Algebraic Number Theory

MATH3066 and MATH4006

Spring 26

Chris Wuthrich

0 Contents

Thanks: These lecture notes are based on many good sources, one of them the excellent notes by Samir Siksek [5]. I also thank the following students for pointing out errors in the notes or the problem sheets, which helped me to improve them: Katie Greenwood, Pallavi Kankani, Marek Kuczynski.

Information on the module

Lecturer : Chris Wuthrich,
christian.wuthrich@nottingham.ac.uk

Lectures :
- Mondays 4 – 6, Physics B23
- Thursdays 11 – 12, Chemistry C15
- Fridays 12 – 1, Physics B21

Office Hours : Mondays 1pm-3pm. But feel free to come to my office C58 anytime to ask questions.

Module webpage : The main module webpage is on moodle:

https://moodle.nottingham.ac.uk/course/view.php?id=160336.

There you will find all the material concerning this module.

Booklist : There are plenty of books and online lecture material on algebraic number theory. This module recommends Samir Siksek's Lecture Notes [5]. More, like [3, 6, 7, 4], are in the list at the end of the notes. Most books on algebraic numbers are in QA 247 in the George Green Library. Please ask if you are interested in a particular topic.

Assessments : For the level 3 version MATH3066 of this module, the assessment is concentrated in a single exam in the May exam period. It is a 3h exam.

The level 4 version MATH4006 has two components: The same exam as the level 3 module, which will count for 90% of the total module mark, and an oral presentation worth 10%.

More information on these assessment will be shared later via the moodle page.

These notes : The notes have been rewritten completely for 2026; and I am writing them as the module progresses. This document changes over the course of the semester, but the latest version is always on moodle.

Please tell me about anything that could be improved or corrected.

Computer software : Not needed at all, but if you wish to experiment with algebraic numbers you may want to try out the free SageMath which is based on python. pari-gp (in C++) and hecke (in Julia) are other options.

All graphics and computations in these notes are done with SageMath.

0.1 Format of this document

All formal statements (Theorem, Lemmas, ...) are formatted like

dummy_thm

Theorem 0.1

We have $2 + 3 = 5$.

and they will have a

Proof. To convince you that they are true with a square when they conclude: □

Also included are

Examples. Always in blue. With a diamond at the end: ◇

Digression

can be ignored safely for the exam, they contain extra material and information for further reading beyond the module material.

0.2 Prerequisites

The material of this module relies on the second year module [Algebra and Number Theory] MATH2015 and the first year [Algebra] MATH1104.

The module has strong links to [Galois Theory] MATH4070/3063, [Further Number Theory] MATH4088/3012, [Commutative Algebra] MATH4087/3022, and [Group Theory] MATH4089/3001. These connections are often explained in digressions.

Here we quickly list the definitions and the basic properties on abelian groups and fields that we assume from the start.

0.2.1 Abelian groups

abgr_subsec

Definition 0.2. An **abelian group** $\langle A, + \rangle$ is a non-empty set A together with an operation $+ : A \times A \to A$ satisfying the following axioms:

(G1 Closure): For all a, $b \in A$, we have $a + b \in A$.
(G2 Associativity): $(a + b) + c = a + (b + c)$ for all a, b, $c \in A$.
(G3 Identity): There is an element $0 = 0_A$ such that $a + 0 = 0 + a = a$ for all $a \in A$.
(G4 Inverses): For each $a \in A$ there is a unique element $-a \in A$ such that $a + (-a) = (-a) + a = 0$.
(G5 Abelian): For all a, b in A, we have $a + b = b + a$.

The basic examples are $\langle \mathbb{Z}, + \rangle$ and the cyclic group $\langle {}^{\mathbb{Z}}/_{m\mathbb{Z}}, + \rangle$ of order m. We will see plenty more.

A group **homomorphism** is a map $\varphi\colon A \to B$ between two groups A and B such that $\varphi(a + a') = \varphi(a) + \varphi(a')$ for all $a, a' \in A$. A **subgroup** is a subset B of a group containing the identity and such that $a - b \in B$ for all $a, b \in B$.

Definition 0.3. Let A be an abelian group and B a subgroup. The quotient group A/B is formed of all cosets $a+B=\{a+b \mid b\in B\}$ endowed with the group law $(a+B)+(a'+B)=(a+a')+B$.

The **kernel** of a group homomorphism φ is the subgroup $\ker\varphi=\{a\in A \mid \varphi(a)=0\}$.

first_iso_thm

Proposition 0.4: First Isomorphism Theorem

If $\varphi\colon A\to B$ is a group homomorphism, then $A/\ker(\varphi)$ is isomorphic to the image $\mathrm{im}(\varphi)$.

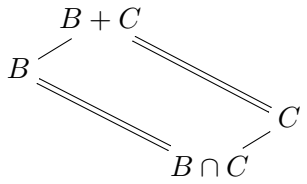
second_iso_thm

Proposition 0.5: Second Isomorphism Theorem

Let B and C be two subgroups of an abelian group A. Then $(B+C)/C$ is isomorphic to $B/(B\cap C)$.

Proof. Consider the map $\phi\colon B\to(B+C)/C$ sending b to $b+C$. A general element of $(B+C)/C$ is of the form $b+c+C$ with $b\in B$ and $c\in C$. But $b+c+C=b+C=\phi(b)$ shows that ϕ is surjective. The kernel is the set of $b\in B$ such that $b\in C$ so $\ker(\phi)=B\cap C$. By the first isomorphism theorem proves the statement now. □

To visualise this theorem, notice that $B\cap C$ is the largest subgroup contained in both B and C. Analogue $B+C$ is the smallest subgroup of A containing both B and C. The inclusions are illustrated in the right hand side picture; the Second Isomorphism Theorem says that the double lines are inclusions giving the same quotient.



0.2.2 Rings

Definition 0.6. A **ring** R is a non-empty set endowed with two binary operations $+ : R\times R\to R$, called **addition**, and $\cdot : R\times R\to R$, called **multiplication**, satisfying:

- **(R1)** $\langle R,+\rangle$ is an abelian group. $0\in R$ denotes the additive identity and $-a$ the additive inverse of $a\in R$.
- **(R2)** The structure $\langle R,\cdot\rangle$ satisfies axioms G1, G2, G3 (the identity is called $1\in R$) and G5, but not G4.
- **(R3)** Distributivity: $a(b+c)=ab+ac$ for all a, b and $c\in R$.

Note that in this module, all rings are commutative rings. Examples are $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Z}/m\mathbb{Z}$ for any integer $m>1$. For any ring R, the ring of polynomials $R[X]$ in a variable X is another important example.

Definition 0.7. A subset I of a ring R is an **ideal** if $\langle I,+\rangle$ is a subgroup and $r\cdot a\in I$ for all $r\in R$ and $a\in I$.

For an ideal I, the quotient R/I carries the structure of a ring with the multiplication given by $(a+I)\cdot(b+I) = (a\cdot b)+I$. The first isomorphism theorem holds for ring homomorphism $\varphi\colon R \to R'$, which are group homomorphisms on the additive structure such that $\varphi(1) = 1$ and $\varphi(a\cdot b) = \varphi(a)\cdot\varphi(b)$.

Proposition 0.8: Correspondence Theorem and Third Isomorphism Theorem

third_is_thm

Let I be an ideal in a ring R. For each ideal J in R such that $J \supset I$, the quotient J/I is an ideal of R/I. Conversely, every ideal of R/I is of the form J/I for some ideal J containing I. The quotient ring $(R/I)\,/\,(J/I)$ is isomorphic to R/J.

Proof. It is a good exercise to verify the following steps:

- If $J \supset I$, then J/I is an ideal of R/I.
- If B is an ideal of R/I, set $J = \bigcup_{b\in B} b \subset R$. Then J is an ideal of R containing I.
- The two constructions are inverse to each other.
- The map $\psi\colon R/I \to R/J$ sending $x+I$ to $x+J$ is well defined
- ψ is surjective.
- The kernel of ψ is J/I.
- Use the first isomorphism theorem for ψ. □

Theorem 0.9: Chinese Remainder Theorem

general_crt_thm

Let I and J be two ideals in a ring R such that $I + J = R$. Then $R/(I\cap J)$ is isomorphic to $R/I \times R/J$.

Definition 0.10. The group of **units** $R^\times$ is the set of elements $a \in R$ such that there exists a $b \in R$ with $a\cdot b = 1$.

An element $a \in R$ is **irreducible** if $a = bc$ with $b, c \in R$ implies that $b \in R^\times$ or $b \in R^\times$. It is **prime** if $a \mid b\cdot c$ implies $a \mid b$ or $a \mid c$.

Definition 0.11. An ideal I is a **prime ideal** if R/I has no non-zero zero-divisors or, equivalently, that $ab \in I$ implies $a \in I$ or $b \in I$.

0.2.3 Fields

Definition 0.12. A **field** is a ring k such that $k^\times = k \setminus \{0\}$.

Equivalently, a field is a ring with exactly two ideals (0) and k. Any ring homomorphism $k \to R$ from a field k is injective.

Proposition 0.13

The ring $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is a prime number.

For a prime number p, we denote the field $\mathbb{Z}/p\mathbb{Z}$ by $\mathbb{F}_p$.

More generally, a quotient ring R/I is a field if and only if I is a **maximal ideal**, which means that there is no ideal J such that $I \subsetneq J \subsetneq R$.

1 Number fields

1.1 Field extensions

Recall that a **field** K is a set with two operations $+$ and $\cdot$ that forms a ring such that the units (invertible elements) are all non-zero elements. Basic examples are the field of rational numbers $\mathbb{Q}$, real numbers $\mathbb{R}$, complex numbers $\mathbb{C}$, and finite fields $\mathbb{F}_p = {}^{\mathbb{Z}}/_{p\mathbb{Z}}$ for any prime number p.

Definition 1.1. If K is a subfield of L, we say that L is an **extension** of K and write L/K.

For instance, $\mathbb{C}$ is an extension of $\mathbb{R}$; but it is also an extension of $\mathbb{Q}$. Instead, $\mathbb{Q}$ cannot be an extension of $\mathbb{F}_p$, since $1+1+\cdots+1$ is never 0 in $\mathbb{Q}$.

If L is an extension of K, then L is naturally given the structure of a vector space over K: The addition of elements in L is the usual addition, and, since K is contained in L, the "scalar multiplication" with $\lambda \in K$ is the usual multiplication.

Definition 1.2. Let L/K be an extension. If the dimension of L as a K-vectors space is finite, we call this dimension the **degree** of the extension and denote it by $[L:K]$.

Now to the subject of this module.

Definition 1.3. A **number field** K is an extension of $\mathbb{Q}$, which is a finite dimensional vector space over $\mathbb{Q}$.

In other words, the additive structure of a number field is of the form $(\mathbb{Q}^d, +)$ with $d = [K:\mathbb{Q}] \geqslant 1$ the degree, but the multiplicative structure is more complicated.

