{35}$ of $\mathbb{Z}[\sqrt{35}]$!

2.8 Sums of squares

Another classical question is to determine those primes that are sums of squares. This problem has many beautiful solutions and is an excellent illustration of the notions of UFD and PID. Note that we can certainly restrict to odd p, because you may remember from earlier in your career that $1 + 1 = 2$. We are now interested in finding integral solutions x and y to the equation

$$x^2 + y^2 = p. \tag{2.8.1}$$

2.8.1 Congruence arguments

One of the first useful techniques in number theory is to look locally. On the most basic level, this means that one check what are the possible solutions of a given equation modulo a power of a suitable prime.

For the equation (2.8.1), the prime power $4 = 2^2$ turns out to be very useful, because modulo 4, all squares are in $\{0, 1\}$. This means that the sums of two squares are always in $\{0, 1, 2\}$, which gives our first useful result:

Proposition 2.8.1. *No prime congruent to* 3 *mod* 4 *is a sum of two squares.*

We have $5 = 2^2 + 1^2$, $13 = 3^2 + 2^2$, $17 = 4^2 + 1^2$, $29 = 5^2 + 2^2$, $37 = 6^2 + 1^2$, and this nice pattern does not continue, but still $41 = 5^2 + 4^2$ et cetera, which leads us to conjecture that all primes congruent to 1 mod 4 are the sum of two squares.

2.8.2 A UFD proof

Now the algebraic number theory comes in. We rewrite (2.8.1) as

$$(x + iy)(x - iy) = p, \tag{2.8.2}$$

an equality in the Euclidean ring (hence PID and UFD) $\mathbb{Z}[i]$. We can now prove our conjecture. First we note that (2.8.2) has a non-zero solution modulo p because we showed in the exercises that $x^2 + 1 = 0$ has a solution modulo p. This means that p is not prime in $\mathbb{Z}[i]$, because the polynomial $x^2 + 1$ factors modulo p to express p as a product of to prime ideals, by the Kummer–Dedekind theorem. Alternative, we can lift the given solution to $\mathbb{Z}$ to obtain an element $x + iy$ such that p divides neither of $x + iy$ or $x - iy$, but does divide their product.

So we can factor $p = \pi_1\pi_2$ into irreducibles. Since $\mathrm{nm}(p) = p^2$ and the elements of norm 1 in $\mathbb{Z}[i]$ are units, we see that we have $\mathrm{nm}(\pi_1) = \mathrm{nm}(\pi_2) = p$. So if we let $\pi_1 = x_1 + iy_1$ and $\pi_2 = x_2 + iy_2$, then (x_1, y_1) and (x_2, y_2) are both solutions to (2.8.1).

2.8.3 A PID proof

There is another way to make the reduction modulo p trick work. Consider the ideal $p\mathbb{Z}[i]$ of $\mathbb{Z}[i]$. We try to determine the ideals of $\mathbb{Z}[i]$ containing p, which are in bijective correspondence with the ideals of $\mathbb{Z}[i]/p\mathbb{Z}[i]$.

Repeating our usual trick, we write $\mathbb{Z}[i]/p\mathbb{Z}[i] = \mathbb{Z}[x]/(p, x^2 + 1) = (\mathbb{Z}/p\mathbb{Z})[x]/(x^2 + 1)$. We have seen that if $p = 1$ mod 4, then the polynomial $x^2 + 1$ has a root r modulo p. We can therefore use the Chinese remainder theorem to write

$$\begin{aligned}(\mathbb{Z}/p\mathbb{Z})[x]/(x^2 + 1) &= (\mathbb{Z}/p\mathbb{Z})[x]/(x + r)(x - r)\\ &\cong (\mathbb{Z}/p\mathbb{Z})[x]/(x + r) \times (\mathbb{Z}/p\mathbb{Z})[x]/(x - r)\\ &\cong (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z}).\end{aligned} \tag{2.8.3}$$

Now let I be an ideal of $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$. If I contains an element of the form $(a, 0)$ with $a \neq 0$ then it contains all such elements, since $\mathbb{Z}/p\mathbb{Z}$ is a field. If I contains an element of the form $(0, b)$ with $b \neq 0$ then it contains all such elements, since $\mathbb{Z}/p\mathbb{Z}$ is a field. So if I contains an element of the form (a, b) with $a \neq 0$, $b \neq 0$, then it is all of $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$.

We conclude that $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$ has exactly two non-trivial ideals, namely $(\mathbb{Z}/p\mathbb{Z}) \times 0$ and $0 \times \mathbb{Z}/p\mathbb{Z}$. So exist exactly two ideals I_1, I_2 of $\mathbb{Z}[i]$ strictly in-between $p\mathbb{Z}[i]$ and $\mathbb{Z}[i]$. Since $\mathbb{Z}[i]$ is a Euclidean domain, it is a principal ideal domain. Therefore we can write $I_1 = (\pi_1)$ and $I_2 = (\pi_2)$. Now note that we must have $\mathrm{nm}(\pi_1) = \mathrm{nm}(\pi_2) = p$. Otherwise either $\mathrm{nm}(\pi_1) = 1$, in which case we would have $I_1 = \mathbb{Z}[i]$, or $\mathrm{nm}(\pi_2) = 1$, which is out for the same reason, or alternatively because we have would then have $p\mathbb{Z}[i] = \pi_1\pi_2\mathbb{Z}[i]$ by Kummer–Dedekind, whence $p\mathbb{Z}[i] = \pi_1\mathbb{Z}[i]$. At this point, you will be able to find many other versions of this proof.

So we solved the equation (2.8.1) for primes. As a challenge (certainly not an insuperable one) you can amuse yourself by determining for which *integers* n the equation $x^2 + y^2 = n$ has integral solutions. Also try to see in how far the resulting solutions are unique.

2.9 Integral points on elliptic curves

In this section, we will find the integral solutions of some equations of the form

$$y^2 = x^3 + d. \tag{2.9.1}$$

Such an equation defines a so-called *elliptic curve* over $\mathbb{Q}$, on which we try to find the integral points. Our solution method is always to rewrite the equation as $(y+\sqrt{d})(y-\sqrt{d}) = x^3$ and then to use appropriate unique factorization arguments in the ring of integers of the number field $\mathbb{Q}(\sqrt{d})$. Of course this may not be a unique factorization domain, but first we treat some examples where it is to fix the idea.

2.9.1 Using unique factorization of elements

We first solve the equation

$$y^2 = x^3 + 1. \tag{2.9.2}$$

by rewriting this as

$$(y+i)(y-i) = x^3 \tag{2.9.3}$$

in the ring $\mathbb{Z}[i]$. This ring is a Euclidean domain and hence a UFD. We now follow a step-by-step approach that is useful in general.

Step 1 y cannot be odd. For this, look modulo 4 to see that in that case y^2+1 would be 2 mod 4, which is not a third power.

Step 2 $(y+i)$ and $(y-i)$ are coprime. Indeed, a common divisor divides $2i$, which is the square of the element $(1+i)$, which has norm 2 and is therefore prime. So if a non-trivial common divisor were to exist at all, then $(1+i)$ would be one. Suppose that $1+i$ divides $y+i$. Writing this out yields $y+i = (a+bi)(1+i) = (a-b)+(a+b)i$. But this would imply that $y = a-b = a+b-2b = 1-2b$ is odd.

Step 3 $(y+i)$ and $(y-i)$ are both cubes. This is true because in the UFD $\mathbb{Z}[i]$, we can write $x^3 = u^3 \prod_i \pi_i^{3n_i}$. If some π_i divides $y+i$, then it does not divide $y-i$ by coprimality. So both are of the form $y+i$ and $y-i$ are of the form $v\prod_i \pi_i^{3n_i}$ as well. This is a cube because the unit group of order 4 of $\mathbb{Z}[i]$ is of order coprime to 3.

Step 4 $(x,y) = (1,0)$ is the only solution. We can conclude this because by our preceding work we have $y+i = (a+bi)^3 = (a^3-3ab^2)+(3a^2b-b^3)i$. This shows that $b = \pm 1$, and then finding the solutions is just a finite check.

This works great, so we continue this approach by solving the equation

$$y^2 = x^3 - 19. \tag{2.9.4}$$

In the ring $\mathbb{Z}[\sqrt{-19}]$, we write $\alpha = \sqrt{-19}$. We can then factor the equation as $(y+\alpha)(y-\alpha) = x^3$.

Step 1 y is not divisible by 19. For this, look modulo 19 to see that then $x = 0$ mod 19. Then look modulo 19^2 to see that $x^3 - 19 = -19$ mod 19^2, which is not a third power.

Step 2 $(y+\alpha)$ and $(y-\alpha)$ are coprime. Indeed, a common divisor divides 2α, which factors into irreducibles as $2 \cdot \alpha$ (check this!). First of all, 2 does not divide $y+\alpha$ in $\mathbb{Z}[\alpha]$. Second, suppose that α divides $y+\alpha$. Then we get an equality $y+\alpha = (a+b\alpha)\alpha = -19b + \alpha a$, which is in contradiction with Step 1.

Step 3 $(y+\alpha)$ and $(y-\alpha)$ are both cubes. Here we can copy-paste: the units ±1 are still all cubes.

Step 4 The equation has no solutions. This follows because this time around we get $y+\alpha = (a^3 - 57ab^2) + (3a^2b - 19b^3)\alpha$. Therefore again $b = \pm 1$, which this time around yields no solutions.

This is also great, but $18^2 + 19 = 7^3$. Our mistake was to assume that $\mathbb{Z}[\alpha]$ is a UFD. Still, this is almost true, because $\mathbb{Z}[\frac{1+\alpha}{2}]$ is a UFD, and in Exercise 2 of Assignment 1 it is shown how this can be used to find all integral solutions of $y^2 = x^3 - 19$.

2.9.2 Using unique factorization of ideals

As an application of the usefulness of the class group, we show how it can be used to determine integral points beyond the UFD case. We solve

$$y^2 = x^3 - 56. \tag{2.9.5}$$

We of course write this as

$$(y+2\alpha)(y-2\alpha) = x^3 \tag{2.9.6}$$

over the ring of integers $\mathcal{O}_K = \mathbb{Z}[\sqrt{-14}]$ of the quadratic field $K = \mathbb{Q}(\sqrt{-14})$. We have determined the class group of $\mathcal{O}_K$ in Example 2.6.2; it is a cyclic group of order 4, generated by one of the ideals $[\mathfrak{p}_3]$ over 3> We will now put this to use. In what follows, we denote $\sqrt{-14}$ by α, as in Example 2.6.2.

Step 1 We are in a hurry and skip this.

Step 2a coprimality of factors on the left hand side. Consider the ideals $(y+2\alpha)$ and $(y-2\alpha)$. Any ideal that divides (that is, contains) both also contains 4α. Using norms and the uniqueness of the prime ideals above 2 and 7, we see that $(4\alpha) = \mathfrak{p}_2^5\mathfrak{p}_7$.

If $\mathfrak{p}_7$ is a factor of $(y+2\alpha)$, then also of x. So the norm of x would be divisible by 7, and hence x itself since x is an integer. Look modulo 49 to see that this cannot happen. Alternatively, since $\mathfrak{p}_7$ is the unique prime of $\mathcal{O}_K$ above 7, we have that $\mathfrak{p}_7$ divides $(y+2\alpha)$ if and only if it divides $(y-2\alpha)$, since these elements have the same norm.

Unfortunately, proving that $\mathfrak{p}_2$ does not divide both $(y+2\alpha)$ and $(y-2\alpha)$ is not possible. Let us first assume that $\mathfrak{p}_2$ is not in the gcd and continue. Note that in this case y certainly cannot be even, since then $(y+2\alpha)$ and $(y-2\alpha)$ would both be divisible by $(2) = \mathfrak{p}_2^2$, hence by $\mathfrak{p}_2$ as well.

Step 3a : Assuming coprimality, we factor both sides of (2.9.6) into ideals. Then by coprimality we see that both $(y+2\alpha) = I^3$ and $(y-2\alpha) = J^3$ are third powers as ideals. These third powers are principal ideals. Now because the class group $\mathrm{Cl}(\mathcal{O}_K)$ has order coprime to 3, this means that both I and J themselves are principal.

Step 4a : Since all units of $\mathbb{Z}[\alpha]$ are third powers, there therefore exists integral a and b such that $y + 2\alpha = (a + b\alpha)^3 = (a^3 - 42ab^2) + (3a^2b - 14b^3)\alpha$. The factor $3a^2 - 14b^2$ of $3a^2b - 14b^3$ cannot be equal to ± 2 because y, and hence hence a, is odd. So b equals ± 2, which does not lead to any solutions.

Step 2b So now we suppose that $\mathfrak{p}_2$ does divide both $(y + 2\alpha)$ and $(y - 2\alpha)$. Taking norms, we see that y is even, and therefore so is x. Write $y = 2y_0$, $x = 2x_0$ to end up with the equation $y_0^2 = 2x_0^3 + 14$. Factor for

$$(y_0 + \alpha)(y_0 - \alpha) = 2x_0^3. \tag{2.9.7}$$

Let G be the gcd of the ideals $(y_0 + \alpha)$ and $(y_0 - \alpha)$. As above, we see that $\mathfrak{p}_7$ does not divide G. We now determine the multiplicity of $\mathfrak{p}_2$ in the factorization of G.

Looking modulo 4, we see that x_0 cannot be even again. This means that the ideal (x_0) does not contain the unique ideal $\mathfrak{p}_2$ above 2. Then factor $(2) = \mathfrak{p}_2^2$ to see that $2x_0^3$ contains $\mathfrak{p}_2$ with multiplicity 2 in its factorization. Using the uniqueness of the prime above 2, which divides the elements $(y_0 \pm \alpha)$ with the same multiplicity, we conclude that the multiplicity of $\mathfrak{p}_2$ in G is exactly one.

Alternatively, G divides $2\alpha = \mathfrak{p}_2^3\mathfrak{p}_7$, so the multiplicity of $\mathfrak{p}_2$ in the factorization of G is at most 3. If the multiplicity were 2 (respectively 3), then the product $(y_0 + \alpha)(y_0 - \alpha)$ would contain $\mathfrak{p}_2$ with multiplicity 4 (respectively 6). But on the other hand, this product equals $(2x_0^3)$, in which $\mathfrak{p}_2$ occurs with multiplicity $2 + 3k$ for some integer k. This is a contradiction, and therefore we again conclude that the multiplicity of $\mathfrak{p}_2$ in G is exactly one.

For the same reason as above, these ideals are not contained in $\mathfrak{p}_7$. So in this case the gcd of $(y_0 + \alpha)$ and $(y_0 - \alpha)$ equals $\mathfrak{p}_2$.

Step 3b We now attempt factorization once more. Write $(y_0 + \alpha) = \mathfrak{p}_2 I_0$, $(y_0 - \alpha) = \mathfrak{p}_2 J_0$. Then I_0 and J_0 are coprime and in the ideal class $-[pp_2] = [\mathfrak{p}_2]$ since $(y_0 + \alpha)$. We have $-[pp_2] = [\mathfrak{p}_2]$ since $[\mathfrak{p}_2] = 2[\mathfrak{p}_3]$ has order 2 in $\mathrm{Cl}(\mathcal{O}_K)$. We also have that $\mathfrak{p}_2 I_0 \mathfrak{p}_2 J_0 = (2)(x_0)^3 = \mathfrak{p}_2^2(x_0)^3$. So $I_0 J_0 = (x_0)^3$, which is a principal ideal and a third power. Since I_0 and J_0 are coprime (finally!) we know by unique factorization of ideals that there exist ideals I_1 and J_1 such that $I_0 = I_1^3$ and $J_0 = J_1^3$. Since third powering sends the class $[\mathfrak{p}_2]$ of $\mathrm{Cl}(\mathcal{O}_K)$ to itself, we see that I_1 and J_1 are again in the class $[\mathfrak{p}_2]$. So $2(y_0 + \alpha) = \mathfrak{p}_2^3 I_0 = \mathfrak{p}_2^3 I_1^3$ is the third power of a principal ideal. Since the units in $\mathcal{O}_K$ are all cubes, we see that $2(y_0 + \alpha)$ is a third power in $\mathcal{O}_K$.

Step 4b Now we can write $2(y_0 + \alpha) = (a + b\alpha)^3 = (a^3 - 42ab^2) + (3a^2b - 14b^3)\alpha$. Factorizing $3a^2b - 14b^3$, we find that $b = \pm 1$. Writing out the corresponding solutions and translating back to x and y, we see that the equation $y^2 = x^3 - 56$ has exactly two solutions $(x, y) = (18, \pm 76)$ in integers.

If the cardinality of the class group is not coprime with 3, then one typically gets infinitely many points on the curve.

2.10 Calculating Galois groups

A final instance where the theory of number rings comes is a very useful practical tool is in calculating Galois groups of irreducible polynomials. Consider such a polynomial, and call it f. Construct the corresponding number field $K = \mathbb{Q}[x]/(f)$ and consider the ring of integers $\mathcal{O}_K$. The technique is to consider a prime $\mathfrak{p}$ of $\mathcal{O}_K$ such that $\mathfrak{p}^2$ does not divide the prime ideal (p) generated by the rational prime $(p) = \mathfrak{p} \cap \mathbb{Z}$. Such a prime is called unramified, and Kummer–Dedekind shows that almost all primes of a number rings are non-ramified. The quotient ring $\mathcal{O}_K/\mathfrak{p}$ is a field because $\mathfrak{p}$ is maximal, and it contains $\mathbb{Z}/p\mathbb{Z}$ as a subfield.

The automorphism group of $\mathcal{O}_K/\mathfrak{p}$ is very simple; it is generated by the Frobenius automorphism $x \mapsto x^p$. The theory of number rings can be used to show that this automorphism group injects into the Galois group of K over $\mathbb{Q}$, and one can describe this injection very precisely up to conjugation in $\mathrm{Gal}(K|\mathbb{Q})$. Ranging over enough primes, this gives a very quick way to find out if the Galois group of f is the full symmetric group, and explicit results by Chebotarev can be exploited to conclude in the (more difficult) case where the Galois group is smaller.