Example. Just for this once, denote by $\sqrt{2.}$ the unique positive real number whose square is 2. Then the subset

$$\left\{ a + b\sqrt{2.} \;\middle|\; a, b \in \mathbb{Q} \right\}$$

of $\mathbb{R}$ is a subfield. As a $\mathbb{Q}$-vector space it is of dimension 2. This is an example of a number field of degree 2. ◇

Instead of viewing fields as subfields of $\mathbb{C}$, we will often prefer to see them as abstract extensions. The prime example of this construction is $\mathbb{C} := \mathbb{R}[X]/(X^2+1)$ which is a field since X^2+1 is an irreducible polynomial in $\mathbb{R}[X]$. The coset $X + (X^2+1)$ is denoted by i and it obeys the rule $i^2 = -1$. Remember that it is a little dangerous* to write $\sqrt{-1}$.

*Because $-1 = \sqrt{-1}\cdot\sqrt{-1} = \sqrt{(-1)\cdot(-1)} = \sqrt{1} = 1$ is wrong. If you think of $\boxed{\sqrt{-1}}$ as one symbol that can be broken up, much like i, then it is all fine.

Theorem 1.4

Let k be a field and $f \in k[X]$ an irreducible polynomial of degree d. Set K to be the field $k[X]/(f)$ and write $\alpha = X + (f) \in K$. Then $f(\alpha) = 0$ and K is a vector space over k of dimension d with basis 1, α, α^2, $\ldots$, α^{d-1}. In particular, every element in K can be written uniquely as $x_0 + x_1\alpha + \cdots + x_{d-1}\alpha^{d-1}$ with $x_i \in k$.

Proof. First, recall that K is a field, because the ideal (f) in $k[X]$ is maximal. Substituting a coset like α into f results in the coset of f applied to any polynomial in the coset because that is how we defined the ring operations in the quotient. Therefore $f(\alpha) = f(X) + (f) = (f)$ is zero in K.

Using long division, any polynomial $g \in k[X]$ can be written as $g = q \cdot f + r$ for unique polynomials q and r with $\deg(r) < \deg(f) = d$. This shows that the coset $g + (f)$ contains a unique element $r = x_0 + x_1\,X + \cdots + x_{d-1}\,X^{d-1}$ of degree smaller than d. Since $g + (f) = x_0 + x_1\,\alpha + \cdots + x_{d-1}\alpha^{d-1}$ with unique $x_i \in k$, we can conclude that 1, α, $\ldots$, α^{d-1} is indeed a basis of K as a k-vector space. Since the basis has d element, the dimension is d. □

We will write $K = k(\alpha)$ and say that K is obtained from k **by adjoining a root α of f**.

In the particular case when $k = \mathbb{Q}$ we get the following: For any irreducible polynomial $f \in \mathbb{Q}[X]$, the field $\mathbb{Q}[X]/(f)$ is a number field of degree $\deg(f)$.

In practice, we work with $\mathbb{Q}(\alpha) = \mathbb{Q}[X]/(f)$ for an irreducible polynomial

$$f = a_d\,X^d + a_{d-1}X^{d-1} + \cdots + a_0$$

with $a_i \in \mathbb{Q}$ in the following way. Every element of $\mathbb{Q}(\alpha)$ can be uniquely written as a "polynomial" of degree at most $d-1$

$$x_0 + x_1\,\alpha + x_2\,\alpha^2 + \cdots + x_{d-1}\,\alpha^{d-1}$$

with $x_i \in \mathbb{Q}$. Addition in $\mathbb{Q}(\alpha)$ is as polynomials which adds up the coefficients, and so is multiplication except that we need to remember that

$$\alpha^d = -\frac{1}{a_d}(a_0 + a_1\,\alpha + a_2\,\alpha^2 + \cdots + a_{d-1}\,\alpha^{d-1})$$

because $f(\alpha) = 0$. Just like we simplify any power of i in $\mathbb{C}$ when multiplying.

Examples.

- The field of Gaussian numbers (which also appears in [Further Number Theory]) is defined to be $\mathbb{Q}(i) = \mathbb{Q}[X]/(X^2+1)$. This is simply $\{a + b\,i \mid a, b \in \mathbb{Q}\}$ and the operations work exactly like in $\mathbb{C}$ except that all coefficients stay rational numbers.
- We can generalise this. Let D be any integer that is not a square so that $X^2 - D$ is irreducible in $\mathbb{Q}[X]$. We will write $\sqrt{D}$ for the generator $X + (X^2 - D)$ in $\mathbb{Q}[X]/(X^2 - D)$ and we will denote this field by $K = \mathbb{Q}(\sqrt{D})$. Then $\sqrt{D}$ is a symbol that satisfies that its square is D. Elements in this field K are written as $a + b\sqrt{D}$ with a and b in $\mathbb{Q}$. Here are some examples of calculations for $D = -7$:

$$(-1 + 3\sqrt{-7}) + (9 - 2\sqrt{-7}) = 8 + \sqrt{-7}$$

$$\begin{aligned}(2+3\sqrt{-7})\cdot(-1-\sqrt{-7}) &= -2-2\sqrt{-7}-3\sqrt{-7}-3\sqrt{-7}^2\\ &= -2-3(-7)-5\sqrt{-7} = 19-5\sqrt{-7}\\ \frac{2+3\sqrt{-7}}{-1-5\sqrt{-7}} &= \frac{(2+3\sqrt{-7})(-1+5\sqrt{-7})}{(-1-5\sqrt{-7})(-1+5\sqrt{-7})}\\ &= \frac{-107+7\sqrt{-7}}{176} = -\frac{107}{176}+\frac{7}{176}\sqrt{-7}\end{aligned}$$

- It should now be clear what the field $\mathbb{Q}(\sqrt[3]{2})$ is. Elements can be written uniquely as $a+b\sqrt[3]{2}+c\sqrt[3]{2}^2$ with $a,b,c\in\mathbb{Q}$. More generally, we want to write $\mathbb{Q}(\sqrt[n]{D})$ for any $n>1$ and any D that is not an n-th power. However, one needs that X^n-D is irreducible. For instance X^4+4 is reducible as it is equal to $(X^2-2X+2)\cdot(X^2+2X+2)$; therefore we shouldn't use the symbol $\sqrt[4]{-4}$.
- However, in most number fields the new root cannot be written using symbols like $\sqrt{\cdot}$. For instance, for $f=X^5-X+1$, we get the degree 5 number field $\mathbb{Q}(\alpha)$ where α satisfies $\alpha^5=-1+\alpha$. The methods in [Galois Theory] will allow to show that α cannot be expressed using only symbols $\pm$, $\cdot$, $\sqrt[n]{\cdot}$. Still we can calculate in $\mathbb{Q}(\alpha)$. Addition is coefficient-by-coefficient, while multiplication is as polynomials but using $\alpha^5=-1+\alpha$:

$$\begin{aligned}(5+4\alpha+3\alpha^2+2\alpha^3+\alpha^4)\cdot(1-\alpha+\alpha^2) &= 5-\alpha+4\alpha^2+3\alpha^3+2\alpha^4+\alpha^5+\alpha^6\\ &= 5-\alpha+4\alpha^2+3\alpha^3+2\alpha^4+(-1+\alpha)+(-\alpha+\alpha^2)\\ &= 4-\alpha+5\alpha^2+3\alpha^3+2\alpha^4\end{aligned}$$

To calculate the inverse of an element like $3+2\alpha+\alpha^4$, one uses the euclidean algorithm to find a Bézout identity in $\mathbb{Q}[X]$, in this case

$$\frac{64X^3+42X^2-52X+253}{1273}\cdot(X^5-X+1)+\frac{-64X^4-42X^3+52X^2-125X+340}{1273}\cdot(X^4+2X+3)=1$$

which, when substituted $X=\alpha$, shows that

$$\frac{1}{3+2\alpha+\alpha^4}=\frac{340-125\alpha+52\alpha^2-42\alpha^3-64\alpha^4}{1273}.$$

◇

Digression

All examples of code in these notes are for SageMath; this is essentially a python library, but for instance "^" is redefined as powering like "**". You can test these and play around with it at https://sagecell.sagemath.org/

```
sage: R.<X> = QQ[]                          # defines X a variable
sage: K.<a> = NumberField(X^5-X+1)          # defines a as a root
sage: (a^4+2*a^3+3*a^2+4*a+5)*(a^2-a+1)     # multiply in K
2*a^4 + 3*a^3 + 5*a^2 - a + 4
sage: 1/(a^4+2*a+3)                         # division in K
-64/1273*a^4 - 42/1273*a^3 + 52/1273*a^2 - 125/1273*a + 340/1273
```

Example. Here a more elaborate example. Define the field of Gaussian numbers to be $k = \mathbb{Q}(i) = \mathbb{Q}[X]/(X^2+1)$; it is a number field of degree 2. Now the polynomial $f = X^2 - 5$ can be viewed as an element of $k[X]$. Since it has no roots in k, it is irreducible. Then the field $K = k[X]/(f)$ is a degree 2 extension of k. Because every element in K can be written as $\alpha + \beta\sqrt{5}$ with $\alpha, \beta \in k$, they can be written as $(a+bi) + (a'+b'i)\sqrt{5}$ with $a, a', b, b' \in \mathbb{Q}$. In other words, it is a $\mathbb{Q}$-vector space of dimension 4 with basis 1, i, $\sqrt{5}$, $i\sqrt{5}$. We can write $K = \mathbb{Q}(i, \sqrt{5})$; it is a number field of degree 4.

Let $\alpha = i + \sqrt{5}$. Then

$$\begin{aligned} & (\alpha - i)^2 = 5 \\ \Rightarrow \quad & \alpha^2 - 2i\alpha - 1 = 5 \\ \Rightarrow \quad & (\alpha^2 - 6)^2 = (2i\alpha)^2 = -4\alpha^2 \\ \Rightarrow \quad & \alpha^4 - 8\alpha^2 + 36 = 0. \end{aligned}$$

The polynomial $X^4 - 8X^2 + 36$ is an irreducible polynomial. The field $\mathbb{Q}[X]/(X^4 - 8X^2 + 36)$ is also a number field of degree 4 and, in fact, we will see that it is isomorphic to K. So $K = \mathbb{Q}(\alpha)$. ◇

In general, for every number field K there is an element α such that $K = \mathbb{Q}(\alpha)$. This is known as the primitive element theorem and it is shown in [Galois Theory]. In practice the method in the above example very often give such an α and its minimal polynomial.

1.2 Algebraic numbers

Definition 1.5. Let K be an extension of $\mathbb{Q}$ and $\alpha \in K$. We say that α is an **algebraic number** if there is a non-zero polynomial $f \in \mathbb{Q}[X]$ such that $f(\alpha) = 0$.

It is crucial here that we ask that the coefficients of f are in $\mathbb{Q}$.

is_alg_number_lem

Lemma 1.6

Let K be a number field and $\alpha \in K$. Then α is an algebraic number.

Proof. By assumption K is a $\mathbb{Q}$-vector space of finite dimension, say d. Then the elements 1, α, $\ldots$, α^d cannot be linearly independent. Hence there exists a linear relation

$$0 = a_0 \cdot 1 + a_1 \cdot \alpha + a_2 \cdot \alpha^2 + \cdots + a_d \cdot \alpha^d$$

with $a_i \in \mathbb{Q}$. This shows that $f(\alpha) = 0$ with $f = a_0 + a_1 X + \cdots + a_d X^d$. □

Examples.