Beyond the vague outline above, this subject is beyond the scope of these notes, but let me just refer to [3, Chapter 8] for a concise and complete exposition.

Chapter 3

Beyond

In this chapter, we consider a few more generalizations and applications of algebraic number theory. We do not always give complete proofs.

3.1 DVRs

In this section, we will prove the Kummer–Dedekind theorem. The fundamental technique used is localization, which is useful for much more general rings than number fields. For the sake of simplicity, we restrict to considering domains.

So let R be a domain, and let S be a multiplicative subset of R. This means that $1 \in S$ and that if $s_1, s_2 \in S$, then so is $s_1 s_2$.

Example 3.1.1. (i) The simplest example is obviously a set S of the form $S = \{f\}_{n \in \mathbb{N}}$, where $f \in R$ is arbitrary. In algebraic geometry, localizing at such an S corresponds to considering certain open subset of the geometric object corresponding to R. However, we will focus on the following example.

(ii) Let $\mathfrak{p}$ be a prime ideal. Then by the very definition of a prime ideal, the complement $S = R \backslash \mathfrak{p}$ is a multiplicative subset.

Definition 3.1.2. Let R be a domain with fraction field K and let S be a multiplicative subset of R. The localization of R at S is the subring

$$S^{-1}R = \left\{ \frac{r}{s} \in K : r \in R, s \in S \right\}. \tag{3.1.1}$$

of K. By abuse of terminology, if $\mathfrak{p}$ is a prime ideal of R then the localized ring $S^{-1}R$ for $S = R \backslash \mathfrak{p}$ is called the localization of R at $\mathfrak{p}$.

By construction, every element of S is invertible in $S^{-1}R$, so one does not "see" the ideals of R intersecting S in $S^{-1}R$ since they contain a unit. Formally, let $\mathrm{Id}(R)$ be the set of integral ideals of R and let $\mathrm{Id}(S^{-1}R)$ be the set of ideals of $S^{-1}R$. (Note that this time $\mathrm{Id}(R)$ consists only of integral ideals, contrary to the situation in Section 1.7 where it denoted the group of fractional ideals. This minor inconsistency is perhaps forgivable.) Consider the map $\varphi : \mathrm{Id}(R) \to \mathrm{Id}(S^{-1}R)$ given by $\varphi(I) = S^{-1}I = \left\{ \frac{i}{s} \in K : i \in I, s \in S \right\}$ and the map $\psi : \mathrm{Id}(S^{-1}R) \to \mathrm{Id}(R)$ given by $\psi(J) = R \cap J$. Also, let $\mathrm{Id}_S(R)$ be the set of ideals of R that do not intersect S.

Proposition 3.1.3. *(i) $S^{-1}I$ is the unit ideal if and only if $I \cap S \neq \emptyset$, so if and only if $I \notin \mathrm{Id}_S(R)$.*

(ii) Every ideal of $S^{-1}R$ is of the form $S^{-1}I$. More precisely, the map $\varphi\psi$ is the identity map on $\mathrm{Id}(S^{-1}R)$.

(iii) The maps φ and ψ induce bijections between the prime ideals in $\mathrm{Id}_S(R)$ *and the prime ideals in* $\mathrm{Id}(S^{-1}R)$*. More precisely, the map $\varphi\psi$ is the identity map on the subset of* $\mathrm{Id}_S(R)$ *consisting of prime ideals.*

Proof. (i) : $S^{-1}I$ is the unit ideal if and only if it contains 1, which is to say, if and only if $1 = i/s$ for some $i \in I$ and $s \in S$.

(ii) : We have to show that if J is an ideal of $S^{-1}R$, we have $J = S{-}1(R \cap J)$. If $x = r/s \in J$, with $r \in R$ and $s \in S$, then we have $r = (r/s)s$, so $r \in R \cap J$. Conversely, if $r/s \in S{-}1(R \cap J)$, with $r \in R \cap J$ and $s \in S$, then $r \in R \cap J \subseteq J$, and $1/s \in S^{-1}R$, so $r/s = (1/s)r \in J$ because J is an ideal of $S^{-1}R$.

(iii) : We have to show that if $\mathfrak{p}$ is a prime ideal of R, we also have the equality $\mathfrak{p} = R \cap S^{-1}\mathfrak{p}$. Since $\mathfrak{p} \subseteq S^{-1}\mathfrak{p}$, the inclusion $\mathfrak{p} \subseteq R \cap S^{-1}\mathfrak{p}$ is trivial. Conversely, suppose that $r \in R \cap S^{-1}\mathfrak{p}$. Then we can write $r = p/s$ with $p \in \mathfrak{p}$ and $s \in S$. Now if $r \notin \mathfrak{p}$, then the equality $p = rs$ is in contradiction with $\mathfrak{p}$ being prime. So $r \in \mathfrak{p}$ and our claim is proved. □

Corollary 3.1.4. *Let R be a domain, and let $\mathfrak{p}$ be a prime ideal of R. Then the localization $R_{\mathfrak{p}}$ has a unique maximal ideal $\mathfrak{p}R_{\mathfrak{p}}$. In other words, every element of $R_{\mathfrak{p}}$ that is not in $\mathfrak{p}R_{\mathfrak{p}}$ is a unit.*

Proof. We have just seen that the ideals of $R_{\mathfrak{p}}$ are exactly the ideals that do not intersect $S = R\backslash\mathfrak{p}$. There is a unique maximal such ideal, namely $\mathfrak{p}$ itself. The correspondences from Proposition 3.1.3 now give what we want. □

Let R be a domain, let $\mathfrak{p}$ be a prime ideal of R, and let S be the complement $R\backslash\mathfrak{p}$. Then the localized ideals $I_{\mathfrak{p}} = S^{-1}I$ contain enough information to reconstruct I.

Theorem 3.1.5. *Let R be a domain, and let I be a fractional ideal of R. Then we have the equality*

$$I = \bigcap_{\mathfrak{m}} I_{\mathfrak{m}} \tag{3.1.2}$$

where $\mathfrak{m}$ runs over the maximal ideals of R.

Proof. One inclusion is obvious, since I injects into $I_{\mathfrak{m}}$ for all $\mathfrak{m}$. Conversely, let α be in the intersection. We want that $\alpha \in I$. Another way of saying this is that the denominator ideal

$$D = \{r \in R : r\alpha \in I\} \subseteq R \tag{3.1.3}$$

contains 1. If not, then D would be contained in a maximal ideal $\mathfrak{m}$ of R. But $\alpha \in I_{\mathfrak{m}}$, so we can write $\alpha = i/s$ with $i \in I$ and $s \in R\backslash\mathfrak{m}$. The element s of D does not belong to $\mathfrak{m}$. Contradiction. □

In the number field case, the intersection from the theorem simply runs over the non-zero prime ideals; this is a consequence of Proposition 1.7.6(D3).

We note the following technical corollary, which is not as obvious as one would like. In fact, we have to impose the demand that R be a number ring.

Corollary 3.1.6. *Let R be a number ring, and let $\mathfrak{p}$ be a prime ideal of R. Then $\mathfrak{p}^n = \mathfrak{p}^n R_{\mathfrak{p}} \cap R$ for all $n \in \mathbb{N}$.*

Proof. Let $I = \mathfrak{p}^n R_\mathfrak{p} \cap R$. Then by Proposition 3.1.5(ii) we have $I_\mathfrak{p} = \mathfrak{p}^n R_\mathfrak{p}$. This is also the localization of $\mathfrak{p}^n$. Now let $\mathfrak{q} \neq \mathfrak{p}$ be another prime ideal. Then we cannot have that $\mathfrak{p}^n \subseteq \mathfrak{q}$, since then $\mathfrak{p} \subseteq \mathfrak{q}$ by the prime ideal property, and therefore $\mathfrak{p} = \mathfrak{q}$ because R is a number ring (see Proposition 1.7.6(D3)). So $\mathfrak{p}^n R_\mathfrak{q} = R_\mathfrak{q}$ by Proposition 3.1.5(i).

Applying Theorem 3.1.5 twice, we see that

$$\mathfrak{p}^n = \mathfrak{p}^n R_\mathfrak{p} \cap \bigcap_{\mathfrak{q} \neq \mathfrak{p}} R_\mathfrak{q} = \mathfrak{p}^n R_\mathfrak{p} \cap \bigcap_{\mathfrak{q}} R_\mathfrak{q} = \mathfrak{p}^n R_\mathfrak{p} \cap R. \tag{3.1.4}$$

□

Note that we are *not* claiming that $\mathfrak{p}^n = (\mathfrak{p}R_\mathfrak{p})^n \cap R$, although that will be true in the situation (described later) when $R_\mathfrak{p}$ is a DVR.

Some properties of rings are local, in the sense that they hold for R if and only if they hold for all its localizations $R_\mathfrak{p}$. The next theorem shows that being integrally closed is a local property. In fact, the situation is even better, since we only have to consider maximal ideals (which are just the non-zero prime ideals if R is a number ring).

Theorem 3.1.7. *Let R be a domain. Then R is integrally closed if and only if all the localizations $R_\mathfrak{m}$ at maximal ideals are integrally closed.*

Proof. To see the "if"-part, we have $R = \cap_\mathfrak{m} R_\mathfrak{m}$, where the $R_\mathfrak{m}$ have the same field of fractions K as R. Now if $\alpha \in K$ is integral over R, then it is integral over all $R_\mathfrak{m}$ as well. But then it is in $\cap_\mathfrak{m} R_\mathfrak{m} = R$.

Conversely, suppose that R is integrally closed. Let $\mathfrak{p}$ be a prime ideal of R, let $S = R \backslash \mathfrak{p}$, and suppose that $\alpha \in K$ is integral over $R_\mathfrak{p}$. Then we have $\alpha^n = \sum c_k \alpha^k$ for some $c_k \in R_\mathfrak{p}$. We can write $c_k = r_k/s_k$, and replacing the s_k by the finite product $s = \prod_k s_k$ if necessary, we may assume that s_k is identical for all k. Then $sc_k \in R$. But we also have $(s\alpha)^n = \sum_k c_k s^{n-k} (s\alpha)^k$, where this time $c_k s^{n-k} \in R$ since $n - k > 0$. So $s\alpha$ is integral over R. But then $s\alpha \in R$ and so $\alpha = (s\alpha)/s \in R_\mathfrak{p}$. □

We again see the usefulness of the scaling trick from Proposition 1.4.1. Invertibility is also a local property.

Theorem 3.1.8. *Let $I = (\alpha_1, \ldots, \alpha_n)$ be a finitely generated fractional ideal of a domain R. Then I is invertible if and only if all its localizations $I_\mathfrak{m}$ at the maximal ideals $\mathfrak{m}$ of R are all principal.*

Proof. First suppose that I is invertible, and let $\mathfrak{p}$ be a prime ideal of R. Then $1 = \sum \alpha_i \beta_i$ for some elements β_i of I^{-1}. Not all products $\alpha_i \beta_i$ are in $\mathfrak{p}$, because then so would be their sum. Say that $\alpha_1 \beta_1 \in R \backslash \mathfrak{p}$. Then also $\alpha_1 \beta_1 \in R_\mathfrak{p} \backslash \mathfrak{p} R_\mathfrak{p}$, which equals the unit group $R_\mathfrak{p}^*$ by Corollary 3.1.4. Now let $\alpha \in I$ be arbitrary. Then $\alpha = \alpha_1 \cdot \alpha\beta_1 \cdot (\alpha_1\beta_1)^{-1}$, where $\alpha\beta_1 \in II^{-1} \subseteq R \subseteq R_\mathfrak{p}$ and $(\alpha_1\beta_1)^{-1} \in R_\mathfrak{p}^* \subseteq R_\mathfrak{p}$. So $\alpha \in \alpha_1 R_\mathfrak{p}$. Since certainly $\alpha_1 \in I_\mathfrak{p}$, we in fact have $I_\mathfrak{p} = \alpha_1 R_\mathfrak{p}$, which is therefore locally principal.

Conversely, suppose that $I_\mathfrak{m}$ is principal for all $\mathfrak{m}$. Given $\mathfrak{m}$, choose an $\alpha_\mathfrak{m} \in K$ such that $I_\mathfrak{m} = \alpha_\mathfrak{m} R_\mathfrak{m}$. Write $\alpha_i = \alpha_\mathfrak{m}(r_i/s_i)$ with $r_i \in I$ and $s_i \in S = R \backslash \mathfrak{m}$. In fact, because I is finitely generated, we can suppose that all s_i equal a fixed element s, as in the proof of Theorem 3.1.7. Then $(s/\alpha)/\alpha_i = r_i \in R$ for all i, so s/α is in I^{-1}. We conclude that $I^{-1}I$ contains the element $(s/\alpha)\alpha = s$, which is in the complement S of $\mathfrak{m}$.

So on the one hand we have $I^{-1}I \subseteq R$ by the definition of I^{-1}. On the other hand, for all maximal ideals $\mathfrak{m}$ of R the ideal $I^{-1}I$ contains an element outside $\mathfrak{m}$. This means that $I^{-1}I$ cannot be a proper ideal, wherefore $I^{-1}I = R$ and I is invertible. □

Proposition 1.7.6 shows that the hypothesis on I being finitely generated is redundant if R is a number ring. From the proof, we immediately obtain the following.

Corollary 3.1.9. *Let R be a domain, and let $\mathfrak{p}$ be prime ideal of R. Then the invertible ideals of the localization $R_{\mathfrak{p}}$ are exactly the principal ideals.*

As an important consequence of our work so far, we obtain the following local-to-global principle. Given a domain R, we denote the group of invertible ideals of R by $I(R)$, and the group of principal ideals of R by $P(R)$. By Example 1.7.12, we have an inclusion $P(R) \subseteq I(R)$.

Theorem 3.1.10. *Let R be a number ring. Then localization induces the isomorphism*

$$\begin{aligned} I(R) &\longrightarrow \bigoplus_{\mathfrak{p}} I(R_{\mathfrak{p}}) = \bigoplus_{\mathfrak{p}} P(R_{\mathfrak{p}}) \\ I &\longmapsto (I_{\mathfrak{p}})_{\mathfrak{p}}, \end{aligned} \tag{3.1.5}$$

where $\mathfrak{p}$ runs over the non-zero prime ideals of R.

Proof. The sum is direct by Proposition 3.1.3(i) because every invertible ideal contains a non-zero element, which is in the complement of all but finitely many ideals by unique factorization. The identification $I(R_{\mathfrak{p}}) = P(R_{\mathfrak{p}})$ is nothing but Corollary 3.1.9. By Proposition 1.7.6(D3), the non-zero prime ideals of R are nothing but the maximal ideals of R. Therefore injectivity follows from Theorem 3.1.5. Try proving the following statements yourself:

(i) By Noetherianness of R (Proposition 1.7.6(D1)), every ideal of $R_{\mathfrak{p}}$ contains $\mathfrak{p}^n R_{\mathfrak{p}}$ for some sufficiently high power n;

(ii) Localizing ideals is compatible with taking their product; that is, $(IJ)_{\mathfrak{p}} = I_{\mathfrak{p}} J_{\mathfrak{p}}$.

It therefore suffices to show that given an ideal $J_{\mathfrak{p}}$ of $R_{\mathfrak{p}}$, there exists an ideal I of R such that the localization of $I_{\mathfrak{p}}$ equals $J_{\mathfrak{p}}$ and $I_{\mathfrak{q}} = R_{\mathfrak{q}}$ for other non-zero $\mathfrak{q} \neq \mathfrak{p}$. We of course take

$$I = J_{\mathfrak{p}} \cap \bigcap_{\mathfrak{q} \neq \mathfrak{p}} R_{\mathfrak{q}} = J_{\mathfrak{p}} \cap \bigcap_{\mathfrak{q}} R_{\mathfrak{q}} = J_{\mathfrak{p}} \cap R. \tag{3.1.6}$$

We have $I_{\mathfrak{p}} = J_{\mathfrak{p}}$ by Proposition 3.1.3(ii) since $I = J_{\mathfrak{p}} \cap R$. Moreover, since for some n we have $\mathfrak{p}^n R_{\mathfrak{p}} \subset J_{\mathfrak{p}}$, we also have $\mathfrak{p}^n \subseteq I$ because of Corollary 3.1.6.

Now suppose that $\mathfrak{q} \neq \mathfrak{p}$. Then we cannot have $I \subseteq \mathfrak{q}$ since this would imply $\mathfrak{p}^n \subseteq \mathfrak{q}$, whence $\mathfrak{p} \subset \mathfrak{q}$ because $\mathfrak{p}$ is prime, which is impossible by Proposition 1.7.6(D3). We conclude that $I_{\mathfrak{q}} = R_{\mathfrak{q}}$ by Proposition 3.1.3(i). □

It should be clear by now that $\mathfrak{p}$ being invertible implies that the ring $R_{\mathfrak{p}}$ has lots of strong properties. In particular, we obtain as a trivial corollary of Theorem 3.1.8 that $\mathfrak{p}R_{\mathfrak{p}}$ should be a principal ideal. In fact, the ring $R_{\mathfrak{p}}$ is then about about as simple to describe as you could wish:

Theorem 3.1.11. *Let R be a number ring, and let $\mathfrak{p}$ be a non-zero prime of R. Then the following are equivalent:*

(i) $\mathfrak{p}$ is invertible;

(ii) $\mathfrak{p}R_{\mathfrak{p}}$ is principal;

(iii) $R_{\mathfrak{p}}$ is a PID, and every ideal of $R_{\mathfrak{p}}$ is a power of $\mathfrak{p}$;

(iv) There exists a $\pi \in R_{\mathfrak{p}}$ such that every non-zero $\alpha \in K$ admits a unique expression $\alpha = u\pi^n$ with $n \in \mathbb{Z}$ and $u \in R_{\mathfrak{p}}$.

Proof. We know that (i) and (ii) are equivalent by Theorem 3.1.8. Indeed, one implication is clear, and if the localization $\mathfrak{p}R_\mathfrak{p}$ is principal, then so is $\mathfrak{p}$ itself by Theorem 3.1.8; at the other non-zero primes $\mathfrak{q}$ of R we have $\mathfrak{p}_\mathfrak{q} = R_\mathfrak{q}$ as in the proof of Corollary 3.1.6.