- We have seen the example $i + \sqrt{5}$ which satisfies $X^4 - 8X^2 + 36 = 0$.
- Any element in $\mathbb{Q}(i)$ can be written as $\alpha = a + b\,i$ with $a, b \in \mathbb{Q}$. Then α is a root of $f = X^2 - 2a\,X + a^2 + b^2$.
- $e^{2\pi i/17} \in \mathbb{C}$ is an algebraic number because it is a root of $X^{17} - 1$.
- If you have been to [Further Number Theory], then the 5-adic number $\alpha = 2 + 5 + 2\cdot 5^2 + 5^3 + 3\cdot 5^4 + \cdots$ lifted by Hensel to be a solution to $X^2 + 1 = 0$ is an algebraic number inside $\mathbb{Q}_5$.

◇

field_gen_by_lem

Lemma 1.7

Let K be an extension of $\mathbb{Q}$ and let $0 \neq \alpha \in K$ be an algebraic number satisfying $f(\alpha) = 0$ for some irreducible polynomial $f \in \mathbb{Q}[X]$ of degree d. Then the subset

$$\{x_0 + x_1\alpha + \cdots + x_{d-1}\alpha^{d-1} \mid x_i \in \mathbb{Q}\}$$

is the smallest subfield containing α. It is a number field isomorphic to $\mathbb{Q}[X]/(f)$.

Proof. The evaluation-at-α map $\mathbb{Q}[X] \to K$ defined by sending X to α is a ring homomorphism. Our set in the question is contained in the image of this homomorphism. In fact, the image is equal to this set as any larger power of α can be expressed as an element in the set using $f(\alpha) = 0$.

The kernel of this homomorphism contains the maximal ideal (f) since $f(\alpha) = 0$. Since the map is not sending everything to 0, the kernel is equal to (f) and hence the first isomorphism theorem yields the statement. □

Examples. This now justifies that $\mathbb{Q}(i, \sqrt{5}) \cong \mathbb{Q}[X]/(X^4 - 8X^2 + 36)$ in the above example.

Let $\alpha = 1.111990\cdots + 1.926023\ldots i$ be one of the third roots of 11 in the complex numbers $\mathbb{C}$. The set $\{a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{Q}\} \subset \mathbb{C}$ is a number field isomorphic to $\mathbb{Q}(\sqrt[3]{11}) = \mathbb{Q}[X]/(X^3 - 11)$. ◇

Theorem 1.8

Let α and β be two algebraic numbers in an extension K of $\mathbb{Q}$. Then $\alpha + \beta$ and $\alpha \cdot \beta$ are also algebraic numbers.

Proof. Suppose α is the root of a polynomial $f \in \mathbb{Q}[X]$ of degree n and β is the root of $g \in \mathbb{Q}[X]$ of degree m. Let L be the $\mathbb{Q}$-vector space spanned by the elements $\alpha^i\beta^j$ with $0 \leqslant i < n$ and $0 \leqslant j < m$. This vector space is of dimension $d \leqslant nm$. If we multiply two elements $\gamma, \gamma' \in L$ then the result is still in L since we can use the equation given by $f(\alpha) = 0$ to replace any power of α bigger than n by an expression in only smaller powers of α and similarly for β. Therefore $\gamma \cdot \gamma' \in L$.

Let now γ be an element in L, like $\alpha + \beta$ or $\alpha \cdot \beta$. Then there will be a linear relation among the $d + 1$ elements 1, γ, γ^2, $\ldots$, γ^d. This shows that γ is algebraic. □

Note that this theorem is amazing. Let $\alpha \in \mathbb{C}$ be a root of $X^{123456789} + X^7 - 11$ and let $\beta \in \mathbb{C}$ be a root of $X^{987654321} + X^6 + X^7 + 67$. The theorem says that the there is a polynomial in $\mathbb{Q}[X]$ whose root is $\alpha + \beta$. It would be very hard to spell out the coefficients of this polynomial.

Digression

As a consequence, the set $\bar{\mathbb{Q}}$ of all algebraic numbers contained in $\mathbb{C}$ is a field. This field $\bar{\mathbb{Q}}$ is an example of an algebraically closed field. As a $\mathbb{Q}$-vector space it has infinite dimension, but it is countable as a set. Non-algebraic numbers are called transcendental. It is known that $e = 2.718\ldots$, proved by Hermite in 1873,

and $\pi = 3.141\ldots$, proved in 1882 by von Lindemann, are transcendental. See [1] baker for proofs. It is not known whether $e + \pi$ is algebraic – probably not.

Let K be a number field and let $\alpha \in K$. From Lemma 1.6 is_alg_number_lem, we know that there is a polynomial $f \in \mathbb{Q}[X]$ such that $f(\alpha) = 0$. Choose now $n \leqslant [K : \mathbb{Q}]$ to be the smallest integer such that the elements $1, \alpha, \ldots, \alpha^n$ are no longer linearly independent. We say that α is an **algebraic number of degree** n.

Since we can express α^n as a linear combination of the smaller powers, we find a polynomial $F_\alpha \in \mathbb{Q}[X]$, which is monic of degree n such that $F_\alpha(\alpha) = 0$. By the minimality of n, this is unique.

min_poly_def

Definition 1.9. For an element α in a number field K, the unique monic polynomial $F_\alpha \in \mathbb{Q}[X]$ of minimal degree such that $F_\alpha(\alpha) = 0$ is called the **minimal polynomial** of α.

Examples. The minimal polynomial of $i + \sqrt{5}$ is $X^4 - 8X^2 + 36$. For the number $e^{2\pi i/6} \in \mathbb{C}$, the minimal polynomial is $X^2 - X + 1$. ◇

Let K be a number field and $\alpha \in K$. We denote by $\mathbb{Q}(\alpha)$ the smallest subfield of K containing α as given by Lemma 1.7 field_gen_by_lem. Its degree is equal to the degree of F_α, which is the degree of α. Often we have $\mathbb{Q}(\alpha) = K$, but certainly not for all α.

Digression

```
sage: R.<X> = QQ[]
sage: K.<a> = NumberField(X^4-8*X^2+36)
sage: RK.<Y> = K[]                # ring K[Y]
sage: (Y^2+1).roots()
[(1/12*a^3 - 1/6*a, 1), (-1/12*a^3 + 1/6*a, 1)]
sage: i = _[0][0]; i^2            # is a square root of -1
-1
sage: (1+a).minpoly()             # minimal polynomial
x^4 - 4*x^3 - 2*x^2 + 12*x + 29
sage: sq5 = (a^3-14*a)/12
sage: sq5.minpoly()               # is a square root of 5
x^2 - 5
```

1.3 Cyclotomic fields

yclotomic_subsec

Let p be an odd prime number. Consider the polynomial $f = 1 + X + X^2 + \cdots + X^{p-1}$. We can also write it as $f = (X^p - 1)/(X - 1)$.

Lemma 1.10

The polynomial $f = 1 + X + X^2 + \cdots + X^{p-1}$ is irreducible

Proof. It is enough to show that $g(X) = f(X + 1) = ((X + 1)^p - 1)/X$ is irreducible. Using the binomial coefficients we can write

$$g = \tbinom{p}{1} + \tbinom{p}{2} X + \cdots + \tbinom{p}{p-1} X^{p-2} + X^{p-1}.$$

To this form, we can apply the Eisenstein criterion: The polynomial is monic, all binomials above are divisible by p and the constant term $\binom{p}{1} = p$ is not divisible by p^2. Therefore g and hence f are irreducible. □

Let $K = \mathbb{Q}(\zeta) = \mathbb{Q}[X]/(f)$ with ζ a root of f. From the second version of f, we see that $\zeta^p = 1$, which is why we call $\zeta = \zeta_p$ a **primitive p-th root of unity**. The number field K is an example of a **cyclotomic field**, the name coming from the division of the circle into equal parts. Such fields are studied classically for their relation to the question whether the regular p-gon can be constructed by ruler and compass.

Every element in K can be written uniquely as $x_0+x_1\zeta+\cdots+x_{p-2}\zeta^{p-2}$ and operations are done as usual subject to the rule $\zeta^{p-1} = -1-\zeta-\zeta^2-\cdots-\zeta^{p-2}$. One special feature of this number field is that the polynomial f factors completely in $K[X]$, namely

$$f = (X-\zeta)(X-\zeta^2)\cdots(X-\zeta^{p-1}).$$

Digression

Number fields $K = \mathbb{Q}[X]/(f)$ with the property that f factors completely in $K[X]$ are called normal and the extension $K/\mathbb{Q}$ is called a Galois extension. These are studied extensively in the module [Galois Theory]. Every number field is a subfield of a normal one, obtained by adding successively roots of f until it factors completely. One attaches to a Galois extension a group, called the Galois group, which allows to characterise all subfields of K. In the case of the cyclotomic field above the group is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\times$, which is isomorphic to a cyclic group of order $p-1$.

The cyclotomic field K is isomorphic to a subfield of $\mathbb{C}$ by sending ζ to a chosen p-th root of unity in $\mathbb{C}$, like $e^{2\pi i/p}$, which forces the map to send ζ^k to $e^{2\pi ik/p}$ for all $1 < k < p$.

In general, for any integer $n > 2$, the n-th cyclotomic field is isomorphic to the subfield of $\mathbb{C}$ generated by $e^{2\pi ik/n}$ with k coprime to n. If n is not prime then the polynomial $1+X+\cdots+X^{n-1}$ is not irreducible as $(X^d-1)/(X-1)$ divides $(X^n-1)/(X-1)$ for any proper divisor d of n. The n-th cyclotomic polynomial, denoted Φ_n, is the one irreducible factor of X^n-1 which is coprime to X^d-1 for any proper divisor of d of n. The corresponding field is the n-th cyclotomic field and its generator is written ζ_n. In other words, $X^n-1 = \prod_{d|n}\Phi_d$ with $\Phi_1 = X-1$. For instance,

$$X^9-1 = (X-1)\cdot(X^2+X+1)\cdot(X^6+X^3+1)$$

and the last factor Φ_9 defines the 9-th cyclotomic field $\mathbb{Q}(\zeta_9)$; it is of degree 6.

1.4 Norm and trace

Let K be a number field and $\alpha \in K$. Consider the map

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

which encodes the multiplication by α. For any $a \in \mathbb{Q}$ and $x, y \in K$, we have $m_\alpha(ax+y) = a\cdot m_\alpha(x)+m_\alpha(y)$ which shows that m_α is a $\mathbb{Q}$-linear map. We can choose a basis of K as a $\mathbb{Q}$-vector space and write out the matrix M_α representing this linear map.

Definition 1.11. The **norm** of α is defined to be $\mathrm{N}_K(\alpha) = \det(m_\alpha) = \det(M_\alpha)$. The **trace** of α is defined to be $\mathrm{Tr}_K(\alpha) = \mathrm{tr}(m_\alpha) = \mathrm{tr}(M_\alpha)$.

By the property of the determinant and the trace, the definition does not depend on the chosen basis. If the field K is clear, we abbreviate to N and Tr.

Examples.

- Take the basis 1, $\sqrt{-5}$ in $\mathbb{Q}(\sqrt{-5})$. Consider $\alpha = 1 + \sqrt{-5}$. Then

$$m_\alpha(1) = 1 + \sqrt{-5} \quad \text{and} \quad m_\alpha(\sqrt{-5}) = -5 + \sqrt{-5}.$$

  Therefore the matrix M_α is

$$\begin{pmatrix} 1 & -5 \\ 1 & 1 \end{pmatrix}$$

  which shows that $\mathrm{N}(\alpha) = 1 - (-5) = 6$ and $\mathrm{Tr}(\alpha) = 2$.
- Let $f = X^3 + X^2 - 2X + 8$ and consider $K = \mathbb{Q}(\alpha) = \mathbb{Q}[X]/(f)$. Let us calculate the norm and trace of $\beta = \frac{1}{2}\alpha + \frac{1}{2}\alpha^2$. As a basis for K, we choose 1, α, and α^2. Then

$$\begin{aligned} m_\beta(1) &= \beta = \tfrac{1}{2}\alpha + \tfrac{1}{2}\alpha^2 \\ m_\beta(\alpha) &= \alpha\beta = \tfrac{1}{2}\alpha^2 + \tfrac{1}{2}\alpha^3 = \tfrac{1}{2}\alpha^2 + \tfrac{1}{2}(-8 - 2\alpha - \alpha^2) = -4 + \alpha \\ m_\beta(\alpha^2) &= \alpha \cdot (\alpha\beta) = -4\alpha + \alpha^2 \end{aligned}$$

  which gives the matrix

$$M_\beta = \begin{pmatrix} 0 & -4 & 0 \\ 1/2 & 1 & -4 \\ 1/2 & 0 & 1 \end{pmatrix}.$$

  Therefore $\mathrm{N}(\beta) = 10$ and $\mathrm{Tr}(\beta) = 2$.
- Let $D \neq 0$ and $D \neq 1$ be an integer that is not a third power. Let $f = X^3 - D$ and write $\sqrt[3]{D}$ for its solution in $K = \mathbb{Q}[X]/(f)$. A general element in K is written in the basis 1, $\sqrt[3]{D}$, $\sqrt[3]{D}^2$ as $\alpha = a + b\sqrt[3]{D} + c\sqrt[3]{D}^2$ for rationals a, b, c. The matrix for m_α in this basis is

$$M_\alpha = \begin{pmatrix} a & cD & bD \\ b & a & cD \\ c & b & a \end{pmatrix}$$

  and so $\mathrm{Tr}(\alpha) = 3a$ and $\mathrm{N}(\alpha) = a^3 + b^3D + c^3D^2 - 3abcD$.

◇

norm_mult_lem

Lemma 1.12

The norm map $\mathrm{N}\colon K \to \mathbb{Q}$ and the trace map $\mathrm{Tr}\colon K \to \mathbb{Q}$ satisfy

$$\mathrm{N}(\alpha \cdot \beta) = \mathrm{N}(\alpha) \cdot \mathrm{N}(\beta) \qquad \text{and} \qquad \mathrm{Tr}(\alpha + \beta) = \mathrm{Tr}(\alpha) + \mathrm{Tr}(\beta)$$

for all $\alpha, \beta \in K$.

Proof. The first follows from $m_{\alpha\cdot\beta} = m_\alpha \circ m_\beta$ once the determinant is applied. Similarly, the second follows from applying the trace to $m_{\alpha+\beta} = m_\alpha + m_\beta$. □

char_poly_lem

Lemma 1.13

Let K be a number field of degree d and let $\alpha \in K$ and write $n = [K : \mathbb{Q}(\alpha)]$. Set

$$\chi_\alpha(X) = \det(XI - M_\alpha) \ \in \mathbb{Q}[X]$$

where M_α is the matrix of m_α with respect to any $\mathbb{Q}$-basis of K. Then

$$F_\alpha^n = \chi_\alpha = X^d - \mathrm{Tr}_K(\alpha)\, X^{d-1} + \cdots + (-1)^d\, \mathrm{N}_K(\alpha).$$

Proof. Assume first that $n = 1$, that is $K = \mathbb{Q}(\alpha)$ and d is the degree of α. Up to sign, $\chi_\alpha = \det(X\,I - M_\alpha)$ is the characteristic polynomial of m_α. By the Cayley-Hamilton theorem, $\chi_\alpha(m_\alpha) = 0$ as a $\mathbb{Q}$-linear map $K \to K$. However $\chi_\alpha(m_\alpha)(x) = \chi_\alpha(\alpha) \cdot x$ for all $x \in K$. Therefore $\chi_\alpha(\alpha) = 0$.

Since F_α is the minimal polynomial, this implies that F_α divides χ_α in $\mathbb{Q}[X]$. But they are of the same degree and both monic, therefore $F_\alpha = \chi_\alpha$.

Now if $n > 1$, write m for the degree of α. We may pick a basis $\beta_1, \ldots, \beta_n$ of K as a $\mathbb{Q}(\alpha)$-vector space. Every element of K can be written as $\sum_{i=1}^n \gamma_i\, \beta_i$ with $\gamma_i \in \mathbb{Q}(\alpha)$ and then we can express γ_i as a sum $\sum_{j=0}^{m-1} x_{i,j}\alpha^j$ with rationals $x_{i,j}$. Therefore the elements $\beta_1, \beta_1\alpha, \ldots, \beta_1\alpha^{d-1}, \beta_2, \ldots, \beta_n\alpha^{d-1}$ form a basis for K as a vector space over $\mathbb{Q}$.

The matrix for m_α in this basis is formed of n blocks along the diagonal of identical matrices C which describe m_α on $\mathbb{Q}(\alpha)$.

$$M_\alpha = \begin{pmatrix} C & & & \\ & C & & \\ & & C & \\ & & & \ddots \\ & & & & C \end{pmatrix}$$

Therefore $\chi_\alpha = \det(X\,I - C)^n = \det(XI - m_\alpha|_{\mathbb{Q}(\alpha)})^n$. Then $F_\alpha^n = \chi_\alpha$ follows from the case $n = 1$.

Finally, the constant term of χ_α is $\chi_\alpha(0) = \det(-M_\alpha) = (-1)^d\,\mathrm{N}(\alpha)$. It is well known from linear algebra that the coefficient of X^{d-1} in the characteristic polynomial is $-\mathrm{Tr}(M_\alpha)$. □

Examples.

- Consider $\alpha = 1+\sqrt{-5}$ in $\mathbb{Q}(\sqrt{-5})$ again. Since $\alpha^2 = 4+2\sqrt{-5} = -4+2(\alpha-1) = 2\alpha-6$ the minimal polynomial of α is $X^2 - 2X + 6$. Therefore the lemma confirms that $\mathrm{Tr}(\alpha) = 2$ and $\mathrm{N}(\alpha) = 6$.
- Since the minimal polynomial of the p-th root of unity $\zeta = \zeta_p$ is $1 + X + \cdots + X^{p-1}$ for any odd prime p, we find that $\mathrm{Tr}(\zeta) = -1$ and $\mathrm{N}(\zeta) = (-1)^{p-1} \cdot 1 = 1$. This would be much more tedious to calculate with the original definition.
- More generally, let $0 \leqslant i < j < p$ and consider $\alpha = \zeta^i - \zeta^j$ in the cyclotomic field $\mathbb{Q}(\zeta)$. Use Lemma 1.12 (norm_mult_lem) to get $\mathrm{N}(\alpha) = \mathrm{N}(\zeta)^i \cdot \mathrm{N}(1-\zeta^{j-i}) = \mathrm{N}(1-\zeta^k)$ with $0 < k < p$. Note that $\mathrm{N}(1-\zeta^k) = \det(I - M_{\zeta^k})$ is the evaluation of the minimal polynomial of ζ^k at 1. But the minimal polynomial of ζ^k is the same as ζ and it is equal to $1 + X + \cdots + X^{p-1}$. Therefore $\mathrm{N}(\zeta^i - \zeta^j) = 1 + 1 + \cdots + 1 = p$.
- We can use the lemma also to calculate the minimal polynomial of $\alpha = a + b\sqrt[3]{D} + c\sqrt[3]{D}^2$ in $\mathbb{Q}(\sqrt[3]{D})$ by calculating the characteristic polynomial of the matrix M_α on

the previous page. It is

$$X^3 - 3a\,X^2 + 3(a^2 - bc)\,X - (a^3 + b^3D + c^3D^2 - 3abcD).$$

◇

trace_nondeg_lem

Lemma 1.14

Let K be a number field.

(i) $\mathrm{N}(\alpha) = 0$ if and only if $\alpha = 0$.

(ii) For any $\alpha \neq 0$, the linear map $\mu_\alpha \colon K \to \mathbb{Q}$ sending β to $\mathrm{Tr}(\alpha \cdot \beta)$ is not the zero map.

(iii) If $\alpha_1, \ldots, \alpha_d$ is a $\mathbb{Q}$-basis of K. Then the rational matrix $T = \big(\mathrm{Tr}(\alpha_i\alpha_j)\big)_{i,j}$ is invertible

As a consequence of the first part the map $\mathrm{N} \colon K^\times \to \mathbb{Q}^\times$ is a group homomorphism.

Proof. (i) We have the following equivalences: $\mathrm{N}(\alpha) = 0 \iff \det(m_\alpha) = 0 \iff \ker(m_\alpha) \neq \{0\} \iff$ there exists $\beta \neq 0$ in K such that $\alpha\beta = 0$. But the last statement is the same as to ask that $\alpha = 0$.

(ii) First for all $\beta, \gamma \in K$ and $a \in \mathbb{Q}$, we have

$$\begin{aligned}\mu_\alpha(a \cdot \beta + \gamma) = \mathrm{Tr}\big((a \cdot \beta + \gamma)\alpha\big) &= \mathrm{Tr}(a \cdot \beta\alpha + \gamma\alpha) \\ &= a \cdot \mathrm{Tr}(\beta\alpha) + \mathrm{Tr}(\gamma\alpha) = a \cdot \mu_\alpha(\beta) + \mu_\alpha(\gamma)\end{aligned}$$

and this shows that μ_α is linear. For $\alpha \neq 0$ it is non-trivial because $\mu_\alpha(1/\alpha) = \mathrm{Tr}(1/\alpha \cdot \alpha) = \mathrm{Tr}(1) = [K : \mathbb{Q}] \neq 0$.

(iii) Suppose $(x_1, \ldots, x_d) \in \mathbb{Q}^d$ is in the kernel of T. But that means that for all j, the sum $\sum_{i=1}^d \mathrm{Tr}(\alpha_i\alpha_j)x_i$ is zero. This sum equals $\mathrm{Tr}(\beta\alpha_j)$ for $\beta = \sum_i x_i\alpha_i \in K$. But then $\mathrm{Tr}(\beta\alpha) = 0$ for all $\alpha \in K$ as the α_j form a basis. By the second point we then have $\beta = 0$ which shows that the kernel of T is trivial. □

Examples.