So suppose that either of (i) or (ii) holds. Then we can write $\mathfrak{p}R_\mathfrak{p} = \pi R_\mathfrak{p} = (\pi)$ for some $\pi \in R_\mathfrak{p}$. (Concretely, this means that the fractional ideal generated by π considered as an element of K contains the prime factor $\mathfrak{p}$ exactly once in its factorization, along with perhaps some other prime ideals, either to positive or negative powers.) We obtain a chain $R \supset (\pi) \supset (\pi^2) \supset \ldots$. It is easy to shows (but you should check this!) that all the inclusions in this chain are proper.

Using Noetherianness as in the proof of Theorem 3.1.10, there is a maximal n such that I is contained in (π^n). Now suppose that $r \in I \backslash (\pi^{n+1})$. Then we have $r = a\pi^n$ since $r \in I$, but a is not in (π) since r is not in (π^{n+1}). Therefore $a \in R_\mathfrak{p} \backslash (\pi) = R_\mathfrak{p} \backslash \mathfrak{p}R_\mathfrak{p}$, which equals $R_\mathfrak{p}^*$ by Corollary 3.1.4. So I contains $(\pi^{n+1}, a\pi^n) = (\pi^n)$, and since we already had the converse inclusion, we see that $I = (\pi^n)$. We have proved (iii).

To show that (iii) implies (iv) proceeds along the same lines, and you are invited to fill in the details to the following argument. Write $\mathfrak{p}R_\mathfrak{p} = (\pi)$ as before. Given α, we take a sufficiently large power π^n such that $r = \pi^n \alpha$ is in $R_\mathfrak{p}$. Then by (ii), we can write $(r) = (\pi)^m = (\pi^m)$ for some m. Hence $r = u\pi^m$ for some $u \in R_\mathfrak{p}^*$ and $\alpha = u\pi^{m-n}$.

For the final implication, assume (iv). The element π^{-1} and its positive powers are not in $R_\mathfrak{p}$, so in fact $R_\mathfrak{p}$ consists of the expressions $u\pi^n$ with n positive. Since π is not a unit, we see that it generates the unique maximal ideal, which is $\mathfrak{p}R_\mathfrak{p}$. We conclude by Theorem 3.1.8 that $\mathfrak{p}$ is invertible, since we have just seen that its localization at $\mathfrak{p}R_\mathfrak{p}$ is, and at the other non-zero primes $\mathfrak{q}$ of R we see that $\mathfrak{p}_\mathfrak{q} = R_\mathfrak{q}$ as in the proof of Corollary 3.1.6. We have proved (i). □

Definition 3.1.12. Let R be a domain satisfying property (iii) of Theorem 3.1.11. Then R is called a discrete valuation ring (or DVR).

We are about to prove an amusing result on orders. First we need the following lemma.

Lemma 3.1.13. *A PID is integrally closed.*

Proof. Let R be a PID with field of fractions K, and let $\alpha = r/s$ be an element of K, with $r, s \in R$. If x is integral over R, then there exist a positive n and $a_i \in R$ such that $x^n = \sum_i a_i x^i$. Multiplying out the denominator, we get $r^n = \sum_i a_i r^i s^{n-i} = s \sum_i a_i r^i s^{n-i-1}$, where $\sum_i a_i r^i s^{n-i-1}$. This means that every irreducible element of R that divides s divides r^n, and therefore r, as well. So we can cancel numerator and denominator against one another to obtain that $x \in R$. □

Theorem 3.1.14. *Let R be an order in a number field K. Then the following are equivalent:*

(i) $R = \mathcal{O}_K$;

(ii) all ideals of R are invertible;

(iii) all localizations $R_\mathfrak{p}$ of R at its non-zero prime ideals are DVRs.

Proof. We have seen in Section 1.7 that (i) implies (ii). Also, (ii) implies (iii) by Theorem 3.1.11. Assuming (iii), we see that R is integrally closed in its field of fractions K by Theorem 3.1.7 (here we use that R is an order). Since R certainly contains $\mathbb{Z}$, it equals the integral closure $\mathcal{O}_K$ of $\mathbb{Z}$ in the field K. □

Example 3.1.15. Let $K = \mathbb{Q}(\sqrt{-19})$, let $R = \mathbb{Z}[\sqrt{-19}]$, and let $\mathfrak{p}_2 = (2, 1 + \sqrt{-19})$ be the unique prime above 2. Then $\mathfrak{p}_2 R_{\mathfrak{p}_2}$ cannot be principal, because it is not invertible in light of the fact that $[\mathcal{O}_K : R] = 2$. For all other primes $\mathfrak{q}$ of R, the localization $R_{\mathfrak{q}}$ are DVRs. For an explicit calculation showing that $R_{\mathfrak{p}_2}$ is not a DVR, see [5, Example 2.10].

We need one final lemma, which uses a local version of the methods used to prove Theorem 1.10.3.

Lemma 3.1.16. *Let R be a number ring, and let $\mathfrak{p}$ be a prime of R. Then the inclusion $R \hookrightarrow R_{\mathfrak{p}}$ induces an isomorphism $R/\mathfrak{p} \to R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$. Moreover, if $\mathfrak{p}$ is an invertible prime of R, then $\mathfrak{p}^n R_{\mathfrak{p}} = (\mathfrak{p}R_{\mathfrak{p}})^n$, and for any n, there are bijections (or rather isomorphisms of R-modules) $R/\mathfrak{p} \to \mathfrak{p}^n/\mathfrak{p}^{n+1}$.*

Proof. The injectivity of the map $R/\mathfrak{p} \to R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$ follows from $R = \mathfrak{p}R_{\mathfrak{p}} \cap R$, proved in Corollary 3.1.6. To prove surjectivity, let $r/s \in R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$. We have to find a $t \in R$ such that $(r/s) - t = (r - st)s$ is in $\mathfrak{p}R_{\mathfrak{p}}$. By Proposition 3.1.3(ii) $r - st \in \mathfrak{p}$. But this is not difficult to arrange; one just takes $t \in R$ to be a preimage of the reduction r/s under the surjection $R \to R/\mathfrak{p}$. Note that this reduction is well-defined since s is not in $\mathfrak{p}$.

Now suppose that $\mathfrak{p}$ is invertible, so that $R_{\mathfrak{p}}$ is a DVR and $\mathfrak{p}R_{\mathfrak{p}} = (\pi)$ say. Then $\mathfrak{p}^n$ cannot equal $\mathfrak{p}^{n+1}$, since multiplying sufficiently many times with the inverse of $\mathfrak{p}$, we would get $\mathfrak{p} = R$. Choose an element $r_n \in \mathfrak{p}^n \backslash \mathfrak{p}^{n+1}$. Consider the maps

$$R/\mathfrak{p}^n = R/(\mathfrak{p}^n R_{\mathfrak{p}} \cap R) \longrightarrow R_{\mathfrak{p}}/\mathfrak{p}^n R_{\mathfrak{p}} = R_{\mathfrak{p}}/(\pi^n) \tag{3.1.7}$$

induced by inclusion, and

$$R/\mathfrak{p} \to \mathfrak{p}^n/\mathfrak{p}^{n+1}. \tag{3.1.8}$$

induced by multiplication with r_n. The map (3.1.7) is again injective. The cardinality of its right hand side equals $[R_{\mathfrak{p}} : \pi^n R_{\mathfrak{p}}]$. Since multiplication with π induces isomorphisms $R/(\pi) \to (\pi)^n/(\pi)^{n+1}$ (this is the key point, so although this is very easy, I want you to check this for yourself!), we have that $[R_{\mathfrak{p}} : \pi^n R_{\mathfrak{p}}] = [R_{\mathfrak{p}} : \pi R_{\mathfrak{p}}]^n = [R_{\mathfrak{p}} : \mathfrak{p}R_{\mathfrak{p}}]^n = [R : \mathfrak{p}]^n$. So if we can show that the map (3.1.8) is injective, then we will have equality of indices everywhere, and the Proposition will be proved. But this is not so difficult; $R/\mathfrak{p}$ is a field, and the homomorphism is non-trivial because r_n is not in $\mathfrak{p}^{n+1}$. Therefore its kernel is trivial and we indeed have an injection. □

Of course, locally, the isomorphisms $R/\mathfrak{p} \to \mathfrak{p}^n/\mathfrak{p}^{n+1}$ in Lemma 3.1.16 are very simple; they become the isomorphisms $R/(\pi) \to (\pi)^n/(\pi)^{n+1}$ induced by multiplying with (a unit times) π.

We can now finally give the proof of Theorem 1.8.4. We denote $R = \mathbb{Z}[\alpha]$ in the proof for simplicity.

Proof. (0): We already saw this in Section 1.8.

(1): To show that the product $\prod \mathfrak{p}_i^{e_i} = \prod (p, g_i(\alpha))^{e_i}$ is in (p), it suffices to show that $\prod g_i(\alpha)^{e_i}$ is. But this is true because the reduction $\prod \overline{g}_i^{e_i}$ equals $\overline{f}$, which is zero in $(\mathbb{Z}/p\mathbb{Z})[\alpha]$.

Suppose that we have the equality $\prod \mathfrak{p}_i^{e_i} = (p)$. Then for all $\mathfrak{p}_i$ we can find an integral I such that $\mathfrak{p}_i I = (p)$. So $\mathfrak{p}_i I(p^{-1}) = R$ and $\mathfrak{p}_i$ is invertible (with inverse $I(p^{-1})$) by Proposition 1.7.14. For the converse inclusion, it now suffices to show that both ideals have index p^d in R. Clearly (p) does, so we are done if we can show that $[R_{\mathfrak{p}_i} : \mathfrak{p}_i^{e_i} R_{\mathfrak{p}_i}] = \mathfrak{p}^{e_i \deg(g_i)}$. This follows from Lemma 3.1.16, since

$$\begin{aligned} [R : \mathfrak{p}_i] &= [\mathbb{Z}[\alpha] : (p, g_i(\alpha))] \\ &= [\mathbb{Z}[x] : (g_i, f) \\ &= [(\mathbb{Z}/p\mathbb{Z})[x] : (p, \overline{g}_i, \overline{f}) \\ &= [(\mathbb{Z}/p\mathbb{Z})[x] : (p, \overline{g}_i). \end{aligned} \tag{3.1.9}$$

(2): Write $r_i = ps_i$ for the fundamental relation

$$ps_i(\alpha) = -q_i(\alpha) g_i(\alpha) \tag{3.1.10}$$

between the generators p and $g_i(\alpha)$ of $\mathfrak{p}_i$. This means that if we can show that either of $s_i(\alpha)$ or $q_i(\alpha)$ is a unit in $R_{\mathfrak{p}_i}$, then we can invert to find a *single* generator of $\mathfrak{p}_i R_{\mathfrak{p}_i}$, in which case this ring will be a DVR by Theorem 3.1.11(ii), and $\mathfrak{p}$ will be invertible by Theorem 3.1.11(i).

First suppose that $e_i = 1$. Then $q_i(\alpha)$ is not in $\mathfrak{p}_i$ since it is non-zero in $(\mathbb{Z}/p\mathbb{Z})[\alpha]$. This means that $q_i(\alpha)$ generates the unit ideal in $R_{\mathfrak{p}_i}$ by Proposition 3.1.3(i), so $q_i(\alpha) \in R_{\mathfrak{p}_i}^*$ and we can invert as desired.

Now suppose that r_i is not in $p^2\mathbb{Z}[x]$, or in other words that the image $\overline{s}_i$ is non-zero in $(\mathbb{Z}/p\mathbb{Z})[x]$. We also have that $\overline{g}_i$ does not divide $\overline{s}_i$, because $\overline{s}_i$ is non-zero and of smaller degree than $\overline{g}_i$. This means that $\overline{s}_i$ is not in the ideal $(\overline{g}_i)$ generated by $\overline{g}_i$ in $(\mathbb{Z}/p\mathbb{Z})[x]$. Since $\overline{g}_i$ divides f, this implies that $\overline{s}_i(\alpha)$ is not in the ideal generated by $\overline{g}_i(\alpha)$ in $(\mathbb{Z}/p\mathbb{Z})[\alpha]$ either. This is turn means that $s_i(\alpha)$ is not in the ideal $\mathfrak{p}_i = (p, g_i(\alpha)$ of $\mathbb{Z}[\alpha]$, and we again get an invertible element $s_i(\alpha) \in R_{\mathfrak{p}_i}^*$.

(3): We already saw this in Section 1.8. □

3.2 S-integers

Definition 3.2.1. Let $\mathcal{O}_K$ be the ring of integers of a number field K. Let S be a finite set of primes of $\mathcal{O}_K$. Then we define the ring $\mathcal{O}_{K,S}$ of *S-integers* as

$$\left\{ \alpha \in K : (\alpha) = \prod_i \mathfrak{p}_i^{n_i} \text{ with } n_i \geq 0 \text{ except possibly if } \pi \in S \right\}. \tag{3.2.1}$$

Unique factorization of ideals shows that the $\mathcal{O}_{K,S}$ are still rings. For example, suppose that α and β are both in $\mathcal{O}_{K,S}$, then write $(\alpha) = \prod_i \mathfrak{p}_i^{n_i}$ and $(\beta) = \prod_i \mathfrak{p}_i^{m_i}$. Then $\alpha + \beta$ is an element of $\prod_i \mathfrak{p}_i^{\min(m_i, n_i)}$, which is again of the required form, hence so is the ideal $(\alpha + \beta)$ contained in it.

The rings $\mathcal{O}_{K,S}$ contain $\mathcal{O}_K$. They are still Dedekind rings, and they may still have non-trivial class group and unit group. In fact, the relations are as follows.

Proposition 3.2.2. *$\mathrm{Cl}(\mathcal{O}_{K,S})$ is the quotient of $\mathrm{Cl}(\mathcal{O}_K)$ by the subgroup generated by the primes in S.*

Proof. The idea is that the ideals that one quotients out are exactly those that become trivial as fractional ideals of $\mathcal{O}_{K,S}$. More precisely, it is easy to see that the map $I(\mathcal{O}_K) \to I(\mathcal{O}_{K,S})$ is surjective and with kernel generated by S. To prove the proposition, we have to show that $I(\mathcal{O}_K)/P(\mathcal{O}_K) \to I(\mathcal{O}_{K,S})/P(\mathcal{O}_{K,S})$ also has kernel generated by S. So suppose that I and J are $\mathcal{O}_K$-ideals that become the same in $I(\mathcal{O}_{K,S})/P(\mathcal{O}_{K,S})$. Then $IJ^{-1} = (\alpha) \prod_i \mathfrak{p}_i^{n_i}$ with $\mathfrak{p}_i$ in S and $\alpha \in K$. So up to a principal ideal, I and J do indeed differ by an element of the subgroup generated by S. □

Proposition 3.2.3. *Let r be the number of real embeddings of K, and let s be its number of pairs of complex conjugate embeddings. Then there exists a finite integer w such that $\mathcal{O}_{K,S}^* \cong \mathbb{Z}/w\mathbb{Z} \times \mathbb{Z}^{r+s+|S|-1}$.*

Proof. One essentially repeats the proof of Dirichlet's unit theorem; w is again the number of roots of unity in $\mathcal{O}_{K,S}$, which is in fact the same as the number of roots of unity in $\mathcal{O}_K$. The difference is that for every prime $\mathfrak{p}$, we get a new generator. The reason for this is that $\mathfrak{p}^n$ is principal for a suitable power n, because the class group of $\mathcal{O}_K$ is finite. Choose a generator u. Then u certainly in $\mathcal{O}_{K,S}$, because it is in $\mathcal{O}_K$, but its inverse will be in $\mathcal{O}_{K,S}$ as well, because it generates the ideal $\mathfrak{p}^{-n}$ and negative exponents at $\mathfrak{p}$ are allowed. □

Why study these rings? Because as the result above shows, taking suitable S-integers kills the class group, which is often useful if one can control the situation at the prime that are in S (which one "throws away" by considering $\mathcal{O}_{K,S}$). Also, in the analogous situation of function fields F of algebraic curves, one typically considers a ring $\mathcal{O}_{F,S}$ with S small but non-empty. This gives functions with poles in a specified finite set, which can be studied to find nice defining equations for the curves involved. For an intuitive exposition of these geometric analogues, also see [4, Section 5.1]; apart from the examples there, it is probably fun to mention that passing from an order of a number ring to a maximal order is the exact analogue of desingularizing a curve over a field. Here many vistas open, and if you feel like riding off into this broad sunset, then by all means. . .

Chapter 4

Exercises

4.1 Assignment 1

All rings under consideration are unital. Moreover, they are commutative unless explicitly stated otherwise. Given an element α of a ring R, we denote the smallest subring of R containing α by $\mathbb{Z}[\alpha]$.

Exercise 1. Let $p > 3$ be a prime.

(i) Show that if p is congruent to 2 modulo 3, then p is not of the form $x^2 + xy + y^2$ with x and y integers.

(ii) Suppose from now on that p is congruent to 1 modulo 3. Use Cauchy's theorem to show that the polynomial $x^3 - 1$ has a root mod p different from 1.

(iii) Show that the polynomial $x^2 + x + 1$ has a root mod p.

(iv) Using the Chinese remainder theorem as in the lecture, show that there are two ideals of $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ strictly between $p\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ and $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$.

(v) Use the fact that $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ is a PID to conclude that p is of the form $x^2 + xy + y^2$ if p is congruent to 1 modulo 3.

Exercise 2.

(i) Show that $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ is the subset $\{a + b\frac{1+\sqrt{-19}}{2} : a, b \in \mathbb{Z}\}$ of $\mathbb{Q}(\sqrt{-19})$.

(ii) Show that $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]^* = \{\pm 1\}$. (Hint: consider the small values of the norm function on the subset $\{x + y\sqrt{-19} : 2x \in \mathbb{Z}, 2y \in \mathbb{Z}\}$ of $\mathbb{Q}(\sqrt{-19})$ containing $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$.)