- For the field $K = \mathbb{Q}(\sqrt{-5})$ with basis 1, $\sqrt{-5}$, the matrix T is equal to

$$T = \begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\sqrt{-5}) \\ \mathrm{Tr}(\sqrt{-5}) & \mathrm{Tr}(-5) \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & -10 \end{pmatrix}.$$

- For the fifth cyclotomic field with the basis 1, ζ, ζ^2, ζ^3 the matrix is

$$T = \begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\zeta) & \mathrm{Tr}(\zeta^2) & \mathrm{Tr}(\zeta^3) \\ \mathrm{Tr}(\zeta) & \mathrm{Tr}(\zeta^2) & \mathrm{Tr}(\zeta^3) & \mathrm{Tr}(\zeta^4) \\ \mathrm{Tr}(\zeta^2) & \mathrm{Tr}(\zeta^3) & \mathrm{Tr}(\zeta^4) & \mathrm{Tr}(1) \\ \mathrm{Tr}(\zeta^3) & \mathrm{Tr}(\zeta^4) & \mathrm{Tr}(1) & \mathrm{Tr}(\zeta) \end{pmatrix} = \begin{pmatrix} 4 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & 4 \\ -1 & -1 & 4 & -1 \end{pmatrix}.$$

◇

Digression

The second statement is equivalent to asking that the extension $K/\mathbb{Q}$ is separable in the language of [Galois Theory].

2 The ring of integers

Let K be a number field. This is the analogue of the field $\mathbb{Q}$. In this section, we will find the analogue of the ring $\mathbb{Z}$ in which we do number theory. Historically, this took a while. For instance $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ is a good ring, but instead $\mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}$ turns out to lack the good properties needed for number theory.

2.1 Finitely generated abelian groups

We first recall some results from the theory of abelian groups as studied in more detail in the module [Group Theory]. We will write all our abelian groups here additively.

Definition 2.1. A **finitely generated abelian group**, or a **figab**[a] **group** for short, is an abelian group $(A, +)$ such that there exists a finite set $\{a_1, a_2, \ldots, a_n\} \subset A$ with the property that every element a in A can be written as

$$a = x_1\, a_1 + x_2\, a_2 + \cdots + x_n\, a_n$$

with $x_1, \ldots, x_n \in \mathbb{Z}$. If furthermore, this representation is unique we say that A is a **free** figab group.

[a] This is my neologism, you won't find it in any book or module. Unfortunately.

By definition, for a free finitely generated abelian group A there exists an isomorphism $A \cong \mathbb{Z}^n$ sending $a \in A$ to the vector $(x_1, \ldots, x_n)$ coming from the unique representation. The integer n is then called the **rank** of A and the set $\{a_1, \ldots, a_n\}$ a **$\mathbb{Z}$-basis** of A.

Lemma 2.2

sub_figab_lem

Let B be a subgroup of a figab group A. Then B is also figab.

Proof. We prove this by induction on the number of generators $\{a_1, \ldots, a_n\}$ of A.

If $n = 1$, then A is a cyclic group. It is well known that any subgroup of a cyclic group is also cyclic.

By induction, we assume the lemma true for any group A generated by $n - 1$ or less elements. Let A' be the subgroup generated by $\{a_1, \ldots, a_{n-1}\}$. By the induction hypothesis, the subgroup $B \cap A'$ is generated by finitely many elements $\{b_1, \ldots, b_i\}$. Consider the quotient homomorphism $\pi\colon A \to A/A'$. Note that the quotient group is generated by $\pi(a_n)$ and hence it is cyclic. Therefore $\pi(B) = B/(B \cap A')$ is cyclic as well. Let us pick an element b_{i+1} in B such that $\pi(b_{i+1})$ generates $\pi(B)$.

We claim that B is generated by $\{b_1, \ldots, b_i, b_{i+1}\}$. Let b be an element in B. Then $\pi(b) = x_{i+1}\, \pi(b_{i+1})$ for some integer x_{i+1} because $\pi(B)$ is cyclic generated by $\pi(b_{i+1})$. Therefore $b' = b - x_{i+1}\, b_{i+1}$ belongs to $B \cap A'$ and as such it can be written as $x_1 b_1 + \cdots + x_i b_i$ for integers $x_1, \ldots, x_i$. Hence $b = x_1\, b_i + \cdots + x_i b_i + x_{i+1} b_{i+1}$ shows that B is finitely generated. □

free_figab_lem

Lemma 2.3

Let B be a subgroup of a free figab group A. Then B is also free of rank smaller or equal to the rank of A.

Proof. Follow the same proof by induction as for the previous lemma. The induction hypothesis is now that $B \cap A'$ is free on the set $\{b_1, \ldots, b_i\}$ with $i \leqslant n-1$. Note there is no choice about the integer x_{i+1} once b_{i+1} is chosen. The induction hypothesis shows that $x_1, \ldots, x_i$ are also uniquely determined and $i+1 \leqslant n$ proves the rank part. □

coker_det_lem

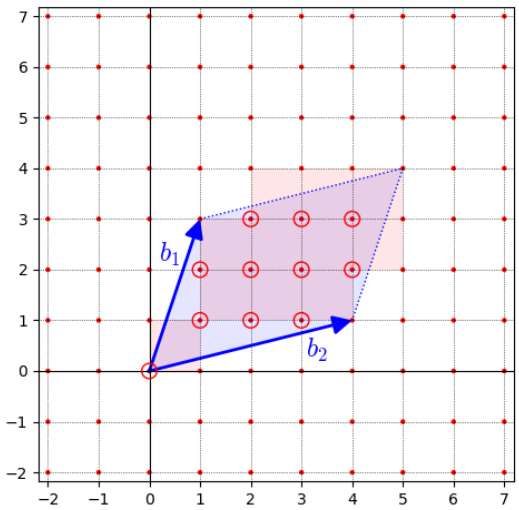
Lemma 2.4

Let $b_1, \ldots, b_n$ be elements in a free rank n figab group with $\mathbb{Z}$-basis $\{a_1, \ldots, a_n\}$. Write $b_j = x_{1,j}\, a_1 + x_{2,j}\, a_2 + \cdots + x_{n,j}\, a_n$ with $x_{i,j} \in \mathbb{Z}$ and set $B = \mathbb{Z}b_1 + \cdots + \mathbb{Z}b_n \leqslant A$. If $\det(x_{i,j}) \neq 0$, then the rank of B is also n and the quotient group A/B is finite of order $|\det(x_{i,j})|$. Otherwise B is of rank smaller than n

Proof. We may suppose that $A = \mathbb{Z}^n$ so that $b_j = (x_{1,j}, \ldots, x_{n,j})$. The set

$$F = \left\{ t_1\, b_1 + \cdots + t_n\, b_n \in \mathbb{R}^n \;\middle|\; 0 \leqslant t_j < 1 \text{ for all } j \right\} \subset \mathbb{R}^n$$

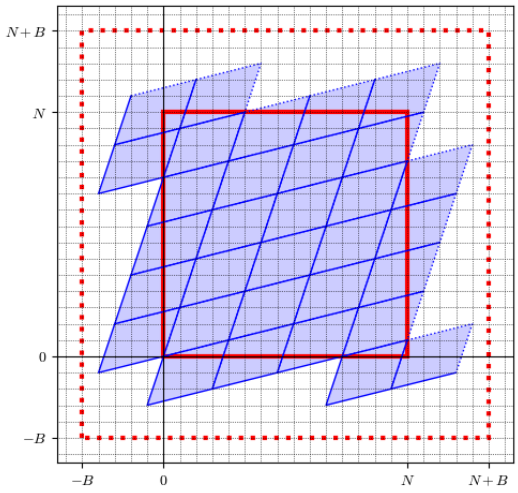
is called a fundamental domain of B. It is a parallelepiped but only with half the side faces included. The volume of F is $|\det(x_{i,j})|$. If this determinant is 0, the vectors are $\mathbb{Q}$-linearly dependent, which after scaling gives a $\mathbb{Z}$-linear relation; therefore the rank must be smaller than n. Assume now $\det(x_{i,j}) \neq 0$.



We claim that the integral points in F (the circled ones in the picture) represent each coset of B exactly once. To see this, take a coset $u + B$ and write u in the $\mathbb{Q}$-basis b_1, $\ldots$, b_n, say $u = \sum_{i=1}^n y_i b_i$ with $y_i \in \mathbb{Q}$. Set $z_i = \lfloor y_i \rfloor \in \mathbb{Z}$ and $t_i = y_i - z_i \in [0, 1)$ for each i. Then $u + B = t + B$ with $t = \sum_i t_i b_i \in F$ since $\sum_i z_i b_i \in B$. This shows every coset has a representative in F. If it had two, then their difference would be a sum $\sum_i s_i b_i \in B$ with $-1 < s_i < 1$, which implies that $s_i = 0$ for all i. This proves the claim and we conclude that the set $\mathbb{Z}^n \cap F$ is a set of representatives of the coset $\mathbb{Z}^n/B$.

It is already clear now that $\mathbb{Z}^n/B$ is finite. It remains to show that $L = \#(\mathbb{Z}^n \cap F)$ is equal to the volume of F. In the above picture, it is not hard to see this by rearranging the bits of the red squares not covered by the blue parallelogram. In general case, this would work, too, but it is not easy to write down. We argue differently here.

There is an integer $B > 0$ such that F is completely contained in the box $[0, B]^n$. Let N be a large integer.



Cover the box $[0, N]^n$ with translates of F by elements in B as illustrated above. Say this needs K copies of F. This means that it covers $K \cdot \mathrm{Vol}(F)$ area and $K \cdot L$ integral points. We have

$$N^n \leqslant K \cdot \mathrm{Vol}(F) \leqslant (N + 2B)^n$$
$$N^n \leqslant K \cdot L \leqslant (N + 2B)^n$$

where the upper bound comes from the fact that the union of all the translated copies of F is contained in the box $[-B, N + B]^n$. This gives

$$\Big(1 + \frac{2B}{N}\Big)^{-n} = \frac{N^n}{(N + 2B)^n} \leqslant \frac{\mathrm{Vol}(F)}{L} \leqslant \frac{(N + 2B)^n}{N^n} = \Big(1 + \frac{2B}{N}\Big)^n.$$

When taking the limit as $N \to \infty$, we can conclude that $L = \mathrm{Vol}(F)$. □

A preferable alternative proof uses the Smith normal form, which we have avoided here.

zbasis_change_cor

Corollary 2.5

The set $\{b_1, \ldots, b_n\}$ is a $\mathbb{Z}$-basis of A if and only if $\det(x_{i,j}) = \pm 1$.

The set of integral matrices with determinant equal to ± 1 is the group $\mathrm{GL}_n(\mathbb{Z})$. They are the allowed changes of $\mathbb{Z}$-bases.

2.2 Algebraic integers

min_poly_def

Recall from Definition 1.9 that each $\alpha \in K$ has a minimal polynomial F_α, which is a monic polynomial with rational coefficients.

Definition 2.6. An element α of a number field K is called an **algebraic integer** if there is a non-zero monic polynomial $f \in \mathbb{Z}[X]$ such that $f(\alpha) = 0$.

Examples.

- The element $\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ is an algebraic integer, since it is a solution to $X^2 - 2 = 0$.
- For any odd prime the primitive p-th root of unity ζ_p from Section 1.3 is an algebraic integer as it satisfies $X^p - 1 = 0$.
- The element $\frac{1}{2} + \frac{1}{2}\sqrt{-3}$ in $\mathbb{Q}(\sqrt{-3})$ is an algebraic integer since it satisfies $X^2 - X + 1 = 0$.
- Any good old integer $a \in \mathbb{Z}$ is an algebraic integer as it is a solution to $X - a = 0$.
- Instead, the rational number $\frac{1}{2}$ is not an algebraic integer: When evaluated on a monic polynomial with integer coefficients, we obtain an expression like $(\frac{1}{2})^n + a_{n-1}(\frac{1}{2})^{n-1} + \cdots + a_0$ which can be shown to be a rational number with denominator 2^n and odd numerator. This is never zero.

◇

int_min_poly_prop

Proposition 2.7

Let α be an element in a number field K with minimal polynomial F_α. Then α is an algebraic integer if and only if F_α has integer coefficients.

Proof. The direction $\Leftarrow$ is obvious.

Assume now that there is some non-zero monic polynomial $f \in \mathbb{Z}[X]$ with $f(\alpha) = 0$. Since $\mathbb{Q}[X]$ is a unique factorisation domain, there is a $h \in \mathbb{Q}[X]$ such that $f = F_\alpha \cdot h$. If F_α were not in $\mathbb{Z}[X]$ there is a prime p dividing the denominator of at least one of its coefficients. Let $u > 0$ be the smallest natural number such that p does not divide any denominator of $p^u F_\alpha$ anymore. Similarly, let $v \geqslant 0$ be the minimal integer such that p does not divide any denominators of $p^v h$. Since $f \in \mathbb{Z}[X]$ and $u + v > 0$, the polynomial $p^{u+v} f$ reduces to the zero polynomial in $\mathbb{F}_p[X]$. However, it is equal to the product of $p^u F_\alpha$ and $p^v h$ which both reduce to non-zero polynomials. This is a contradiction with $\mathbb{F}_p[X]$ being an integral domain. □

int_norm_cor

Corollary 2.8

If α is an algebraic integer in the number field K, then $\mathrm{N}_K(\alpha)$ and $\mathrm{Tr}_K(\alpha)$ are integers.

Proof. By Proposition 2.7, the minimal polynomial F_α has integer coefficients. By Lemma 1.13, the trace and the norm of α are two coefficients of a power of F_α. □

The converse of this corollary is not true in general; just take a root of $X^3 + X^2 + \frac{1}{7}X + 1$. It is not an algebraic integer, but has integral norm and trace.

We will now aim for yet another way of characterising that an algebraic number is an algebraic integer. It is analogous to that algebraic numbers are characterised by the fact that the field they generate is finite dimensional over $\mathbb{Q}$.

If α is an element of a number field K, we define

$$\mathbb{Z}[\alpha] = \Big\{ P(\alpha) \;\Big|\; P \in \mathbb{Z}[X] \Big\};$$

this is the abelian group generated by $\{\alpha^j \mid j \in \mathbb{Z}\}$. But it is also a ring as it is the image of the evaluation-at-α map $\mathbb{Z}[X] \to K$.

Examples.

- If $a \in \mathbb{Z}$ then $\mathbb{Z}[a] = \mathbb{Z}$.
- The ring $\mathbb{Z}[\frac{1}{5}] \subset \mathbb{Q}$ is the set of all rational numbers whose denominator is a power of 5. Note this is not a figab group because any finite list of element like $\{a_1/5^{n_1}, a_2/5^{n_2}, \ldots, a_i/5^{n_i}\}$ generates a group contained in the set of rational numbers with denominator dividing $5^{\max\{n_1,\ldots,n_i\}}$.
- For $\alpha = i$ one finds the ring of Gaussian integer $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$. This is a free abelian group of rank 2 generated by 1 and i.
- Similarly, the ring $\mathbb{Z}[\zeta_p]$ is generated by 1, ζ_p, ζ_p^2, $\ldots$, ζ_p^{p-1} as an abelian group. Since $1 + \zeta_p + \cdots + \zeta_p^{p-1} = 0$, it is also generated by any $p-1$ of them; in fact, it is a free group of rank $p-1$.

$\diamond$

int_figab_prop

Proposition 2.9

Let α be an element in a number field K. Then α is an algebraic integer if and only if $\mathbb{Z}[\alpha]$ is a figab group.

Proof. $\Rightarrow$: Let d be the degree of the minimal polynomial F_α which we know to be in $\mathbb{Z}[X]$ by Proposition 2.7. Since $F_\alpha(\alpha) = 0$, we can express α^d as a $\mathbb{Z}$-linear combination of smaller powers of α. Similar for α^{d+1} and all higher powers. Therefore $\{1, \alpha, \ldots, \alpha^{d-1}\}$ generates $\mathbb{Z}[\alpha]$ as an abelian group.

$\Leftarrow$: Let $\{\alpha_1, \alpha_2, \ldots, \alpha_r\}$ be a set that generates $\mathbb{Z}[\alpha]$ as an abelian group. For each i, there is a polynomial $P_i \in \mathbb{Z}[X]$ such that $\alpha_i = P_i(\alpha)$. Pick an integer N greater than $\deg(P_i)$ for all i. Then $\alpha^N = x_1\alpha_1 + \cdots + x_r\alpha_r$ for some integers $x_i \in \mathbb{Z}$. Set $f = X^N - x_1 P_1(X) - \cdots - x_r P_r(X)$ which is a monic polynomial in $\mathbb{Z}[X]$. Further more $f(\alpha) = \alpha^N - x_1 P_1(\alpha) - \cdots - x_r P_r(\alpha) = 0$. By definition this means that α is an algebraic integer. $\square$

Theorem 2.10

Let K be a number field. The set of all algebraic integers in K is a subring of K.

Proof. Since $\mathbb{Z} \subset K$, certainly the set is non-empty. Let α and β be two algebraic integers. By Proposition 2.9, the abelian groups $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ are finitely generated, say generated by $\{1, \alpha, \ldots, \alpha^n\}$ and $\{1, \beta, \ldots, \beta^m\}$ respectively. The rings $\mathbb{Z}[\alpha\beta]$ and $\mathbb{Z}[\alpha + \beta]$ are contained in the abelian group generated by $\{\alpha^i\beta^j \mid 0 \leqslant i \leqslant n,\ 0 \leqslant j \leqslant m\}$. By Lemma 2.2, these two rings are therefore also figab groups. By Proposition 2.9 again, $\alpha\beta$ and $\alpha + \beta$ are also algebraic integers. This shows that the set of all algebraic integers in K is closed under addition and multiplication, which means that it is a subring. $\square$

Definition 2.11. The set of algebraic integers in a number field K is called its **ring of integers** and denoted by $\mathcal{O}_K$ or simply $\mathcal{O}$ if K is understood.

You will find that it is sometimes also called the maximal order of K. An order in K is a subring that is a figab group and that contains a basis of K as a vector space. One can show that any order is a subring of $\mathcal{O}_K$.

Corollary 2.12

full_lattice_cor

(i) For any number field K, we have $\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$. In particular, the algebraic integers within $\mathbb{Q}$ are exactly the usual integer $\mathbb{Z}$.

(ii) For any number field K, we have $\mathbb{Q} \cdot \mathcal{O}_K = K$. This means that for any α in K there is an integer n such that $n\alpha \in \mathcal{O}_K$.

Proof. (i) The minimal polynomial of a rational number a is $X - a$ and that is in $\mathbb{Z}[X]$ only if $a \in \mathbb{Z}$.

(ii) Let n be the least common denominator of the coefficients of the minimal polynomial F_α of α. Set $g(X) = n^{\deg(F_\alpha)} F_\alpha(X/n)$. This is a monic polynomial and its coefficients are integers. Since $n\alpha$ is a root of g, it follows that $n\alpha \in \mathcal{O}_K$. □

2.3 Quadratic fields

quadratic_subsec

Definition 2.13. A **quadratic field** is a number field of degree 2.

Lemma 2.14

Any quadratic field is of the form $\mathbb{Q}(\sqrt{D})$ for some non-zero squarefree integer $D \neq 1$.

Proof. Pick an $\alpha \in \mathcal{O}_K$ in the quadratic field K which is not in $\mathbb{Z}$. It must satisfy a quadratic polynomial $X^2 + aX + b = 0$ with $a, b \in \mathbb{Z}$. By the formula for the quadratic equation, we have $\alpha = \frac{1}{2}(-a \pm \sqrt{a^2 - 4b})$. Note $a^2 - 4b \neq 0$ as $\alpha \notin \mathbb{Q}$. Write $a^2 - 4b = A^2 \cdot D$ with D squarefree and $A \in \mathbb{N}$. Since $\sqrt{D} = (2\alpha + a)/A$ is in K, it turns out that $K \supset \mathbb{Q}(\sqrt{D})$. As they are both $\mathbb{Q}$-vector spaces of dimension 2, they must be equal. □

Example. We wish to determine the ring of integers of $\mathbb{Q}(\sqrt{-3})$. Let $\alpha = a + b\sqrt{-3}$ for rational numbers a and b. Then $\alpha^2 = a^2 + 3b^2 + 2ab\sqrt{-3}$. This shows that α satisfies the polynomial equation

$$X^2 - 2a\,X + a^2 + 3b^2 = 0$$

This is the minimal polynomial of α.

int_min_poly_prop

By Proposition 2.7, $\alpha \in \mathcal{O}_K$ if and only if $-2a$ and $a^2 + 3b^2$ are integers.

The first condition implies that $a = \frac{n}{2}$ for an integer n. If $n^2/4 + 3b^2$ is an integer, then the denominator of b cannot be any larger than 2. Therefore there is an integer m such that $b = \frac{m}{2}$. While the first condition is now satisfied the second condition says that $n^2 + 3m^2 \in 4\mathbb{Z}$. It is easy to see that this means either than both n and m are even or that they are both odd. Therefore there is an integer k such that $n = 2k + m$. We found that all algebraic integers are of the form

$$\frac{2k+m}{2} + \frac{m}{2}\sqrt{-3} = k + m\frac{1+\sqrt{-3}}{2}$$

for integers k and m. This means that $\mathcal{O}_K$ is contained in $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$. Conversely, for all k and m integers, we do obtain algebraic integers as $\frac{1}{2}(1+\sqrt{-3})$ is in $\mathcal{O}_K$. Therefore

$$\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right].$$

◇

It may be a good idea to do a few more concrete examples before passing on to the next theorem.

Theorem 2.15

Let $D \neq 1$ be a non-zero squarefree integer. If $D \equiv 1 \pmod 4$, then the ring of integers $\mathcal{O}_K$ of the quadratic field $K = \mathbb{Q}(\sqrt{D})$ is equal to

$$\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right].$$

In all other cases, we have $\mathcal{O}_K = \mathbb{Z}\left[\sqrt{D}\right]$.

Proof. As D is squarefree, we have $D \not\equiv 0 \pmod 4$.

Let $\alpha = a + b\sqrt{D}$ with rationals a and b. The minimal polynomial is

$$F_\alpha = X^2 - 2a\,X + a^2 - b^2 D.$$

To ask that $\alpha \in \mathcal{O}_K$ is to ask that $2a$ and $a^2 - b^2 D$ are both integers. If so, there is an integer n such that $a = n/2$ and an integer m such that $b = m/2$. Then α is an algebraic integer if $n^2 - m^2 D \equiv 0 \pmod 4$.