(iii) Modify the proof from the lectures and use the fact that $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ *is* a UFD (unlike $\mathbb{Z}[\sqrt{-19}]$) to show that the only integer solutions to $y^2 = x^3 - 19$ are $(7, \pm 18)$.

Exercise 3.

(i) Consider the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Let $a = ((p-1)/2)!$, considered as an element of $\mathbb{F}_p$. Show that $a^2 = -1$ in $\mathbb{F}_p$ if $p \equiv 1 \mod 4$.

(ii) Now let F be a general field, and let $f \in F[x]$ be a polynomial over F. Show that if r is a root of f, then $x - r$ divides f.

(iii) Show that a polynomial of degree d over a field F admits at most d roots.

(iv) Show that a finite subgroup of the group of units F^* of a field F is cyclic. (Hint: All elements of order d, say, are roots of the polynomial $x^d - 1$. What happens to the number of such elements if the group in question is not cyclic?)

(v) Conclude that $\mathbb{F}_p$ has cyclic unit group, hence contains an element of order 4 if $p \equiv 1 \mod 4$.

Exercise 4.

(i) Let L_1 and L_2 be finite extensions of a field K, both contained in a bigger extension M of K. Let L_1L_2 be the compositum of L_1 and L_2, that is, the smallest subfield of M containing both L_1 and L_2. Show that $[L_1L_2 : L_1] \leq [L_2 : K]$. If you wish, you may assume (though this is not true in general) that $L_1 = K(\beta_1)$ and $L_2 = K(\beta_2)$ are both generated over K by a single element.

(ii) Show that if $[L_1 : K]$ and $[L_2 : K]$ are coprime, then $[L_1L_2 : K] = [L_1 : K][L_2 : K]$.

(iii) Find an example where neither of L_1, L_2 is contained in the other and $[L_1L_2 : K] < [L_1 : K][L_2 : K]$. Show that equality need not hold in (1).

Exercise 5. Let I be an ideal of a ring R, and let $q : R \to R/I$ be the quotient map.

(i) Show that if S is a subring of R, then S/I is a subring of R/I.

(ii) Show that if $\overline{S}$ is a subring of R/I, then $q^{-1}(\overline{S})$ is a subring of R.

(iii) Show that the maps in (i) and (ii) establish a bijective correspondence between the set of subrings of R containing I and the set of subrings of R/I.

Exercise 6. Let K be a number field, and let $R \subset K$ be a subring.

(i) Exploit minimal polynomials to show that if I is a non-zero ideal of R, then $I \cap \mathbb{Z}$ is a non-zero ideal of $\mathbb{Z}$.

(ii) Suppose that K is the field of fractions of R. Show that every $\alpha \in K$ can be written as $\alpha = r/n$, with $r \in R$ and $n \in \mathbb{N}$.

4.2 Assignment 2

Exercise 1. Let L_1 and L_2 be number fields, both subfields of a bigger field M. The solution of the previous set of exercises shows that the compositum L_1L_2 is a number field, and that all the elements of L_1L_2 can be written as x_1x_2, with $x_1 \in L_1$ and $x_2 \in L_2$. You may assume this in the current exercise.

(i) Let $\mathcal{O}_{L_1}\mathcal{O}_{L_2}$ be the subring of M generated by the rings of integers $\mathcal{O}_{L_1}$ and $\mathcal{O}_{L_2}$. Show that $\mathcal{O}_{L_1}\mathcal{O}_{L_2}$ is in fact a subring of L_1L_2.

(ii) Let $d = [L_1L_2 : \mathbb{Q}]$. Show that $\mathcal{O}_{L_1}\mathcal{O}_{L_2}$ contains a free abelian group of rank d by adapting a basis of L_1L_2 over $\mathbb{Q}$ to find d elements in $\mathcal{O}_{L_1}\mathcal{O}_{L_2}$ that are independent over $\mathbb{Q}$.

(iii) Show that $\mathcal{O}_{L_1}\mathcal{O}_{L_2}$ is a subset of $\mathcal{O}_{L_1L_2}$, and use this to conclude that $\mathcal{O}_{L_1}\mathcal{O}_{L_2}$ is an order in L_1L_2.

Exercise 2. Let K be a number field of degree 3. Show that K is isomorphic to a quotient $\mathbb{Q}[x]/(f)$, with $f = x^3 + ax + b$ in $\mathbb{Z}[x]$ irreducible in $\mathbb{Q}[x]$. You may not use the result quoted in the lectures that every number field is defined by some irreducible polynomial over $\mathbb{Q}$.

Exercise 3. Let $K = \mathbb{Q}[x]/(f)$ be a number field of degree 3, with $f = x^3 + ax + b$ in $\mathbb{Z}[x]$ irreducible in $\mathbb{Q}[x]$. Let r be the image of x in K.

(i) Show that the ring $\mathbb{Z}[r]$ is an order in K.

(ii) Show that the trace of an element $n_2r^2 + n_1r + n_0$, where $n_2, n_1, n_0 \in \mathbb{Q}$, equals $-2an_2 + 3n_0$.

(iii) Show that the norm of an element $n_2r^2 + n_1r + n_0$, where $n_2, n_1, n_0 \in \mathbb{Q}$, equals $a^2n_0n_2^2 - abn_1n_2^2 - 2an_0^2n_2 + an_0n_1^2 + b^2n_2^3 + 3bn_0n_1n_2 - bn_1^3 + n_0^3$.

(iv) Let $B = \{1, r, r^2\}$. Show that $\Delta_B(K) = -4a^3 - 27b^2$.

Exercise 4. Let K be a number field of degree d, and let $B = \{b_1, ..., b_d\}$ be a subset of K of cardinality d such that the matrix $(\mathrm{tr}(b_ib_j))_{i,j=1}^d$ has non-zero determinant $\Delta_B(K)$.

(i) Show that B is a basis for K as a vector space over $\mathbb{Q}$.

(ii) Show the result not proved in the lectures: if the elements of B are integral and $\Delta_B(K)$ is square-free, then $\mathcal{O}_K = \mathbb{Z}b_1 + \ldots + \mathbb{Z}b_d$.

Exercise 5. Let K be a number field, let $\mathcal{O}_K$ be its ring of integers, and let $B = \{b_1, ..., b_d\}$ be a subset of K of cardinality d such that $\mathcal{O}_K = \mathbb{Z}b_1 + \ldots + \mathbb{Z}b_d$. Define the trace-dual basis $B^\dagger = \{b'_1, \ldots, b'_d\}$ by the property $\mathrm{tr}(b_ib'_j) = \delta_{i,j}$ (Kronecker delta).

(i) Show that the $\mathbb{Z}$-span $\mathbb{Z}b'_1 + \ldots + \mathbb{Z}b'_d$ of $B^\dagger$ does not depend on the choice of B. This abelian group is called the trace dual (or inverse different) of $\mathcal{O}_K$, and we denote it by $\mathcal{O}_K^\dagger$.

(ii) Show that $\mathcal{O}_K^\dagger$ contains $\mathcal{O}_K$, and that the discriminant $\Delta(K)$ is nothing but the index $[\mathcal{O}_K^\dagger : \mathcal{O}_K]$.

Exercise 6. Let $K = \mathbb{Q}[x]/(f)$ be the number field defined by the irreducible cubic polynomial $f = x^3 - 2x - 2$. Let r be the image of x in K.

(i) Show that for the basis $B = \{1, r, r^2\}$ of K as a vector space over $\mathbb{Q}$ we have $\Delta_B(K) = -76$.

(ii) Show that $\mathbb{Z}[r]$ is of index at most 2 in $\mathcal{O}_K$, and that if $[\mathcal{O}_K : \mathbb{Z}[r]] = 2$, then an element of the form $n_2r^2 + n_1r + n_0$, with $n_2, n_1, n_0 \in \{0, 1/2\}$ not all zero, would be be integral.

(iii) Show that $\mathcal{O}_K = \mathbb{Z}[r]$.

Exercise 7. Counterexamples!

(i) Give an example of non-trivial number field K (so $K \neq \mathbb{Q}$) and a proper subring R of K such that K is the fraction field of R, but R is not an order in K.

(ii) Give an example of two number fields L_1 and L_2 contained in a bigger number field M such that $\mathcal{O}_{L_1L_2} \neq \mathcal{O}_{L_1}\mathcal{O}_{L_2}$.

Hint: There exist solutions where K, L_1, L_2 are quadratic.

4.3 Assignment 3

Exercise 1. We are going to show that a PID is a UFD.

(i) Prove that a PID is Noetherian.

(ii) Let R be a Noetherian domain. Use Noetherian induction to show that any non-zero element of R can be written as a product of irreducible elements.

(iii) Now let R be a PID. Recall from the lectures that all irreducible elements of a PID are prime. Use this and the previous result to show that a PID is a UFD.

Exercise 2. Let R be a Dedekind ring, and let I and J be ideals of R. Then we can define the product IJ and the sum $I + J$ of I and J. Let $\{\mathfrak{p}_i\}_{i=1}^N$ be the set of prime ideals of R occurring in the factorization of either of I and J, and write $I = \prod_{i=1}^N \mathfrak{p}_i^{m_i}$ and $J = \prod_{i=1}^N \mathfrak{p}_i^{n_i}$, with m_i, n_i (not necessarily strictly) positive integers.

(i) We know that $IJ = \prod_{i=1}^N \mathfrak{p}_i^{m_i+n_i}$. Show that $I + J = \prod_{i=1}^N \mathfrak{p}_i^{\min(m_i,n_i)}$.

(ii) Conclude that I and J are coprime if and only if the prime factorizations of I and J have no factor in common.

(iii) The moral of the story is that summing ideals corresponds to taking greatest common divisors, reflecting the multiplicative nature of ideals. Which operation corresponds to taking least common multiples? Prove your answer.

Exercise 3. Let $\mathfrak{p}$ be a prime ideal of the ring of integers $\mathcal{O}_K$ of a number field K.

(i) Show that $\mathfrak{p} \cap \mathbb{Z}$ is generated by a prime p, and that $\mathbb{Z}/p\mathbb{Z}$ is a subring of $\mathcal{O}_K/\mathfrak{p}$.

(ii) Show that $\mathrm{nm}(\mathfrak{p})$ is a power of p.

(iii) Suppose that $\mathcal{O}_K = \mathbb{Z}[\alpha]$, and let h be the minimal polynomial of α. Let $\overline{g}_1, ..., \overline{g}_n$ be the monic factors of the reduction $\overline{h}$ of h modulo p, of degrees $f_1, ..., f_n$ respectively, and suppose that we have $\overline{h} = \prod_{i=1}^n \overline{g}_i^{e_i}$ for positive integers e_i. Choose lifts g_i in $\mathbb{Z}[x]$ reducing to $\overline{g}_i$ modulo p, and set $\mathfrak{p}_i = (p, g_i(\alpha))$. Show that $\mathrm{nm}(\mathfrak{p}_i) = p^{f_i}$ and $\sum_{i=1}^n e_i f_i = d$. You are not required to prove this, but this formula also holds if $\mathcal{O}_K$ is not of the special form above!

Exercise 4. Show that every quadratic field embeds into a cyclotomic field. You may use that the Gauss sum $S = \sum_{i=1}^{p-1} \left(\dfrac{i}{p}\right) \zeta_p^i$ satisfies $S^2 = \left(\dfrac{-1}{p}\right) p$.

Exercise 5. Let $n \geq 3$ be an integer, not necessarily squarefree.

(i) Suppose that n is even. Determine all possible expressions of n as a product of units and irreducibles in $\mathbb{Z}[\sqrt{-n}]$ (up to the usual ambiguity), and prove that your answer is correct. Conclude that $\mathbb{Z}[\sqrt{-n}]$ is not a UFD.

(ii) Suppose that n is odd. Show that if $\mathbb{Z}[\sqrt{-n}]$ is a UFD, then all solutions of the equation $y^2 + n = x^2$ have the property that n divides y. Conclude that $\mathbb{Z}[\sqrt{-n}]$ is not a UFD.

Now look up the Stark-Heegner theorem and marvel at how close you came to proving it.

Exercise 6. Let K be the field $\mathbb{Q}(\sqrt{-15})$, let $R = \mathcal{O}_K$ be the ring of integers of K, and let $S = \mathbb{Z}[\sqrt{-15}]$.

(i) Use the Kummer–Dedekind theorem to factor the ideals (2), (3), (5), (7), (11), (13), (17), (19) in R and S.

(ii) Determine which of the prime ideals in these factorizations are invertible and which are principal.

Exercise 7. Let R be as in the previous exercise. Let $\alpha = \frac{-1+\sqrt{-15}}{2}$ and consider the prime ideals $\mathfrak{p} = (2, \alpha)$ and $\mathfrak{q} = (17, \alpha + 6)$ of R.

(i) Show that $\mathfrak{p}$ and $\mathfrak{q}$ are not principal, but that $\mathfrak{p}^2$, $\mathfrak{p}\mathfrak{q}$ and $\mathfrak{q}^2$ are.

(ii) Use the prime ideals $\mathfrak{p}$ and $\mathfrak{q}$ to construct an element of R that admits two distinct factorizations into irreducibles.

4.4 Assignment 4

Exercise 1. Let $R = \mathbb{Z}[3\sqrt{13}]$. Find

(i) all non-invertible prime ideals of R,

(ii) a non-zero ideal of R that is not a product of prime ideals, and

(iii) two ideals I and J of R such that $\operatorname{nm}(IJ) \neq \operatorname{nm}(I)\operatorname{nm}(J)$.

Prove that your answers are correct.

Exercise 2. Let $f = x^3 + 15x + 20$, and let $K = \mathbb{Q}[x]/(f)$. Determine the ring of integers $\mathcal{O}_K$ of K.

Exercise 3. Let $f = x^3 + x + 14$, let $K = \mathbb{Q}[x]/(f)$, and let r be the image of x in K. Factorize the ideal $(5r^2 + r + 151, -8r^2 + 5r - 7)$ into prime ideals in the ring of integers $\mathcal{O}_K$.

Exercise 4. Let $K = \mathbb{Q}(\sqrt{29})$ and $L = \mathbb{Q}(\sqrt{-29})$. Determine the unit groups of $\mathcal{O}_K$ and $\mathcal{O}_L$. Show that the class group of $\mathcal{O}_K$ is trivial, and that the class group of $\mathcal{O}_L$ is cyclic of order 6, generated by $(3, 8 + \sqrt{-29})$.

Exercise 5. Solve the equation $y^2 = x^3 - 33$ in integers.

Exercise 6. And if you can solve this, then I have nothing more to teach you. Let $f = x^3 - 3x - 10$, and let $K = \mathbb{Q}[x]/(f)$. Determine the class number of the ring of integers $\mathcal{O}_K$.

Chapter 5

Solutions

5.1 Solutions to Assignment 1

Exercise 1.

(i) Modulo 3, the form $x^2 + xy + y^2$ only takes the values 0 and 1, as can be verified by trying all nine possible values of the tuple (x, y).

(ii) Every non-zero element of $\mathbb{Z}/p\mathbb{Z}$ is invertible (use Euclid's algorithm, for example). So the unit group $(\mathbb{Z}/p\mathbb{Z})^*$ has order $p - 1$. This order is divisible by 3. Therefore there is a non-trivial α modulo p such that α^3 equals the unit element 1.

(iii) This follows from the factorization $x^3 - 1 = (x - 1)(x^2 + x + 1)$; the α above is not a zero of the first factor, so it is a zero of the second.

(iv) Since $\frac{-1+\sqrt{-3}}{2} = -1 + \frac{1+\sqrt{-3}}{2}$, we have $\mathbb{Z}[\frac{-1+\sqrt{-3}}{2}] = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$. But $\frac{1+\sqrt{-3}}{2}$ has minimal polynomial $x^2 + x + 1$, so $\mathbb{Z}[\frac{-1+\sqrt{-3}}{2}] = \mathbb{Z}[x]/(x^2 + x + 1)$. Now the ideals in question correspond to ideals of the quotient ring $\mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]/p\mathbb{Z}[\frac{-1+\sqrt{-3}}{2}] \cong \mathbb{Z}[x]/(x^2 + x + 1, p) \cong (\mathbb{Z}/p\mathbb{Z})[x]/(x^2 + x + 1)$. But the latter polynomial has a root modulo p, hence two roots, so as in the lecture, we can apply the Chinese remainder theorem to see that this ring is isomorphic to $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. And we also saw that this ring has two non-trivial ideals.

(v) Let π_1, π_2 be generators of the ideals above. Then $\operatorname{nm}(\pi_1) = p$. Indeed, this norm is integral. It is also positive, since the norm on $\mathbb{Q}(\sqrt{-3})$ is. Furthermore, because p is contained in the ideal generated by π_1, there exists some π_1' such that $\operatorname{nm}(\pi_1 \pi_1') = \operatorname{nm}(\pi_1) \operatorname{nm}(\pi_1')$. First of all, if $\operatorname{nm}(\pi_1) = 1$, then π_1 is a unit, hence it would generate the full ring, which we know that it does not. Secondly, if $\operatorname{nm}(\pi_1) = p^2$, then π_1' would be a unit, hence π_1 would generated the same ideal as p, also not true by construction. So indeed $\operatorname{nm}(\pi_1) = p$. Now write $\pi_1 = x + \frac{1+\sqrt{-3}}{2} y$. Then $p = \operatorname{nm}(\pi_1) = x^2 + xy + y^2$.

Exercise 2.

(i) This set certainly contains $\alpha = \frac{1+\sqrt{-19}}{2}$ and the unit element, so we need only verify that it is closed under addition and multiplication. We can use the fact that α has monic polynomial $x^2 - x + 5$ and proceed as in the lectures. Alternatively, there is a direct verification by the formula

$$\begin{aligned}(a_1+b_1\alpha)(a_2+b_2\alpha) &= a_1a_2+(a_1b_2+a_2b_1)\alpha+b_1b_2\alpha^2\\ &= (a_1a_2-5b_1b_2)+(a_1b_2+a_2b_1)\alpha.\end{aligned} \tag{5.1.1}$$

(ii) We have to find the units, or alternatively the elements of $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ whose norm is in $\{\pm1\}$. Consider an element of the form $\frac{x+y\sqrt{-19}}{2}$, with $x, y \in \mathbb{Z}$. The norm of such an element equals $\frac{x^2+19y^2}{4}$. If $y \neq 0$, then this cannot be in $\{\pm1\}$. The solutions are then easily found, namely $(\pm2, 0)$, leading to the elements ±1 of $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$.

(iii) This is the same as finding the solutions to $(y+\sqrt{-19})(y-\sqrt{-19}) = x^3$, a problem in $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$. Now we mimic the lecture.

Step 1. y is not divisible by 19. Indeed, look modulo 19 to see that then $x \equiv 0 \mod 19$. Now look modulo 19^2: get $y^2 \equiv x^3 - 19 \equiv -19 \mod 19^2$, which is not a square.

Step 1'. y is divisible by 2. After all, in the other case $y^2 + 3 \equiv 4 \mod 8$, which is not a third power.

Step 2. $(y+\sqrt{-19})$ and $(y-\sqrt{-19})$ are coprime in the ring $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$. To see this, note that a common divisor would have to divide the difference $2\sqrt{-19}$. Both 2 and $\sqrt{-19}$ are prime elements of $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$, the latter because its norm is prime and the former because no elements of norm 2 exist. So either 2 or $\sqrt{-19}$ would divide both $(y+\sqrt{-19})$ and $(y-\sqrt{-19})$. In the former case, y would have to be odd, otherwise the quotient would not be in $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$; in the latter, it would have to be a divisible by 19, because $\sqrt{-19}(a+b\frac{1+\sqrt{-19}}{2}) = \frac{-19}{4}b+(a+b)\sqrt{-19}$. But we just excluded these cases.

Step 3. Both $(y+\sqrt{-19})$ and $(y-\sqrt{-19})$ are cubes in the ring $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$. This follows from exactly the same UFD argument as that given in the lecture.

Step 4. Now we can find all solutions. We have $y+\sqrt{-19} = (\frac{a+b\sqrt{-19}}{2})^3$, where a and b are integers with the same parity. We get

$$\begin{aligned}y+\sqrt{-19} &= \left(\frac{a+b\sqrt{-19}}{2}\right)^3\\ &= \frac{a^3-57ab^2}{8}+\frac{3a^2b-19b^3}{8}\sqrt{-19}.\end{aligned} \tag{5.1.2}$$

We get $b(3a^2-19b^2) = 3a^2b-19b^3 = 8$, so b divides 8. Running over all possible cases, we get our solutions.

Exercise 3.

(i) We have

$$a^2 = (-1)^{\frac{p-1}{2}} \prod_{g\in(\mathbb{Z}/p\mathbb{Z})^*} g. \tag{5.1.3}$$

In the second product, we can cancel all g such that $g^{-1} \neq g$ with their inverses, leaving us only with $g = -1$, which is therefore the value of the product. Now note that the first power equals 1 if and only if $p \equiv 1 \mod 4$.

(ii) Apply division with remainder to see that $f = g(x-r)+c$ for some constant c and conclude that $c = 0$.

(iii) If there were more than d roots, the polynomial would have more than d non-trivial factors, hence degree strictly larger than d because of unique factorization.

(iv) Call the group in question G. By the classification theorem for abelian groups, if G were not cyclic, then there would exist some prime p such that G contains the subgroup $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. So G would have at least p^2 elements of multiplicative order p. In which case the polynomial $x^p - 1$ would have at least p^2 roots.

(v) This is now immediate: if g is a generator of the cyclic group $(\mathbb{Z}/p\mathbb{Z})^*$ of order $p-1$, then $g^{\frac{p-1}{4}}$ has order 4.

Exercise 4.

(i) We may assume that the extension $L_2|K$ is infinite (otherwise there is nothing to prove). In that case, L_2 is spanned as a vector space by finitely many elements. Hence it is also generated by finitely many elements as a field extension of K. So write $L_2 = K(\beta_1, ..., \beta_n)$. Then by the tower law (Proposition 1.1.8)

$$\begin{aligned}[L_2 : K] &= [K(\beta_1, \dots \beta_n) : K(\beta_1, \dots \beta_{n-1})] \cdots [K(\beta_1) : K] \\ &= [K(\beta_1, \dots \beta_{n-1})(\beta_n) : K(\beta_1, \dots \beta_{n-1})] \cdots [K(\beta_1) : K]\end{aligned} \tag{5.1.4}$$

On the other hand, since L_2 is generated by $\beta_1, \dots, \beta_n$ as an extension of K, the compositum L_1L_2 is generated by $\beta_1, \dots, \beta_n$ as an extension of L_1. So

$$\begin{aligned}[L_1L_2 : L_1] &= [L_1(\beta_1, \dots \beta_n) : L_1(\beta_1, \dots \beta_{n-1})] \cdots [L_1(\beta_1) : L_1] \\ &= [L_1(\beta_1, \dots \beta_{n-1})(\beta_n) : L_1(\beta_1, \dots \beta_{n-1})] \cdots [L_1(\beta_1) : L_1]\end{aligned} \tag{5.1.5}$$

So by induction, we may assume that $L_2 = K(\beta)$ for some $\beta \in M$. In that case, the degree of the extension $[K(\beta) : K]$ is nothing but the degree of the minimal polynomial f of β over K. That polynomial will also vanish in β when considered as an element of the polynomial ring $L_1[x]$. Hence the minimal polynomial of β over L_1 divides f_K, which upon taking degrees yields the inequality that we had to prove.

(ii) We have $[L_1L_2 : K] = [L_1L_2 : L_1][L_1 : K] = [L_1L_2 : L_2][L_2 : K]$. Hence both $[L_1 : K]$ and $[L_2 : K]$ divide $[L_1L_2 : K]$, which is therefore greater than or equal to $[L_1 : K][L_2 : K]$. On the other hand $[L_1L_2 : K] = [L_1L_2 : L_1][L_1 : K] \leq [L_1L_2 : L_1][L_1 : K]$.

(iii) Take $K = \mathbb{Q}$ and $M = \overline{\mathbb{Q}}$, and let $L_1 = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, $L_2 = \mathbb{Q}(\sqrt{2}, \sqrt{5})$. Then $L_1L_2 = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$. We have

$$[L_1L_2 : K] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) : \mathbb{Q}(\sqrt{2}, \sqrt{3})][\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]. \tag{5.1.6}$$

Let us show that all these extensions have degree 2. We assume that $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ and treat the case $[\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) : \mathbb{Q}(\sqrt{2}, \sqrt{3})] = 2$; the others are easier. Since $\sqrt{5}$ is the root of a degree 2 polynomial over $\mathbb{Q}$, it suffices to show that it is not the root of a degree 1 polynomial over $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. That is, we have to show that 5 is not a square in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Using the usual reduction process, we see that an element of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is of the form $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$.

One calculates (using the basis $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$) that the trace of such a number equals $4a$. On the other hand, the trace of $\sqrt{5}$ equals 0, so were are reduced to considering elements of the form $b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$. These square to

$$2b^2 + 3c^2 + 6d^2 + 6cd\sqrt{2} + 4bd\sqrt{3} + 2bc\sqrt{5}. \tag{5.1.7}$$

Since this has to equal 5, and we supposed that $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ was a basis of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$, we see that two of the elements b, c, d equal 0. Say $b = c = 0$. Then we get the impossible demand $6d^2 = 5$.

Similar reasoning shows $[L_1 : K] = [L_2 : K] = 4$. We have our counterexample, which by the tower law immediately yields a counterexample to (1).

Exercise 5.

(i) Certainly the unit element is in the image $S/I = \{r + I : r \in s\} \subset R/I$. Since $q(s_1) + q(s_2) = q(s_1 + s_2)$ and $q(s_1)q(s_2) = q(s_1 s_2)$, the image is closed under taking sum and products as well. It is therefore a subring.

(ii) Again the given inverse image contains the unit element of R. If $q(r_1) = s_1 \in \overline{S}$ and $q(r_2) = s_2 \in \overline{S}$, then $q(r_1 + r_2) = s_1 + s_2 \in \overline{S}$ and $q(r_1 r_2) = s_1 s_2 \in \overline{S}$.

(iii) We check that the maps are inverse to one another. Since q is surjective, we have $q(q^{-1}(\overline{S})) = \overline{S}$ for any subring $\overline{S}$ of S/I. On the other hand, if S is a subring of R containing I, then $q^{-1}(q(S)) = S$. Indeed, it suffices to prove $q^{-1}(q(S)) \subset S$, and if $r \in R$ is such that $q(r) \in q(S)$, then $r + I = s + I$ for some $s \in S$. So r is in $s + I$, which is a subset of S by hypothesis.

As a concluding remark, note that the demand on containing I is certainly necessary! In the case of Exercise 1(v), both $\mathbb{Z}$ and $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ map surjective to $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]/(\pi_1) = \mathbb{Z}/p\mathbb{Z}$. Only one of these, namely $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$, contains the principal ideal (π_1).

Exercise 6.

(i) Let $r \in R$ be non-zero, and let f be its minimal polynomial over $\mathbb{Q}$ (which we defined to be monic). Let N be such that $Nf \in \mathbb{Z}[x]$. Let $Nf = \sum_{i=0}^{d} a_i x^i$ with $a_i \in \mathbb{Z}$. Then $a_0 \neq 0$ because f is a minimal polynomial and r is not zero. We see that $a_0 = -\sum_{i=1}^{d} a_i r^i$. The element on the right hand side is in I because the a_i are in $\mathbb{Z} \subset R$.

(ii) Given α, we define the denominator ideal $\mathfrak{d} = \{\beta \in R : \beta\alpha \in R\}$. This is an ideal of the ring R, and it is not empty because K is the fraction field of R (so that if we write $\alpha = r_1/r_2$ with the r_i in R, then $r_2 \in \mathfrak{d}$). Let n be an element of the intersection $\mathfrak{d} \cap \mathbb{Z}$. Then by construction of $\mathfrak{d}$ there exists an $r \in R$ such that $\alpha = r/n$.

5.2 Solutions to Assignment 2

Exercise 1.

(i) $\mathcal{O}_{L_1}$ is a subring of L_1, and $\mathcal{O}_{L_2}$ is a subring of L_2. Now $L_1 L_2$ is the smallest *field* containing both L_1 and L_2, so it is certainly a *ring* containing the two, and therefore both $\mathcal{O}_{L_1}$ and $\mathcal{O}_{L_2}$ as well. Hence it contains the smallest subring $\mathcal{O}_{L_1}\mathcal{O}_{L_2}$ of M containing $\mathcal{O}_{L_1}$ and $\mathcal{O}_{L_2}$.

(ii) Let $b_1, \dots, b_d$ be a $\mathbb{Q}$-basis of $L_1 L_2$. Write $b_i = \beta_i \gamma_i$ with $\beta_i \in L_1$ and $\gamma_i \in L_2$. We have seen in a previous exercise that there exist non-zero integers m_i and n_i such that $m_i \beta_i \in \mathcal{O}_{L_1}$ and $n_i \gamma_i \in \mathcal{O}_{L_2}$. Then $\{m_1 n_1 b_1, \dots, m_d n_d b_d\}$ is again a $\mathbb{Q}$-basis for $L_1 L_2$ because the elements $m_i n_i$ are in $\mathbb{Q}$. But this basis is contained in $\mathcal{O}_{L_1}\mathcal{O}_{L_2}$ by construction.

(iii) The elements in $\mathcal{O}_{L_1}$ are all integral, and so are the elements in $\mathcal{O}_{L_2}$. Use the fact that integral elements form a subring to conclude that the ring $\mathcal{O}_{L_1}\mathcal{O}_{L_2}$ is indeed contained in the ring of integers $\mathcal{O}_{L_1 L_2}$ of $L_1 L_2$. By the classification theorem of finitely generated abelian groups, it is an order; indeed, it is both contained in $\mathcal{O}_{L_1 L_2}$, which is a free abelian group of rank d, and contains the $\mathbb{Z}$-span of the $m_i n_i b_i$, which is a free abelian group of rank d because the $m_i n_i b_i$ are independent over $\mathbb{Q}$.

Exercise 2. Let β be an arbitrary element of L that is not in $\mathbb{Q}$. Such an β exists because $[L : \mathbb{Q}] = 3$. Consider the subfield $\mathbb{Q}(\beta)$ of L. Then by the tower law we have $[L : \mathbb{Q}(\beta)][\mathbb{Q}(\beta) : \mathbb{Q}] = [L : \mathbb{Q}] = 3$. Since β is not in $\mathbb{Q}$, the inclusion $\mathbb{Q} \subseteq \mathbb{Q}(\beta)$ is proper. Therefore $[\mathbb{Q}(\beta) : \mathbb{Q}] > 1$. This forces $[L : \mathbb{Q}(\beta)] = 1$, which just means that $L = \mathbb{Q}(\beta)$.

We have seen in the lectures that if we let f_β be the minimal polynomial of β, then $\mathbb{Q}(\beta) = \mathbb{Q}[x]/(f_\beta)$. So L is defined by the polynomial f_β. Suppose that $f_\beta = x^3 + a_1x^2 + b_1x + c_1$ with $a_1, b_1, c_1 \in \mathbb{Q}$. Then note that $\gamma = \beta - (a_1/3)$ still generates $\mathbb{Q}(\beta)$, because any expression in β can be transformed by linear substitution into one in γ, and vice versa. Moreover, γ satisfies $f_\beta(\gamma - (a_1/3)) = f_\beta(\beta) = 0$. Therefore $f_\beta(x - (a_1/3))$ is the miminimal polynomial f_γ of γ, because it is monic and of the correct degree. But $f_\beta(x - (a_1/3))$ has second coefficient equal to zero. To sum up: γ has minimal polynomial $f_\gamma = f_\beta(x - (a_1/3)) = x^3 + a_2x + b_2$ for some $a_2, b_2 \in \mathbb{Q}$.

We have seen in the lectures that there exists a non-zero integer N such that $\delta = N\gamma$ is integral. Of course δ still generates L because it is a $\mathbb{Q}$-multiple of γ. Explicitly, δ is a zero of the polynomial $f_\gamma(x/N)$, and hence also of the monic polynomial $N^3 f_\gamma(x/N) = x^3 + N^2a_2x + N^3b_2$, which by an argument as above equals the minimal polynomial f_δ of δ. The fact that $N\gamma$ is integral merely means that $a_3 = N^2a_2$ and $b_3 = N^3b_2$ are both integral. It is also directly clear that this is the case for big N. We get our final solution: we can take $f = f_\delta = x^3 + a_3x + b_3$.

Exercise 3.

(i) Because r is integral and the zero of a monic polynomial of degree 3, we have $\mathbb{Z}[r] = \mathbb{Z} + \mathbb{Z}r + \mathbb{Z}r^2$, which is a free abelian group of rank 3 because the minimal polynomial of r is of degree 3, which precludes dependencies.

(ii) On the basis B, multiplication by r is described by left multiplication by the matrix

$$M_r = \begin{pmatrix} 0 & 0 & -b \\ 1 & 0 & -a \\ 0 & 1 & 0 \end{pmatrix}. \tag{5.2.1}$$

Hence by additivity and distributivity, multiplication by $n_2r^2 + n_1r + n_0$ is described by the matrix $n_2M_r^2 + n_1M_r + n_0$, which equals

$$\begin{aligned} & n_2 \begin{pmatrix} 0 & -b & 0 \\ 0 & -a & -b \\ 1 & 0 & -a \end{pmatrix} + n_1 \begin{pmatrix} 0 & 0 & -b \\ 1 & 0 & -a \\ 0 & 1 & 0 \end{pmatrix} + n_0 \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ & = \begin{pmatrix} n_0 & -bn_2 & -bn_1 \\ n_1 & -an_2 & -an_1 - bn_2 \\ n_2 & n_1 & n_0 \end{pmatrix}. \end{aligned} \tag{5.2.2}$$

The trace of $n_2r^2 + n_1r + n_0$ is the trace of this matrix, which is indeed $-2an_2 + 3n_0$.

(iii) Take the determinant of the same matrix.

(iv) The given value is the determinant of the matrix

$$\begin{pmatrix} \mathrm{tr}(r^0r^0) & \mathrm{tr}(r^0r^1) & \mathrm{tr}(r^0r^2) \\ \mathrm{tr}(r^1r^0) & \mathrm{tr}(r^1r^1) & \mathrm{tr}(r^1r^2) \\ \mathrm{tr}(r^2r^0) & \mathrm{tr}(r^2r^1) & \mathrm{tr}(r^2r^2) \end{pmatrix}. \tag{5.2.3}$$

We can find the given traces by taking traces of the powers M_r^i for $0 \leq i \leq 4$. We thus end up with the determinant of the matrix

$$\begin{pmatrix} 3 & 0 & -2a \\ 0 & -2a & -3b \\ -2a & -3b & 2a^2 \end{pmatrix}, \tag{5.2.4}$$

which is indeed $-4a^3 - 27b^2$.

Exercise 4.

(i) Say that b_d could be expressed as a combination of $b_1, \ldots b_{d-1}$. Then by the linearity of the trace, the final row of the trace matrix would be a combination of the previous ones, and the determinant would be 0.

(ii) Consider the $\mathbb{Z}$-span $L = \mathbb{Z}b_1 + \ldots + \mathbb{Z}b_d$. Then L is an abelian subgroup of $\mathcal{O}_K$. Let B' be a $\mathbb{Z}$-basis of $\mathcal{O}_K$. Then we have $B = SB'$ for some integral matrix S. Then $\Delta_B(K) = [\mathcal{O}_K : L]^2 \Delta_{B'}(K) = [\mathcal{O}_K : L]^2 \Delta(K)$ by the lecture. Because $\Delta_B(K)$ is square-free, this shows that the index $[\mathcal{O}_K : L]$ equals 1. So in fact $L = \mathcal{O}_K$, and L is a ring.

Exercise 5.