First, we assume that $D \equiv 2$ or 3 modulo 4. In this case, the congruence forces both n and m to be even. It follows that α lies in $\mathbb{Z}\left[\sqrt{D}\right]$. This proves $\subset$ inclusion in the statement, the $\supset$ follows from the fact that $\sqrt{D}$ is an algebraic integer.

Now to the case when $D \equiv 1 \pmod 4$. Then the congruence gives two options, either both n and m are even or they are both odd. We get an integer k such that $n = 2k+m$. Now α is $k + m(1+\sqrt{D})/2$. This shows that $\mathcal{O}_K$ is contained in $\mathbb{Z}\left[(1+\sqrt{D})/2\right]$. Conversely, the element $(1+\sqrt{D})/2$ has minimal polynomial $X^2 - X + (1-D)/4$. Since $D \equiv 1 \pmod 4$, this polynomial has integer coefficients, showing the reverse inclusion. □

2.4 Some properties of the ring of integers

The first property is crucial and tells is that the additive structure of $\mathcal{O}_K$ is just isomorphic to $\mathbb{Z}^{[K:\mathbb{Q}]}$; but again the multiplicative structure is harder. This theorem is, however, not so easy to prove.

Theorem 2.16

fin_gen_thm

Let K be a number field of degree d. Then the ring of integers $\mathcal{O}_K$ is a free figab group of rank d.

Proof. Pick a $\mathbb{Q}$-basis $\alpha_1, \ldots, \alpha_d$ of K. By Corollary full_lattice_cor 2.12, there is an integer n such that $n\alpha_i \in \mathcal{O}$. Therefore, by replacing the basis by these multiples, we may assume $\alpha_i \in \mathcal{O}$ for all i.

Define $A = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \cdots + \mathbb{Z}\alpha_d$, which is a free figab group inside $\mathcal{O}$. We aim to show the opposite, namely that $\mathcal{O}$ is included in a free figab group; we will use the integrality property of the trace map to construct this group. Set

$$\delta(A) = \left\{ x \in K \;\middle|\; \operatorname{Tr}(x\alpha) \in \mathbb{Z} \text{ for all } \alpha \in A \right\}$$

By Corollary int_norm_cor 2.8, we have $\mathcal{O} \subset \delta(A)$. First, we can restate the condition by using our basis elements α_i, then we use the same basis to write $x \in K$ as $x_1\alpha_1 + \cdots x_d\alpha_d$ with $x_i \in \mathbb{Q}$:

$$\begin{aligned}
\delta(A) &= \left\{ x \in K \;\middle|\; \operatorname{Tr}(x\alpha_i) \in \mathbb{Z} \text{ for all } 1 \leqslant i \leqslant d \right\} \\
&= \left\{ \sum_{j=1}^{d} x_j\alpha_j \in K \;\middle|\; \sum_{j=1}^{d} x_j \operatorname{Tr}(\alpha_i\alpha_j) \in \mathbb{Z} \text{ for all } 1 \leqslant i \leqslant d \right\} \\
&= \left\{ \sum_{j=1}^{d} x_j\alpha_j \in K \;\middle|\; T\,(x_1, \ldots, x_d)^\intercal \in \mathbb{Z}^d \right\} \\
&= \left\{ \sum_{j=1}^{d} x_j\alpha_j \in K \;\middle|\; (x_1, \ldots, x_d)^\intercal \in T^{-1}\,\mathbb{Z}^d \right\}
\end{aligned}$$

where $T = \left(\operatorname{Tr}(\alpha_i\alpha_j)\right)_{i,j}$ is the invertible matrix that appeared in Lemma trace_nondeg_lem 1.14.

The vectors in $T^{-1}\mathbb{Z}^d$ are $\mathbb{Z}$-linear combination of the columns of T^{-1} as they are T^{-1} multiplied with the standard basis vectors in $\mathbb{Z}^d$. If $(t_{1,j}, t_{2,j}, \ldots, t_{d,j})^\intercal$ is the j-th column of T^{-1} with $t_{ij} \in \mathbb{Q}$, then the algebraic numbers $\tau_j = t_{1,j}\alpha_1 + \cdots + t_{d,j}\alpha_d$ generate $\delta(A)$. Therefore $\delta(A) = \mathbb{Z}\tau_1 + \ldots + \mathbb{Z}\tau_d$ is a free figab group. Since $\mathcal{O} \subset \delta(A)$, the same is true for $\mathcal{O}$ by Lemma free_figab_lem 2.3. □

Instead of $\delta(A)$, one can also show that $\mathcal{O} \subset \frac{1}{\det(T)}A$, since T^{-1} is equal to the product of $(\det T)^{-1}$ and an integer matrix. Since T is the matrix expressing the $\mathbb{Z}$-basis elements α_i in terms of the $\mathbb{Z}$-basis of $\delta(A)$, the size of $\#\delta(A)/A$ is equal $|\det(T)|$, which is called the discriminant of A.

Example. We go through the proof of the theorem with the example $\mathbb{Q}(\sqrt{-3})$ taking the initial $\mathbb{Q}$-basis to be $\{1, \sqrt{-3}\}$. Recall that the trace of $a + b\sqrt{-3}$ is $2a$. The trace of $(a + b\sqrt{-3}) \cdot \sqrt{-3}$ is $2 \cdot (-3b)$. We find

$$\delta(A) = \left\{ a + b\sqrt{-3} \;\middle|\; a, b \in \mathbb{Q} \text{ such that } 2a \in \mathbb{Z} \text{ and } -6b \in \mathbb{Z} \right\}$$

This is really a free abelian group generated by $\frac{1}{2}$ and $\frac{1}{6}\sqrt{-3}$. The matrix T is equal to

$$T = \begin{pmatrix} \operatorname{Tr}(1) & \operatorname{Tr}(\sqrt{-3}) \\ \operatorname{Tr}(\sqrt{-3}) & \operatorname{Tr}(-3) \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & -6 \end{pmatrix}$$

whose determinant is -12. The inverse is

$$T^{-1} = \begin{pmatrix} 1/2 & 0 \\ 0 & -1/6 \end{pmatrix}$$

showing that $\delta(A) = \mathbb{Z}\frac{1}{2} + \mathbb{Z}(-\frac{1}{6}\sqrt{-3})$. The proof concluded with

$$\mathcal{O}_K \subset \delta(A) \subset \tfrac{1}{-12}A = \tfrac{1}{12}\mathbb{Z} + \tfrac{1}{12}\sqrt{-3}\,\mathbb{Z}.$$

This is true as we know that $\mathcal{O}_K$ is generated by 1 and $\frac{1}{2} + \frac{1}{2}\sqrt{-3}$. One can show that $\delta(\mathcal{O})/\mathcal{O}$ is cyclic of order 3. ◇

Definition 2.17. If a set $\{\alpha_1, \ldots, \alpha_d\}$ is a $\mathbb{Z}$-basis of $\mathcal{O}_K$, we call it an **integral basis** of K. The determinant $\Delta_K = \det(\mathrm{Tr}(\alpha_i\alpha_j))_{i,j} \in \mathbb{Z}$ is called the **discriminant** of K. The set $\mathfrak{d} = \delta(\mathcal{O}_K)$ is called the **codifferent** of K.

Examples.

- From Section 2.3, we know the ring of integers in a quadratic field. If D is an integer congruent to 2 or 3 modulo 4, then $\{1, \sqrt{D}\}$ is an integral basis for $\mathbb{Q}(\sqrt{D})$. The discriminant is

$$\Delta_{\mathbb{Q}(\sqrt{D})} = \det\begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\sqrt{D}) \\ \mathrm{Tr}(\sqrt{D}) & \mathrm{Tr}(D) \end{pmatrix} = \det\begin{pmatrix} 2 & 0 \\ 0 & 2D \end{pmatrix} = 4D.$$

  Instead when $D \equiv 1 \pmod 4$ and D is not a square, then $\{1, \frac{1}{2} + \frac{1}{2}\sqrt{D}\}$ is an integral basis. This time, we find

$$\Delta_{\mathbb{Q}(\sqrt{D})} = \det\begin{pmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\frac{1}{2} + \frac{1}{2}\sqrt{D}) \\ \mathrm{Tr}(\frac{1}{2} + \frac{1}{2}\sqrt{D}) & \mathrm{Tr}(\frac{1+D}{4} + \frac{1}{2}\sqrt{D}) \end{pmatrix} = \det\begin{pmatrix} 2 & 1 \\ 1 & \frac{1+D}{2} \end{pmatrix} = D.$$

◇

It is tempting to think that the ring of integers has a basis of the form 1, α, $\ldots$, α^{d-1} for some α. It this happens, then $\mathcal{O}_K = \mathbb{Z}[\alpha]$ is called **monogenic**. The following example shows that that there are non-monogenic ring of integers.

Example. Let K be the number field $\mathbb{Q}(\alpha)$ with $\alpha^3+\alpha^2-2\alpha+8 = 0$. Set $\beta = \frac{1}{2}\alpha+\frac{1}{2}\alpha^2$, which can be shown to be an algebraic integer, just like α. In an exercise, you will show that $\mathcal{O} = \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\beta$.

Suppose that 1, γ, γ^2 is also an integral basis. Write $\gamma = x + y\alpha + z\beta$ for unknown $x, y, z \in \mathbb{Z}$. A little computation can show the following

$$\begin{aligned} \alpha^2 &= -\alpha + 2\beta \\ \alpha\beta &= -4 + \alpha \\ \beta^2 &= -2 - 2\alpha + \beta \end{aligned}$$

which allows us to express γ^2:

$$\gamma^2 = (x^2 - 8yz - 2z^2) + (2xy - y^2 + 2yz - 2z^2)\alpha + (2xz + 2y^2 + z^2)\beta.$$

Now the change of basis matrix is

$$\begin{pmatrix} 1 & x & x^2 - 8yz - 2z^2 \\ 0 & y & 2xy - y^2 + 2yz - 2z^2 \\ 0 & z & 2xz + 2y^2 + z^2 \end{pmatrix}$$

whose determinant factors as $(y+z)(2y^2 - yz + 2z^2)$. If this determinant was equal to ± 1, then $y+z = \pm 1$. Plugging $z = \pm 1 - y$ into the second factor gives $5y^2 \mp 5y + 2 \equiv 2 \pmod 5$, which can never be equal to ± 1.

Since only matrices with determinant ± 1 are allowed to change of basis by Corollary 2.5, we see that no γ exists such that $\mathcal{O}$ is equal to $\mathbb{Z}[\gamma]$. ◇

Digression

The calculation of the ring of integer is a number field is not really very complicated in practise. For full details on the algorithm, see Section 4.4 in [2]. cohen

```
sage: R.<X> = QQ[]
sage: K.<a> = NumberField(X^3+X^2-2*X+8)
sage: OK = K.ring_of_integers()
sage: OK.basis()
[1, 1/2*a^2 + 1/2*a, a^2]
sage: K.discriminant()
-503
```

Proposition 2.18

int_closed_prop

Let K be a number field and $\alpha \in K$. If there is a non-zero monic polynomial $f \in \mathcal{O}_K[X]$ with $f(\alpha) = 0$, then $\alpha \in \mathcal{O}_K$.