(i) Because the trace pairing is non-degenerate, B' is well-defined and spans K over $\mathbb{Q}$. So every element of K allows an expression $c_1 b'_1 + \ldots + c_d b'_1$, with $c_i \in \mathbb{Q}$. By the defining property of the b'_i, the $\mathbb{Z}$-span of $\{b'_1, \ldots, b'_d\}$, which consists of those combinations with $c_i \in \mathbb{Z}$, can equally well be described as

$$\{\alpha \in K : \mathrm{tr}(\alpha b_i) \in \mathbb{Z} \text{ for all } 0 \leq i \leq d\}. \tag{5.2.5}$$

or again more intrinsically

$$\{\alpha \in K : \mathrm{tr}(\alpha r) \in \mathbb{Z} \text{ for all } r \in \mathcal{O}_K\}. \tag{5.2.6}$$

(ii) The first statement follows because $\mathcal{O}_K$ is a subring on which tr takes integral values. Let S be an integral matrix such that $B = SB'$. Then by expressing the b_i in terms of the b'_i using S, we can express the trace matrix $T = (\mathrm{tr}(b_i b_j))_{i,j=1}^d$ in terms of $T' = (\mathrm{tr}(b_i b'_j))_{i,j=1}^d$; we simply have $T = ST'$. We know that $\det(S) = [\mathcal{O}_K^\dagger : \mathcal{O}_K]$, so now it just suffices to observe that T' equals the identity matrix by construction.

Exercise 6.

(i) Skip back a few exercises.

(ii) The first statement follows because $[\mathcal{O}_K : \mathbb{Z}[r]]^2$ has to divide $\Delta_B(K)$. Therefore if $x \in \mathcal{O}_K$, then $2x \in \mathbb{Z}[r]$. In other words, $\mathcal{O}_K$ is contained in $(1/2)\mathbb{Z}[r]$. If $\mathcal{O}_K \neq \mathbb{Z}[r]$, then by subtracting suitable elements of $\mathbb{Z}[r]$, we obtain one of the given representatives of $(1/2)\mathbb{Z}[r]/\mathbb{Z}[r]$.

(iii) Calculating dependencies as in the notes, we find the following minimal polynomials:

$$\begin{array}{cc} \frac{1}{2} & x - \frac{1}{2} \\ \frac{r}{2} & x^3 - \frac{1}{2}x - \frac{1}{4} \\ \frac{r^2}{2} & x^3 - 2x^2 + x - \frac{1}{2} \\ \frac{1+r}{2} & x^3 - \frac{3}{2}x^2 + \frac{1}{4}x - \frac{1}{8} \\ \frac{1+r^2}{2} & x^3 - \frac{7}{2}x^2 + \frac{15}{4}x - \frac{13}{8} \\ \frac{r+r^2}{2} & x^3 - 2x^2 - x - \frac{1}{4} \\ \frac{1+r+r^2}{2} & x^3 - \frac{7}{2}x^2 + \frac{7}{4}x - \frac{3}{8} \end{array} \tag{5.2.7}$$

None of these polynomials have integral coefficients, so by the above, we see that $\mathcal{O}_K = \mathbb{Z}[r]$. Alternatively, use the norm form in the previous exercise to calculate the norms of these elements without calculating their minimal polynomials themselves, and deduce a contradiction by using the fact that the norm of an algebraic integer is in $\mathbb{Z}$ by Proposition 1.3.12.

Exercise 7.

(i) Let R be the set whose members are those elements of $\mathbb{Q}(\sqrt{5})$ of the form $a + b\sqrt{5}$, with a, b rational numbers whose denominator is not divisible by 2. This is certainly a subring, because we have $(a_1+b_1\sqrt{5})(a_2+b_2\sqrt{5}) = (a_1a_2+5b_1b_2)+(a_1b_2+a_2b_1)\sqrt{5}$. It is not an order because it contains the set of rational numbers whose denominator is not divisible by 2. And we can use the proof in the lectures to show that this is not a finitely generated abelian group; if it had a finite set of generators, then the powers of, say, 3 that could occur in the denominators would be bounded, and we know that they are not. We conclude that R is not finitely generated either, so it is not an order in K.

(ii) Take $L_1 = \mathbb{Q}(\sqrt{3})$ and let $L_2 = \mathbb{Q}(\sqrt{7})$. Then we know from the lectures that $\mathcal{O}_{L_1} = \mathbb{Z}+\mathbb{Z}\sqrt{3}$ and $\mathcal{O}_{L_2} = \mathbb{Z}+\mathbb{Z}\sqrt{7}$. Therefore $\mathcal{O}_{L_1}\mathcal{O}_{L_2} = \mathbb{Z}+\mathbb{Z}\sqrt{3}+\mathbb{Z}\sqrt{7}+\mathbb{Z}\sqrt{21}$. Let $B = \{1, \sqrt{3}, \sqrt{7}, \sqrt{21}\}$. Then B is a $\mathbb{Q}$-basis of L_1L_2, since if not, then we would have $[L_1L_2 : \mathbb{Q}] = 2$ by an argument as in the first solution in this batch, whence $L_1 = L_2$, and we know from the lecture that this is not true. Therefore $\mathcal{O}_{L_1}\mathcal{O}_{L_2}$ is a free abelian group on the generators in B. But $\mathcal{O}_{L_1L_2}$ also contains the integral element $(1 + \sqrt{21})/2$, which has representation $\{(1/2), 0, 0, (1/2)\}$ in this basis and is therefore not in $\mathcal{O}_{L_1}\mathcal{O}_{L_2}$.

5.3 Solutions to Assignment 3

Exercise 1.

(i) Every ideal is finitely generated. Heck, every ideal is generated by a single element! So the statement follows from Proposition 1.7.2.

(ii) Consider the set S of prime ideals of R generated by elements for which the desired property does not hold. Then by Noetherianness, S has a maximal element I. Let r be a generator of I. Then r is not irreducible. So write $r = st$, with s and t non-units. Then the ideals (s) and (t) both properly contain I. Indeed, if we had $(r) = (s)$, then we have $r = us$ for some unit u. But because R is a domain, we then have $r = u$, contradiction. Therefore there exist expressions for s and r as products of irreducible elements. Multiplying, we get such an expression for s. Contradiction.

(iii) It only remains to show uniqueness of the factorization. So let r be a non-zero element of R, and consider two factorizations $r = up_1 \cdots p_m$ and $r = vq_1 \cdots q_n$ of x as a product of a unit and some irreducibles. We have seen that the ideal (p_1) is prime. So one of the q_i is in (p_1). We may assume that q_1 is. If we can show that q_1 equals p_1 up to a unit, then we are done, because we can then divide the two expressions for r by p_1 and continue by induction. So we have to show that $(p_1) = (q_1)$, and we already know that $(q_1) \subseteq (p_1)$. Write $q_1 = sp_1$. Then because q_1 is irreducible, s is a unit. We are done.

Exercise 2.

(i) As shows in Corollary 1.7.19, we have an inclusion of ideals $K_1 \subseteq K_2$ if and only if there exist prime ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_m$ such that $K_1 = \mathfrak{q}_1 \cdots \mathfrak{q}_m K_2$. Therefore an ideal of the form $\prod_{i=1}^N \mathfrak{p}_i^{\ell_i}$ contains I if and only if $\ell_i \leq m_i$, and it contains J if and only if $\ell_i \leq n_i$. It therefore contains both I and J if and only if $\ell_i \leq \min(m_i, n_i)$. But the ideal $I + J$ is the smallest ideal containing both I and J, and therefore is indeed the product $\prod_{i=1}^N \mathfrak{p}_i^{\min(m_i,n_i)}$.

(ii) By unique factorization, the product on the right equals the unit ideal if and only if $\min(x_i, y_i) = 0$ for all i, which is equivalent with the absence of common factors in the factorization.

(iii) In $\mathbb{Z}$, the least common multiple of two integers $\prod_{i=1}^N p_i^{m_i}$ and $\prod_{i=1}^N p_i^{n_i}$ is $\prod_{i=1}^N p_i^{\max(m_i,n_i)}$. Generalizing this operation by using prime ideals, this is just taking the intersection $I \cap J$ of I and J. To prove this, recall from Corollary 1.7.19 that $K_1 \subseteq K_2$ for ideals K_1 and K_2 if and only if there exist prime ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_m$ such that $K_1 = \mathfrak{q}_1 \cdots \mathfrak{q}_m K_2$. Therefore an ideal of the form $\prod_{i=1}^N \mathfrak{p}_i^{\ell_i}$ is contained in I if and only if $\ell_i \geq m_i$, and it is contained in J if and only if $\ell_i \geq n_i$. It is therefore is contained in both I and J if and only if $\ell_i \geq \max(m_i, n_i)$. But the ideal $I \cap J$ is the largest ideal contained in both I and J, and therefore is indeed the product $\prod_{i=1}^N \mathfrak{p}_i^{\max(m_i,n_i)}$.

Exercise 3.

(i) Consider the canonical map $\mathbb{Z} \to \mathcal{O}_K/\mathfrak{p}$ obtained by composing the inclusion $\mathbb{Z} \to \mathcal{O}_K$ and the projection $\mathcal{O}_K \to \mathcal{O}_K/\mathfrak{p}$. This map has kernel $\mathfrak{p} \cap \mathbb{Z}$. This kernel is non-zero, because we have seen that every ideal of a number ring contains some non-zero element. On the other hand, the kernel will be a prime ideal, since $\mathcal{O}_K/\mathfrak{p}$ is an integral domain. The kernel is therefore generated by some prime p, and we then have $\mathfrak{p} \cap \mathbb{Z} = (p)$. By construction, the induced map $\mathbb{Z}/p\mathbb{Z} \to \mathcal{O}_K/\mathfrak{p}$ is an injection.

(ii) The ring $\mathcal{O}_K/\mathfrak{p}$ is a finite integral domain, hence a field. (See also the proof of Proposition 1.7.5.) It contains $\mathbb{Z}/p\mathbb{Z}$ as a subfield, and its cardinality is therefore a power of p.

(iii) We can now give a more explicit expression of the previous result. The quotient $\mathcal{O}_K/\mathfrak{p}$ is in this case nothing but the quotient $(\mathbb{Z}/p\mathbb{Z})[x]/(g_i)$. Every element of this ring has a unique expression of the form $a_0 + a_1 x + \ldots + a_{d-1}x^{d-1}$ for $a_i \in \mathbb{Z}/p\mathbb{Z}$, so we get p^{f_i} elements and therefore indeed $\mathrm{nm}(\mathfrak{p}) = \#(\mathcal{O}_K/\mathfrak{p}_i) = p^{f_i}$. The equality $d = \sum e_i f_i$ follows by comparing degrees in the factorization of h modulo p.

Exercise 4. The key realization is the simple observation that the cyclotomic extension of $\mathbb{Q}$ defined by the n-th roots of unity is contained in the cyclotomic extension defined by the mn-th roots of unity.

Theorem 1.6.7 on Gauss sums shows that given a prime p, we can embed either $\mathbb{Q}(\sqrt{p})$ or $\mathbb{Q}(\sqrt{-p})$ into the cyclotomic extension defined by, say, the n-roots of unity. But since $\sqrt{-1}$ is a fourth root of unity, this shows equally well that both of these fields can be embedded into the cyclotomic extension defined by the $4n$-th roots of unity, which contains both the n-th roots of unity and $\sqrt{-1}$.

Now let $n = \pm \prod_{i=1}^{f} p_i$ be an arbitrary integer. Then since $\sqrt{n} = \sqrt{\pm 1}\sqrt{p_1} \cdots \sqrt{p_f}$, it suffices to construct a cyclotomic extension containing $\sqrt{-1}, \sqrt{p_1}, \ldots \sqrt{p_f}$. By the previous paragraph, we can choose n_i be such that the n_i-th cyclotomic extension contains $\sqrt{p_i}$. Construct the product $n = 4\prod_{i=1}^{f} n_i$. Then by our first observation, the n-th cyclotomic extension achieves our purpose.

Exercise 5.

(i) Consider the norm form $\mathrm{nm}(x + y\sqrt{n}) = x^2 + ny^2$ on $\mathbb{Z}[\sqrt{-n}]$. This is a positive integral function, and if y is non-zero, then its value is at least n. If a factorization contains a factor with non-zero y, then it contains at least two such factors. Combining these statements, we see that the only factorizations of n in which a factor which non-zero y occurs is (up to multiplication with units) $n = -\sqrt{-n}\sqrt{-n}$.

There can be only one other factorization, namely the factorization of n into primes in $\mathbb{Z}$. These primes remain irreducible in $\mathbb{Z}[\sqrt{-n}]$ because their norm is strictly smaller than n^2, which by the argument above precludes the occurrence of factors with non-zero y.

Considering the norm form again, we see that he only units in $\mathbb{Z}[\sqrt{-n}]$ are ± 1. So the factorizations obtained above are not equivalent. Hence $\mathbb{Z}[\sqrt{-n}]$ is not a UFD because, well, no U.

(ii) We write the equation as $(y + \sqrt{-n})(y - \sqrt{-n}) = x^2$. Suppose that $\mathbb{Z}[\sqrt{-n}]$ is a UFD. Then any common factor on the left-hand side divides $2\sqrt{-n}$. So because both 2 and $\sqrt{-n}$ are irreducible (consider the norm form!), if there were a common factor, then either 2 would $\sqrt{-n}$ would be a common factor as well. But 2 can certainly not be a common factor because $y + \sqrt{-n}$ is not a multiple of 2 in $\mathbb{Z}[\sqrt{-n}]$. If $\sqrt{-n}$ were a common factor, then $y + \sqrt{-n} = (a + b\sqrt{-n})\sqrt{-n}$ for some a and b, which would imply that y is divisible by n, a case that does not interest us.

So we have $(y + \sqrt{-n})(y - \sqrt{-n}) = x^2$ with $(y + \sqrt{-n})$ and $(y - \sqrt{-n})$ coprime. The right-hand side, is a square, hence so are the coprime factors on the left. So $y + \sqrt{-n} = (a + b\sqrt{-n})^2 = \ldots + 2ab\sqrt{-n}$ for some integral a and b, which is impossible. Hence if $\mathbb{Z}[\sqrt{-n}]$ is a UFD, all solutions of $y^2 + n = x^2$ in integers have the property that y is divisible by n.

Both there do exist solutions of $y^2 + n = x^2$ in integers for which y is not divisible by n, for example $x = (n+1)/2$ and $y = (n-1)/2$. Therefore $\mathbb{Z}[\sqrt{-n}]$ is not a UFD.

Exercise 6.

(i) By far the easiest way to solve everything at one stroke is to tabulate the values of

$f = x^2 - x + 4$ and $g = x^2 + 15$.

n	-9	-8	-7	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5	6	7	8	9
$f(n)$	94	76	60	46	34	24	16	10	6	4	4	6	10	16	24	34	46	60	76
$g(n)$	96	79	64	51	40	31	24	19	16	15	16	19	24	31	40	51	64	79	96

(5.3.1)

Given a prime p, we look at the numbers between $-p/2$ to $p/2$ and see if a value is 0 modulo p. This will then give us a root, and then a prime ideal. Fix the notation $\beta = \sqrt{-15}$, $\alpha = (1+\beta)/2$ for the roots of g and f. We then see the following.

In R we have the factorizations $(2) = (2, \alpha)(2, \alpha - 1)$, $(3) = (3, \alpha + 1)^2$, $(5) = (5, \alpha + 2)^2$, $(7) = (7)$, $(11) = (11)$, $(13) = (13)$, $(17) = (17, \alpha - 6)(17, \alpha + 5)$, $(19) = (19, \alpha - 9)(19, \alpha + 8)$.

In S we have the factorizations $(3) = (3, \beta)^2$, $(5) = (5, \beta)^2$, $(7) = (7)$, $(11) = (11)$, $(13) = (13)$, $(17) = (17, \beta - 6)(17, \beta + 6)$, $(19) = (19, \alpha - 9)(19, \alpha + 9)$.

In S, Kummer–Dedekind shows that $(2, \beta - 1)$ is the unique prime ideal containing (2). However, it does not give a factorization. We now show that (2) does not factor into prime ideals, independent of the Theorem. The ideal (2) has norm 4. This implies that only primes above 2 can divide it. We do not have equality $(2, \beta - 1) = (2)$, because the norms of these ideals are 2 and 4, respectively. So we are done if we can show that $(2, \beta - 1)^2$ properly contains (2), because in that case neither do higher powers work.

We have $(2, \beta - 1)^2 = (4, 2\beta - 2, -14 - 2\beta) = (4, 2\beta - 2)$. The quotient $S/(2, \beta - 1)^2$ is therefore isomorphic with $\mathbb{Z}[x]/(x^2 - 15, 4, 2x - 2)$, or to $(\mathbb{Z}/4\mathbb{Z})[x]/(x^2 - 15, 2x - 2)$. Using $x^2 - 15$, we can represent every element of this ring by a polynomial of degree at most 1. Subtracting multiples of 4 and $2x - 2$ then gives the non-equivalent representatives $0, 1, 2, 3, x, x + 1, x + 2, x + 3$. In other words, the norm of the ideal $(2, \beta - 1)^2$ equals 8, and therefore it cannot be equal to (2).

Alternatively, you may want to check directly (as in Section 2.5) that $(2, \beta - 1)$ is not invertible. Then we cannot have $(2) = (2, \beta - 1)I$ for some other ideal, because then $I(2)^{-1}$ would be an inverse for $(2, \beta - 1)$.

(ii) In R, all prime ideals are invertible. Theorem 1.8.4(2) shows that the only primes of S that may not be invertible are above the index $[R : S]$, that is, above 2. And indeed $(2, \beta - 1)$ is not invertible, because the corresponding division with remainder gives $f(1) = 16$, which is in $2^2\mathbb{Z}[x]$.

Principality can be investigated by using the norm form. In S, we get $\mathrm{nm}(x + y\sqrt{-15}) = x^2 + 15y^2$. This does not assume values in $\{2, 3, 5\}$, so the prime ideals of S above these rational primes are not principal. Of course (7), (11) and (13) are. As for 17 and 19, the primes above 17 are again not principal, but those above 19 are, since there exists an element $\gamma = 2 + \sqrt{-15}$ of norm 19 in S, which therefore generates one of these ideals; $19/\gamma$ then necessarily generates the other.

Every element of R is of the form $(x + y\sqrt{-15})/2$ with x and y integral (even though not every element of this form is in R). The norm form then becomes $(x^2 + 15y^2)/4$. The analysis is norm slightly more difficult, but it turns out that the primes above $2, 3, 5$ are again not principal. Of course (7), (11) and (13) are again principal. As for 17 and 19, the primes above 17 are again not principal, since $x^2 + 15y^2 = 68$ has no integral solutions, but the primes above 19 are, since we can use the generators from S.

Note that we need not treat the case R and S separately in these questions. In fact, Proposition 1.8.1 shows that when not above 2, we could simply have restricted to S in the previous part of the question and extended the ideals obtained to R.

Exercise 7.

(i) We have seen in the previous exercise that $\mathfrak{p}$ and $\mathfrak{q}$ are not principal. On the other hand, $\mathfrak{p}^2 = (2, \alpha)^2 = (4, 2\alpha, \alpha - 4) = (\alpha)$ because $4 = -\alpha^2 - \alpha$. Using Proposition 2.4.1, we see that the element $\alpha + 6$ generates an ideal of norm 34. I claim that $\alpha + 6$ is in both $\mathfrak{p}$ and $\mathfrak{q}$. Assuming this, we know that $(\alpha + 6) \subseteq \mathfrak{pq}$. So the ideal $I = \mathfrak{pq}(\alpha + 6)^{-1}$ is integral, but by the Kummer–Dedekind theorem and the multiplicativity of the norm for ideals of $\mathcal{O}_K$ (Theorem 1.10.3), we see that $\mathrm{nm}(I) = \mathrm{nm}(\mathfrak{p})\,\mathrm{nm}(\mathfrak{q})/\,\mathrm{nm}((\alpha{+}6)) = 2{\cdot}17/34 = 1$. Therefore $I = R$ and $(\alpha{+}6) = \mathfrak{pq}$ is principal. And therefore $\mathfrak{q}^2 = (\mathfrak{pq})^2/\mathfrak{p}^2$ is principal as well.

Now to prove our claim. As in the discussion after Proposition 1.8.2, we see that $\mathfrak{p}$ corresponds to the evaluation $\mathcal{O}_K = \mathbb{Z}[\alpha] \to \mathbb{Z}/2\mathbb{Z}$ sending α to 0. The element $(\alpha + 6)$ in the kernel of this evaluation, which is $\mathfrak{p}$. Hence so is the ideal $(\alpha + 6)$ generated by it. And from the description of $\mathfrak{q}$, it is obvious that $(\alpha{+}6)$ is contained in it.

(ii) The ideal $I = \mathfrak{p}^2\mathfrak{q}^2$ is principal because both $\mathfrak{p}^2$ and $\mathfrak{q}^2$ are. Let $x = (I)$, $(y_1) = \mathfrak{p}^2$, $(y_2) = \mathfrak{q}^2$, and $(z_1) = \mathfrak{pq}$. Then up to units we have $x^2 = y_1y_2 = z^2$, because we are in a domain and all these elements generate the same ideals.

Now y_1, y_2, and z are irreducible. Indeed, if they were not, then the factors in a factorization would generate strictly larger ideals, hence $\mathfrak{p}$ or $\mathfrak{q}$ would be principal, and we know that this is not the case. Also, these irreducible elements are not equivalent under multiplication with a unit. This follows from the fact that they generates different ideals. We have our distinct factorizations $x = uy_1y_2 = vz^2$.

5.4 Solutions to Assignment 4

Exercise 1.

(i) Let S be the ring of integers $\mathbb{Z}[\frac{1+\sqrt{13}}{2}]$ of the fraction field $K = \mathbb{Q}(\sqrt{13})$ of R. Then R is an order in K which has index 6 in S. By Theorem 1.8.4(2) and Proposition 1.8.1, we see that the only non-invertible prime ideals of R are over 2 and 3, the prime divisors of 6. Let $\alpha = 3\sqrt{13}$ be the generator of R. It has minimal polynomial $f = x^2 - 117$. Modulo 2, this factors as $(x - 1)^2$, the square root of which we can lift to $x - 1$. The corresponding remainder term equals $f(1) = -116$, which is divisible by 4. So the unique prime ideal $(2, \alpha - 1)$ above 2 is not invertible. Modulo 3, we have to factor x^3, and lifting the factor to x, we get a remainder equal to 117, which is divisible by 9, so the unique prime ideal $(3, \alpha)$ above 3 is non-invertible as well.

(ii) Let $\mathfrak{p}_2$ be the prime ideal $(2, \alpha - 1)$. We know that $\mathfrak{p}_2$ is not invertible. I claim this this implies that the principal ideal (2) is not a product of prime ideals. Indeed, $\mathfrak{p}_2$ is the unique prime of R over 2, so (2) would then have to be a power of $\mathfrak{p}_2$. But if we had $\mathfrak{p}_2^n = (2)$, then $\mathfrak{p}_2$ would have inverse $\mathfrak{p}_2^{n-1}(2)^{-1}$.

(iii) The ideal $\mathfrak{p}_2$ has norm 2, whereas the ideal (2) has norm 4. On the other hand, I claim that $\mathfrak{p}_2^2$ has norm 8. So we can take $I = J = \mathfrak{p}_2$.

To show our claim, consider the ideal $\mathfrak{p}_2^2 = (4, 2\alpha - 2, \alpha^2 - 2\alpha + 1) = (4, 2\alpha - 2, 118 - 2\alpha) = (4, 2\alpha - 2)$. The quotient $R/\mathfrak{p}_2^2$ is isomorphic with $(\mathbb{Z}[x]/(x^2 - 117))/(4, 2x - 2)(\mathbb{Z}[x]/(x^2 - 117))$, which is just $\mathbb{Z}[x]/(4, 2x - 2, x^2 - 117)$ or $\mathbb{Z}/4\mathbb{Z}[x]/(2x - 2, x^2 - 1)$. Using $x^2 - 1$, every class in the quotient can be represented by an element of the form $a_0 + a_1 x$, with a_0, a_1 in $\mathbb{Z}/4\mathbb{Z}$. Modding out the multiples of $2x - 2$, we get the classes $0, 1, 2, 3, x, x + 1, x + 2, x + 3$, of which there are 8.

A more slick proof is as follows. We certainly have an inclusion $\mathfrak{p}_2^2 \subseteq 2$, so if the norm of $\mathfrak{p}_2^2$ were to equal 4, then we would have an equality $\mathfrak{p}_2^2 = (2)$, and showed in part (ii) that this is impossible.

Conversely, the methods above also give an alternative proof of the fact that (2) is not a product of prime ideals. Indeed, only the prime ideal $\mathfrak{p}_2$ contains 2, so (2) would then have to be a power of $\mathfrak{p}_2$. It is not the first power because its norm equals 4, but neither can it be a higher power of $\mathfrak{p}_2$, since these are all contained in $\mathfrak{p}_2^2$ and therefore have norm at least 8.

Exercise 2. Let r be the image of x in K. The discriminant -24300 of f factors as $-2^2 3^5 5^2$. So the only primes that could divide the index $[\mathcal{O}_K : \mathbb{Z}[r]]$ are $2, 3, 5$.

Modulo 5, we get the factorization x^3. Lifting to the factor x, we get remainder $f(0) = 20$, which is not in $5^2\mathbb{Z}[x]$. Therefore 5 does not divide the index $[\mathcal{O}_K : \mathbb{Z}[r]]$.

Modulo 3, we get the factorization $x^3 - 1 = (x - 1)^3$. Lifting to the factor $x - 1$, we get remainder $f(1) = 36$, which is in $3^2\mathbb{Z}[x]$. So here the prime 3 does divide the index $[\mathcal{O}_K : \mathbb{Z}[r]]$. We have to enlarge the ring, and know how to do this by Kummer–Dedekind. Division with remainder gives $f = (x^2 + x + 16)(x - 1) + 36$, so we know that the element $\beta = (r^2 + r + 16)/3$ is integral. We may as well take $\beta = (r^2 + r + 1)/3$ instead, since it differs by an integer. Let us now consider the ring $\mathbb{Z}[\beta]$. It can be described as $\mathbb{Z}[x]/(f_\beta)$, where $f_\beta = x^3 + 9x^2 + 27x - 13$ is the minimal polynomial of β (see the notes for details on how to calculate these minimal polynomials). Modulo 3, this polynomial factors as $x^3 - 1 = (x - 1)^3$ again, but this time the remainder $f(1)$ under division with the lift $x - 1$ equals $f_\beta(1) = 24$, which is not in $3^2\mathbb{Z}[x]$. We conclude that 3 does not divide the index $[\mathcal{O}_K : \mathbb{Z}[\beta]]$.

Modulo 2, we get the factorization $x^3 - x = x(x - 1)^2$. The first factor does not correspond to a non-invertible ideal because it occurs only once. Lifting the other factor to $x - 1$, we get remainder $f(1) = 36$, which is in $2^2\mathbb{Z}[x]$. So the prime 2 also divides the index $[\mathcal{O}_K : \mathbb{Z}[r]]$. We have to enlarge the ring, and know how to do this by Kummer–Dedekind. Division with remainder gives $f = (x^2 + x + 16)(x - 1) + 36$, so we know that the element $\gamma = (r^2 + r + 16)/2$ is integral. We may as well take $\gamma = (r^2 + r)/2$ instead, since it differs by an integer. Let us now consider the ring $\mathbb{Z}[\gamma]$. It can be described as $\mathbb{Z}[x]/(f_\gamma)$, where $f_\gamma = x^3 + 15x^2 + 75x - 10$ is the minimal polynomial of γ. Modulo 2, this polynomial factors as $x^3 + x^2 + x = x(x^2 + x + 1)$. Both factors are single, so the corresponding ideals are invertible and we see that 2 does not divide the index $[\mathcal{O}_K : \mathbb{Z}[\beta]]$.

Now let R be the ring $\mathbb{Z}[r, \beta, \gamma]$. I claim that $R = \mathcal{O}_K$. Indeed, R is certainly a subring of $\mathcal{O}_K$. The index $[\mathcal{O}_K : R]$ can only contain the primes 2 and 3 because R contains $\mathbb{Z}[r]$, but neither do these primes occur in the index because R contains $\mathbb{Z}[\gamma]$ and $\mathbb{Z}[\beta]$, in which no enlargement at 2, respectively 3, takes place as the primes above theses rational primes are already invertible in these rings. So $[\mathcal{O}_K : R] = 1$ and $\mathcal{O}_K = R$.

Exercise 3. Let $x_1 = 5r^2 + r + 151$, let $x_2 = -8r^2 + 5r - 7$. Let $I_0 = (x_1, x_2)$ be the ideal of the order $\mathbb{Z}[r]$ generated by x_1 and x_2, and let I be the ideal of $\mathcal{O}_K$ extending I_0, that is, the ideal generated by the same elements as a subset of $\mathcal{O}_K$. Calculating the necessary matrices and taking the determinants, we see that x_1 and x_2 have norm $3^2 \cdot 13^2 \cdot 2153$ and $-2^2 \cdot 3^2 \cdot 7 \cdot 13 \cdot 29$ in $\mathbb{Z}[r]$, respectively. The norm of I divides both these norms, and hence $3^2 \cdot 13$ as well. So we factor the ideals (3) and (13) in $\mathbb{Z}[r]$ first.

Modulo 13, the polynomial f factors as $x^3 + x + 1 = (x + 6)(x^2 - 6x - 2)$. These factors are both single, so these ideals are invertible and 13 does not divide the index $[\mathcal{O}_K : \mathbb{Z}[r]]$. We get a single ideal $\mathfrak{p}_{13} = (13, r + 6)$ of norm 13, which is the kernel of the map $\mathbb{Z}[r] \to \mathbb{Z}/13\mathbb{Z}$ sending r to -6. Under this map, both x_1 and x_2 are sent to 0, so I_0 is contained in the prime ideal $\mathfrak{p}_{13}$ (and I in its extension to $\mathcal{O}_K$). It is not contained in the other prime ideal above 13 because we have already exhausted the factor 13 in the gcd above.

Modulo 3, the polynomial f factors as $x^3 + x - 1 = (x + 1)(x^2 - x - 1)$. These factors are both single, so these ideals are invertible and 3 does not divide the index $[\mathcal{O}_K : \mathbb{Z}[r]]$. We get an ideal $\mathfrak{p}_3 = (3, r + 1)$ of norm 3 and an ideal $\mathfrak{q}_9 = (3, r^2 - r - 1)$ of norm 3^2. The ideal $\mathfrak{p}_3$ is the kernel of the map $\mathbb{Z}[r] \to \mathbb{Z}/3\mathbb{Z}$ sending r to -1. Under this map, neither of x_1 and x_2 are sent to 0, so if it I is contained in a prime ideal above 13 at all, then in (the extension of) $\mathfrak{q}_3$. But again, since neither x_1 and x_2 are in $\mathfrak{p}_3$, both are in fact in $\mathfrak{q}_3$ for reasons of norm, and $\mathfrak{q}_3$ divides I.

Of course one can calculate $\mathcal{O}_K$, but why bother? The factorizations above show that neither 3 nor 13 divides the index $[\mathcal{O}_K : \mathbb{Z}[r]]$, so the ideals in these rings are in correspondence by Proposition 1.8.1. Since we have exhausted or gcd, we get the factorization $I = \mathfrak{q}_9\mathfrak{p}_{13}$ in $\mathcal{O}_K$.

A final word of caution. Contrary to the impression that this exercise may convey, it is of course possible that the norms of generators are all divisible by a prime p, but the resulting ideal is not divisible by a prime over p. For example, take the two ideals of $\mathbb{Z}[i]$ of norm 5 and choose generators π_1, π_2. Then both generators of the ideal $I = (\pi_1, \pi_2)$ have norm divisible by 5, while I is of course the unit ideal by coprimality.

Exercise 4. The unit group of $\mathcal{O}_L$ is easiest to calculate. The ring $\mathcal{O}_L$ equals $\mathbb{Z}[\sqrt{-29}]$, and the positive norm form $x^2 + 29y^2$ only assumes the values ± 1 for $(x, y) = (\pm 1, 0)$, so we have $\mathcal{O}_L = \{\pm 1\}$. As for $\mathcal{O}_K$, we have $\mathcal{O}_K = \mathbb{Z}[\alpha]$, where $\alpha = (1 + \sqrt{29})/2$, and K embeds into $\mathbb{R}$. So the roots of unity of $\mathcal{O}_K$ are contained in, and hence equal to $\{\pm 1\}$. By Dirichlet's unit theorem, we need only one other element of infinite order to generate the unit group. Evaluating the minimal polynomial $\alpha^2 - \alpha - 7$ at small values $u = 2 + \alpha$ as a "small" unit of norm -1. We want to show that -1 and u generate $\mathcal{O}_K^*$.

If not, then either u or $-u$ is a strict power u_0^k of another unit u_0. Suppose first that $u = u_0^k$. Write $u_0 = a + b\alpha$. Then if a and b had different sign, so would the entries coefficients of u, which is not true. Neither can we have a, b negative if k is odd, and if k is even, then we can always change u_0 to $-u_0$. So we may suppose that a and b are positive. It is clear that we have $b \neq 0$. Then since $\alpha^2 = \alpha + 7$, the values of the coefficients a and b become strictly larger for each larger power of u_0. This leaves us to check a and b between 0 and 2, which makes it feasible to verify that u is not a power of another unit.

On the other hand, suppose that $u = -u_0^k$. Again we see that a and b have the same sign, and we may once more suppose that a and b are both positive. Choosing the embedding $\alpha \mapsto (1 + \sqrt{29})/2$ under which α is positive, we now immediately get a contradiction.

Now for the class groups. Let us start with $\mathcal{O}_K$. The Minkowski bound $\frac{2!}{2^2}\sqrt{29} = \sqrt{29}/2$ is strictly smaller than 3, so we only have to look at the ideals of norm 2 over 2. But the polynomial $x^2 - x - 7$ is irreducible modulo 2, yielding a prime of norm 4. So there are no primes of norm 2, and the class group is trivial.

As for $\mathcal{O}_L$, we now get the Minkowski bound $\frac{4}{\pi}\frac{2!}{2^2}\sqrt{4 \cdot 29}$. This bound is strictly smaller than 7, so we factor the ideals above $2, 3, 5$ using Kronecker-Dedekind. As in the previous exercise set, we tabulate small values of f:

n	-4	-3	-2	-1	0	1	2	3	4
$f(n)$	45	38	33	30	29	30	33	38	45

(5.4.1)

If we let $\beta = \sqrt{-29}$, then we have $(2) = (2, \beta - 1)^2 = \mathfrak{p}_2^2$, $(3) = (3, \beta - 1)(3, \beta + 1) = \mathfrak{p}_3\mathfrak{q}_3$, and $(5) = (5, \beta - 1)(5, \beta + 1) = \mathfrak{p}_5\mathfrak{q}_5$. This already shows that the class group is generated by the classes $[\mathfrak{p}_2], [\mathfrak{p}_3] = -[\mathfrak{q}_3]$ and $[\mathfrak{p}_5] = -[\mathfrak{q}_5]$. Now the fact that $f(1) = 30$ implies that the ideal $(\alpha - 1)$ has norm 30, which after factoring will express $[\mathfrak{p}_2]$ in terms of $[\mathfrak{p}_3]$ and $[\mathfrak{p}_5]$. The element $\alpha - 4$ similarly generates and ideal of norm $45 = 3^2 \cdot 5$. So we can express $[\mathfrak{p}_5]$ in terms of $[\mathfrak{p}_3]$. Therefore $\mathfrak{p}_3$, which we can choose to be the ideal given in the question, generates the class group. (Factoring ideals by the usual methods above, we see more precisely that $(\alpha - 1) = \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5$ and $(\alpha - 4) = \mathfrak{p}_3^2\mathfrak{q}_5$.)

Now the ideals $\mathfrak{p}_3$, $\mathfrak{p}_3^2$ and $\mathfrak{p}_3^3$ are not principal because the norm form does not assume values in $\{3, 9, 27\}$ except for the element 3 or norm 9, which does not generate $\mathfrak{p}_3^2$ but rather $\mathfrak{p}_3\mathfrak{q}_3$. On the other hand, we now see that $2[\mathfrak{p}_3] = -[\mathfrak{q}_5] = [\mathfrak{p}_5] = -[\mathfrak{p}_3] - [\mathfrak{p}_2]$. So $3[\mathfrak{p}_3] = [\mathfrak{p}_2]$. But $2[\mathfrak{p}_2] = 0$ because $\mathfrak{p}_2^2 = (2)$. So $\mathfrak{p}_3$ is indeed of order 6.

Exercise 5. We can factor $(y + \sqrt{-33})(y - \sqrt{-33}) = x^3$ in $R = \mathbb{Z}[\sqrt{-33}]$. This is the ring of integers $\mathcal{O}_K$ of the field $K = \mathbb{Q}(\sqrt{-33})$. The Minkowski bound for K equals 7, so we write $\alpha = \sqrt{-33}$ and factor the ideals primes $2, 3, 5, 7$ for $(2) = (2, \alpha - 1)^2 = \mathfrak{p}_2^2$, $(3) = (3, \alpha)^2 = \mathfrak{p}_3$, $(5) = (5) = \mathfrak{p}_{25}$ and $(7) = (7, \alpha - 2)(7, \alpha + 2) = \mathfrak{p}_7\mathfrak{q}_7$. We have $f(3) = 42$, which indicates that the classes $[\mathfrak{p}_7]$ and $[\mathfrak{q}_7] = -[\mathfrak{p}_7]$ above 7 can be expressed in terms of $\mathfrak{p}_2$ and $\mathfrak{p}_3$. Furthermore, since both $\mathfrak{p}_2$ and $\mathfrak{p}_3$ square to principal ideals, we have $2[\mathfrak{p}_2] = 2[\mathfrak{p}_3] = 0$. In particular, the order of the class group $\mathrm{Cl}(\mathcal{O}_K)$ is a power of 2.

The greatest common divisor of the ideals $(y+\sqrt{-33})$ and $(y-\sqrt{-33})$ divides $(2\sqrt{-33})$. This ideal factors as $\mathfrak{p}_2^2\mathfrak{p}_3\mathfrak{p}_{11}$, where $\mathfrak{p}_{11}$ is the unique ideal of $\mathcal{O}_K$ above 11. Since the norms of the elements $y + \sqrt{-33}$ and $y - \sqrt{-33}$ are equal and $\mathfrak{p}_3$ and $\mathfrak{p}_{11}$ are the unique ideals of $\mathcal{O}_K$ above 3 and 11, we see that $\mathfrak{p}_3$ and $\mathfrak{p}_{11}$ divide either none or both of $y + \sqrt{-33}$ and $y - \sqrt{-33}$. But if they divided both, then they would occur with larger multiplicity in $(2\sqrt{-33})$. As for $\mathfrak{p}_2$, if this were to divide $(y + \sqrt{33})$, then this element would be sent to zero under the homomorphism $\mathcal{O}_K \to \mathcal{O}_K/\mathfrak{p}_2 \cong \mathbb{Z}/2\mathbb{Z}$ corresponding to $\mathfrak{p}_2$, which sends α to 1. But then y would be odd. This is impossible, because in that case $y^2 + 33$ is congruent to 2 modulo 4, which is not a third power.

Alternatively, if $\mathfrak{p}_2$ divides the greates common divisor, then by using a similar uniqueness argument we see that either $\mathfrak{p}_2^2$ or $\mathfrak{p}_2^4$ is the *exact* power of $\mathfrak{p}_2$ in the factorization of the prime ideal generated by x^3, a contradiction with the fact that this ideal is a third power.

So the ideals $(y + \sqrt{-33})$ and $(y - \sqrt{-33})$ are coprime. The product of these ideal is a third power, hence so are the ideals themselves because of coprimality. But since the order of the class group is a power of 2, it is in particular coprime with 3, which means that any principal ideal that is a third power is in fact the third power of a principal ideal. Since all units of $\mathcal{O}_K$ are third powers, we conclude that $y + \sqrt{-33} = (a + b\sqrt{-33})^3 = \ldots + (3a^2b - 33b^3)\sqrt{-33}$ for integral a and b, which is impossible.

Exercise 6. Let r be the image of x in K. We know how to calculate the discriminant $\Delta_A(K)$ for the basis $A = \{1, r, r^2\}$ from a previous exercise sheet, and it equals -2592. This number factors as $-2^5 3^4$. So the only primes that can divide the index $[\mathcal{O}_K : \mathbb{Z}[r]]$ are 2 and 3, and we have to use Kummer–Dedekind to analyse the situation at those primes.

Modulo 3, we get the factorization $x^3 - 1 = (x-1)^3$. Lifting to the factor $x - 1$, we get remainder $f(1) = -12$, which is not in $3^2\mathbb{Z}[x]$. Therefore 3 does not divide the index $[\mathcal{O}_K : \mathbb{Z}[r]]$.

Modulo 2, we get the factorization $x^3 - x = x(x-1)^2$. Lifting to the factor $x - 1$, we get remainder $f(1) = -12$, which is in $2^2\mathbb{Z}[x]$. So here the prime 2 does divide the index $[\mathcal{O}_K : \mathbb{Z}[r]]$. We have to enlarge the ring, and know how to do this by Kummer–Dedekind. Division with remainder gives $f = (x^2 + x - 2)(x-1) - 12$, so we know that the element $\beta = (r^2 + r - 2)/2$ is integral. We may as well take $\beta = (r^2 + r)/2$ instead, since it differs by an integer. Let us now consider the ring $\mathbb{Z}[\beta]$. It can be described as $\mathbb{Z}[x]/(g)$, where $g = x^3 - 3x^2 - 6x - 10$ is the minimal polynomial of β (again, if you do not already know how to calculate such a minimal polynomial, then this process is explained in Section 2.1 of the notes). Modulo 2, the polynomial g factors as $x^3 - x^2 = x^2(x-1)$. This time the remainder $f(0)$ under division with the lift x equals $g = -10$, which is not in $2^2\mathbb{Z}[x]$. We conclude that 2 does not divide the index $[\mathcal{O}_K : \mathbb{Z}[\beta]]$.

Reasoning as before, we see that $\mathcal{O}_K = \mathbb{Z}[r, \beta]$, and also that $\Delta(K) = -2^5 3^4/2^2 = -2^3 3^4$ since $\mathcal{O}_K$ contains $\mathbb{Z}[r]$ as a subring of index 2. This is not immediately of the pleasing form $\mathbb{Z}[\gamma]$ because a discriminant calculation shows that for the basis $B = \{1, \beta, \beta^2\}$ we have $\Delta_B(K) = -2^3 3^6 = 3^2 \Delta(K)$, so $[\mathcal{O}_K : \mathbb{Z}[\beta]] = 3$. In fact, I do not know if there exists a γ generating $\mathcal{O}_K$. Still, we can determine the factorizations of integral prime ideals. Indeed, as long as we are not above 2, then we work in $\mathbb{Z}[r]$, then Kummer–Dedekind tells us that we can factor in $\mathbb{Z}[r]$ and extend the resulting primes to $\mathcal{O}_K$. And when not above 3, we can use the ring $\mathbb{Z}[\beta]$. Alternatively, we have seen Proposition 1.8.1 that as long as we are not above 2, then the ideals off $\mathcal{O}_K$ correspond to those of $\mathbb{Z}[r]$, and when not above 3, the ideals off $\mathcal{O}_K$ correspond to those of $\mathbb{Z}[\beta]$. This means we can still determine the class group of $\mathcal{O}_K$.

The polynomial f has a single real root. Therefore the Minkowski bound for K equals $\frac{4}{\pi}\frac{3!}{3^3}\sqrt{648}$, which is strictly smaller than 8. So we have to factor the rational primes up to 7. Using Kummer–Dedekind gives $(2) = (2, \beta)^2(2, \beta - 1) = \mathfrak{p}_2^2\mathfrak{q}_2$, $(3) = (3, r-1)^3$, $(5) = (5, r)(5, r^2 + 2) = \mathfrak{p}_5\mathfrak{q}_{25}$, $(7) = (7, r+3)(7, r^2 - 3r - 1) = \mathfrak{p}_7\mathfrak{q}_{49}$.

We make a small table of values of f and g.

n	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5	6
$f(n)$	-208	-120	-62	-28	-12	-8	-10	-12	-8	8	42	100	188
$g(n)$	-298	-180	-98	-46	-18	-8	-10	-18	-26	-28	-18	10	62

(5.4.2)

The value $f(0) = -10$ implies a relations between an ideal above 2 and $\mathfrak{p}_5$, so since $[\mathfrak{p}_5] + [\mathfrak{q}_{25}] = 0$ anyway, we can discard the ideals above 5 from the list of generators. Similarly, the small value $g(4) = -18$ shows that $(4 - \beta)$ is contained in an ideal above 2. Since $(4 - \beta)$ is sent to 0 under the homomorphism $\mathbb{Z}[\beta] \to \mathbb{Z}[\beta]/(2, \beta) \cong \mathbb{Z}/2\mathbb{Z}$ sending β to 0, and to 1 under the homomorphism corresponding to $\mathfrak{q}_2$, we see that in fact $(4 - \beta) = \mathfrak{p}_2\mathfrak{p}_3^3$, whence the relation $[\mathfrak{p}_2] = -2[\mathfrak{p}_3]$ in the class group. Since $3[\mathfrak{p}_3] = 0$, we have $[\mathfrak{p}_2] = [\mathfrak{p}_3]$ and $[\mathfrak{q}_2] = -[\mathfrak{p}_2] = -[\mathfrak{p}_3]$. So it remains to look for a dependency involving $\mathfrak{p}_7$, which can be found by considering the ideal $(3 - \beta)$ of norm $f_\beta(3) = -28$. This shows that $[\mathfrak{p}_7]$ can be expressed in terms of the the classes of the ideals above 2. hence in terms of $[\mathfrak{p}_3]$. We see that $[\mathfrak{p}_3]$ generates the class group, and we already knew that $3[\mathfrak{p}_3] = 0$ from Kummer–Dedekind. We are going to show that $[\mathfrak{p}_3]$ is non-trivial, or in other words that $\mathfrak{p}_3$ is not principal.

As an aside, closer analysis yields the following equalities. You can test your factorization skills by reproducing them, but see also below for some examples. When dealing with a very big field, it is usually wiser to systematically write down the relations in the class group resulting from these factorization and then apply some linear algebra over $\mathbb{Z}$. We have $(-5-r) = \mathfrak{p}_2^3\mathfrak{p}_3\mathfrak{p}_5$, $(-3-r) = \mathfrak{p}_2^2\mathfrak{p}_7$, $(-2-r) = \mathfrak{q}_2^2\mathfrak{p}_3$, $(-1-r) = \mathfrak{p}_2^3$, $(-r) = \mathfrak{q}_2\mathfrak{p}_5$, $(1-r) = \mathfrak{p}_2^2\mathfrak{p}_3$, $(2-r) = \mathfrak{q}_2^3$, $(3-r) = \mathfrak{p}_2^3$, $(4-r) = \mathfrak{q}_2\mathfrak{p}_3\mathfrak{p}_7$, $(5-r) = \mathfrak{p}_2^2\mathfrak{p}_5^2$ and $(-5-\beta) = \mathfrak{q}_2^3\mathfrak{p}_3^2\mathfrak{p}_5$, $(-4-\beta) = \mathfrak{p}_2\mathfrak{p}_7^2$, $(-2-\beta) = \mathfrak{p}_2\mathfrak{p}_3^2$, $(-1-\beta) = \mathfrak{q}_2^3$, $(-\beta) = \mathfrak{p}_2\mathfrak{p}_5$, $(1-\beta) = \mathfrak{q}_2\mathfrak{p}_3^2$, $(3-\beta) = \mathfrak{q}_2\mathfrak{p}_7$, $(4-\beta) = \mathfrak{p}_2\mathfrak{p}_3^2$, $(5-\beta) = \mathfrak{q}_2\mathfrak{p}_5$.

We now have to think a little about the unit group $\mathcal{O}_K^*$. Since K allows an embedding into $\mathbb{R}$, the only roots of unity are ± 1, and Dirichlet shows that $\mathcal{O}_K^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$. We will find a generator of $\mathcal{O}_K^*/(\mathcal{O}_K^*)^3 \cong \mathbb{Z}/3\mathbb{Z}$. In fact, we will find a unit u that generates the unit group along with -1, but it is difficult to prove statement of this kind, and for determining the class group in this case, it suffices to find a generator of $\mathcal{O}_K^*/(\mathcal{O}_K^*)^3$.

We look for suitable units of infinite order by finding elements generating the same ideals. For this, we can look in the list of small values of f. We find that $(-1-r)$, $(2-r)$ and $(3-r)$ all generate ideals of norm 8. The ideals in $\mathcal{O}_K$ above 2 are the extensions of the ideals above 2 in $\mathbb{Z}[r]$ (that is, they do not, as usually happens, split up further), so we can identify the factorizations by looking in the ring $\mathbb{Z}[r]$. There the ideals $\mathfrak{p}_2$ and $\mathfrak{q}_2$ correspond to the homomorphisms $\mathcal{O}_K \to \mathbb{Z}/2\mathbb{Z}$ sending r to 1 and 0, respectively. We see that $-1-r$ and $3-r$ are not in $\mathfrak{q}_2$, and that $2-r$ is not in $\mathfrak{p}_2$. Therefore $(2-r) = \mathfrak{q}_2^3$ and $(-1-r) = (3-r) = \mathfrak{p}_2^3$. We find the unit $(-1-r)/(3-r) = -\beta - r - 2$.

An alternative way to see this is to rewrite r in terms of β by the usual linear algebra process in Section 2.1. We have $r = (\beta^2 - 2\beta - 5)/3$. The primes $\mathfrak{p}_2$ and $\mathfrak{q}_2$ correspond to the homomorphisms $\mathbb{Z}[\beta] \to \mathbb{Z}/2\mathbb{Z}$ sending β to 0 and 1, respectively. Evaluating r, we again see that it gets sent to 1 and 0, respectively, so that we can proceed as above.

If you are uncomfortable with this switching between r and β, then you can also use the small values of β. We spot two ideals $(-2-\beta)$ and $(4-\beta)$ of norm 18. Since there is a unique ideal of $\mathcal{O}_K$ over 3, we only have to see which ideals above 2 occur in their factorizations. Now because 2 is coprime to the index $[\mathcal{O}_K : \mathbb{Z}[\beta]]$, the ideals of these rings over 2 are in bijective correspondence by the Proposition 1.8.1. And $\mathfrak{p}_2$, respectively $\mathfrak{q}_2$, corresponds to the evaluation $\mathbb{Z}[\beta] \to \mathbb{Z}/2\mathbb{Z}$ sending β to 0 and 1, respectively. We now see that $(-2-\beta) = (4-\beta) = \mathfrak{p}_2\mathfrak{p}_3^2$, and obtain the unit $(-2-\beta)/(4-\beta) = \beta + r + 2$, the same as the previous unit up to multiplication by the root of unity -1.

So let $u = \beta + r + 2 = (1+r)/(3-r) = (-2-\beta)/(4-\beta)$. We show that u generates $\mathcal{O}_K^*/(\mathcal{O}_K^*)^3$. For this, it suffices to find a prime of $\mathcal{O}_K$ modulo which u is not a third power. There are loads of clever methods to refine this search if you know a lot about finite fields (3 should divide $q - 1 = p^f - 1$, et cetera), but in this case you quickly find a small prime that works. Look modulo $\mathfrak{p}_7$. Since the tables show that $\mathfrak{p}_7 = (7, r+3) = (7, \beta - 3)$, the element u is sent to $3 - 3 + 2 = (1-3)/(3+3) = (-2-3)/(4-3) = 2$ modulo 7, which is not a third power. Our claim is proved.

We now show that $\mathfrak{p}_3$ is not principal, which will show that $\mathrm{Cl}(\mathcal{O}_K) \cong \mathbb{Z}/3\mathbb{Z}$. Suppose that $\mathfrak{p}_3 = (x)$ for some $x \in \mathcal{O}_K$. Then $(3) = \mathfrak{p}_3^3 = (x^3)$, so since we can change x by an element of $\mathcal{O}_K^*$ and hence x^3 by an element of $(\mathcal{O}_K^*)^3$, we either have $3 = y^3$, $3 = uy^3$, or $3 = u^{-1}y^3$ for some $y \in \mathcal{O}_K$. In other words, either 3, $3u$, or $3u^{-1}$ would be a third power. We can look modulo 7 again to exclude 3 and $3u^2$. To exclude $3u$, we have to search a little further in our table, to get the prime $\mathfrak{p}_{13} = (13, r+6) = (13, \beta - 2)$ above 13. Here u evaluates to $2 - 6 + 2 = (1-6)/(3+6) = (-2-2)/(4-2) = -2$, and $3u$ to -6, which is not a third power modulo 13 since its fourth power does not equal 1.

We are done: $\mathrm{Cl}(\mathcal{O}_K)$ is isomorphic with $\mathbb{Z}/3\mathbb{Z}$, generated by the class $[\mathfrak{p}_3]$.

Bibliography

[1] J. Bosman and F. Bouyer. Algebraic Number Theory. Notes at http://www2.warwick.ac.uk/fac/sci/maths/people/staff/bouyer/algebraic_number_theory.pdf.

[2] S. Lang. *Algebraic Number Theory.* Springer, 1994.

[3] J. Milne. Algebraic Number Theory. Notes at http://jmilne.org/math/CourseNotes/ant.html.

[4] W. Stein. Introduction to Algebraic Number Theory. Notes at http://modular.math.washington.edu/129-05/notes/129.pdf.

[5] P. Stevenhagen. Number Rings. Notes at http://websites.math.leidenuniv.nl/algebra/ant.pdf.

Index