You will find in textbooks that this is stated by saying that $\mathcal{O}_K$ is integrally closed.

Proof. Write $f = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ with $a_i \in \mathcal{O}_K$. Again α^n and all larger power of α are in $A = \mathcal{O}_K + \mathcal{O}_K\alpha + \cdots + \mathcal{O}_K\alpha^{n-1}$. By the previous proposition, we know that $\mathcal{O}_K$ is finitely generated as a group. Now $\mathbb{Z}[\alpha]$ is contained in the figab group A and, by Lemma 2.2, sub_figab_lem it is also a figab group, which shows that α is in $\mathcal{O}_K$ by Proposition 2.9. int_figab_prop □

Recall that the group of units of the ring $\mathcal{O}_K$ is defined to be

$$\mathcal{O}_K^\times = \{\alpha \in \mathcal{O}_K \mid 1/\alpha \in \mathcal{O}_K\}.$$

Proposition 2.19

units_norm_prop

Let $\alpha \in \mathcal{O}_K$ be an algebraic integer in a number field K. Then $\alpha \in \mathcal{O}_K^\times$ if and only if $\mathrm{N}(\alpha) = \pm 1$.

Proof. $\Rightarrow$: If α is invertible, there exists another algebraic integer $\beta \in \mathcal{O}_K$ such that $\alpha\beta = 1$. Then $\mathrm{N}(\alpha) \cdot \mathrm{N}(\beta) = \mathrm{N}(1) = 1$. By Corollary 2.8, int_norm_cor both $\mathrm{N}(\alpha)$ and $\mathrm{N}(\beta)$ are integers. This leaves only the possibility that $\mathrm{N}(\alpha) = \mathrm{N}(\beta) = 1$ or $\mathrm{N}(\alpha) = \mathrm{N}(\beta) = -1$.

$\Leftarrow$: Assume $\mathrm{N}(\alpha) = \pm 1$ and write d for the degree of α. Consider the reversed polynomial $g(X) = X^d \cdot F_\alpha(1/X)$. It has integer coefficients since $\alpha \in \mathcal{O}_K$. The leading term of g is the constant term of F_α, which is ± 1 by Lemma 1.13. char_poly_lem After possibly switching the sign, we get a monic polynomial $\pm g \in \mathbb{Z}[X]$ which has $1/\alpha$ as a root. Therefore $1/\alpha \in \mathcal{O}_K$ which shows that $\alpha \in \mathcal{O}_K^\times$. □

Example. For the cyclotomic field $\mathbb{Q}(\zeta)$ with an odd prime p, we have seen that $\mathrm{N}(\zeta^i) = 1$ so these are all units; but that is not surprising as the inverse is ζ^{p-i}.

However, for any $0 \leqslant i < j < p$, we have seen that $\mathrm{N}(\zeta^j - \zeta^i) = p$. Consider fractions of two of these algebraic integers, like for any $1 < i < p$

$$\xi = \frac{\zeta^i - 1}{\zeta - 1} = 1 + \zeta + \zeta^2 + \cdots + \zeta^{i-1}.$$

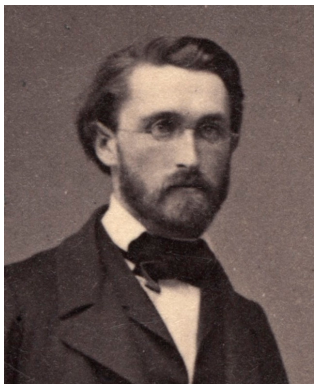
As the norm is multiplicative, we must have $\mathrm{N}(\xi) = 1$. The right hand side shows that $\xi \in \mathbb{Z}[\zeta]$. If we know that $\mathcal{O}_{\mathbb{Q}(\zeta)} = \mathbb{Z}[\zeta]$, which is one of the later exercises for this chapter, this shows that ξ is a unit. Though, we can also verify it directly: Let j be an inverse of i modulo p so that $\zeta^{ij} = \zeta^1$. Then

$$\frac{1}{\xi} = \frac{\zeta - 1}{\zeta^i - 1} = \frac{\zeta^{ij} - 1}{\zeta^i - 1} = 1 + \zeta^i + \zeta^{2i} + \cdots + \zeta^{(j-1)i}$$

is also an algebraic integer. ◇

3 Factorisation of ideals

In the 1840ies Ernst Eduard Kummer (1810–1893) developed his idea of "ideal numbers" to deal with the problem that unique factorisation does not hold in general rings. Julius Wilhelm Richard Dedekind (1831–1916) can be credited with the formalisation of the notion of "ideals".



3.1 A ring of integers without greatest common divisors

Let R be a ring. We say that an element $a \in R$ is irreducible if it cannot be written as a product of two non-units. In $\mathbb{Z}$ the irreducible elements are $\pm p$ for a prime p. In many rings it is easy to show that every element can be written as a product of irreducible elements and units; just factor it until it cannot be broken up anymore. The proof of the unique factorisation in $\mathbb{Z}$ and in the Gaussian integers $\mathbb{Z}[i]$ relies on the existence of a greatest common divisor (gcd). It turns out very few rings of integers have a gcd.

Let us now consider the example of the ring $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$, which is the ring of integers in the quadratic field $\mathbb{Q}(\sqrt{-5})$. Recall that in a ring of integers, units are exactly the elements of norm ± 1 by Proposition 2.19 and, in an exercise, we have seen that there are none, but ± 1. We have the following identity

$$6 = 3 \cdot 2 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}).$$

We will show that 2, 3 and $1 \pm \sqrt{-5}$ are all irreducible elements in this ring. The norms of these elements are

$$\mathrm{N}(6) = 36,\ \mathrm{N}(3) = 9,\ \mathrm{N}(2) = 4,\ \mathrm{N}(1 + \sqrt{-5}) = 6,\ \text{and}\ \mathrm{N}(1 - \sqrt{-5}) = 6.$$

If $1 + \sqrt{-5} = \alpha\beta$ for two non-units $\alpha, \beta \in \mathcal{O}_K$, then $\mathrm{N}(\alpha) \cdot \mathrm{N}(\beta) = 6$. Thus, one has to have norm ± 2 the other norm ± 3. However $2 = \mathrm{N}(a + b\sqrt{-5}) = a^2 + 5b^2$ is impossible: b must be zero otherwise $a^2 + 5b^2 \geqslant 5 > 0$, but then $2 = a^2$ has no solution. In the same fashion $3 = a^2 + 5b^2$ is also impossible. The negative values are also no option as $a^2 + 5b^2 \geqslant 0$. Since this is similar for 3, 2, and $1 - \sqrt{-5}$, factorisation into irreducible is not unique in this ring $\mathcal{O}_K$

Another related concept also fails to be useful: An element a in a ring R is a prime element if $a \mid bc$ implies $a \mid b$ or $a \mid c$ for all $b, c \in R$. None of our four elements is a

prime element in $\mathcal{O}_K$: For instance $1+\sqrt{-5}$ divides $3\cdot 2$, but it cannot divide either 3 nor 2; this is best argued again using the norm.

We will abandon those two concepts from our study of algebraic integers. Historically the next big step forward was made by Kummer who introduced abstract "ideal" numbers that represent the non-existing gcd. For instance, if we want to factor 6 further than above, we need a new thing that behaves like $\gcd(3, 1+\sqrt{5})$. It was Dedekind that realised that one can create concrete objects that act like these gcds.

The idea is to remember that in the integers $\gcd(a,b)$ is also the smallest non-zero number that can be written as $a\,x + b\,y$ as x and y run through all integers. Here "smallest" can be viewed as ordered by the absolute value or when ordered by divisibility, i.e., there is an element g which divides all elements of this form. In our example, we would want to find an element in the set

$$I = \{3\,x + (1+\sqrt{-5})\,y \;\mid\; x, y \in \mathcal{O}_K\}.$$

If we order the elements in this set I by their norm, we find elements in it of norm 0, 6, 9, 21, 24, 30, ... Taking one of smallest norm like $1+\sqrt{-5} \in I$ does not help: Not every element of I is a multiple of it.

Dedekind's idea was not to bother with picking a good element in I, but to take the set I itself as the replacement for the gcd. Writing it as $I = (3, 1+\sqrt{-5})$ reminds us of the notation of the gcd. Our aim is now to give sense to the expression $6 = I_1 \cdot I_2 \cdot I_3 \cdot I_4$ with $I_1 = (3, 1+\sqrt{-5})$, $I_2 = (3, 1-\sqrt{-5})$, $I_3 = (2, 1+\sqrt{-5})$, and $I_4 = (2, 1-\sqrt{-5})$ and in what sense this is a unique factorisation. We will later apply it to solve diophantine equations over $\mathbb{Q}$ to illustrate that this is really a very powerful method.

3.2 Ideals

Let R be a ring.

Definition 3.1. A subset $I \subset R$ is an **ideal** if it is an additive subgroup of $(R,+)$ such that $ax \in I$ for all $a \in R$ and $x \in I$.

If a_1, a_2, ..., a_r are elements in R, we denote by

$$(a_1, a_2, \ldots, a_r) = a_1\,R + a_2\,R + \cdots + a_r\,R = \{a_1x_1 + a_2x_2 + \cdots + a_rx_r \;\mid\; x_i \in R\}$$

the ideal in R generated by these elements. In particular, for any $a \in R$, the ideal $(a) = aR$ is a **principal ideal**.

We can define operations on ideals. If I and J are ideals then

$$I + J = \{a + b \mid a \in I, b \in J\} \text{ and } I \cdot J = \Big\{\sum_{i=1}^{s} a_i b_i \;\Big|\; a_i \in I, b_i \in J\Big\}.$$

In terms of generators, say $I = (a_1, \ldots, a_r)$ and $J = (b_1, \ldots, b_s)$, we can write

$$I + J = (a_1, \ldots, a_r, b_1, \ldots, b_s) \text{ and } I \cdot J = (a_1b_1, a_1b_2, \ldots, a_1b_s, a_2b_1, \ldots, a_rb_s).$$

The intersection of two ideals is also an ideal, but that is not easily expressed in terms of generators. The union is not in general an ideal; $I + J$ takes the role of the smallest ideal containing $I \cup J$. The zero ideal $(0) = \{0\}$ satisfies $(0) + I = I$ and $(0) \cdot I = (0)$, while the ideal $(1) = R$ has the properties $(1) + I = (1)$ and $(1) \cdot I = I$, for all ideals I.

Definition 3.2.
- We say I **divides** J, written $I \mid J$, if there is an ideal I' such that $J = II'$.
- Two ideals I and J are **coprime** if $I + J = (1)$.
- An ideal is **prime** if $ab \in I$ implies $a \in I$ or $b \in I$.

Recall that an ideal is prime if and only if R/I is an integral domain. Note that the words "coprime" and "prime" usually refer to factorisation property, but our definitions here do not refer to the divisibility properties. Later we will correct this and link it to the divisibility by ideal.s

ideal_figab_lem

Lemma 3.3

Let K be a number field. Then any ideal $I \neq (0)$ in the ring of integers $\mathcal{O}_K$ is a free figab of rank $d = [K : \mathbb{Q}]$.

Proof. As I is a subgroup of $\mathcal{O}_K$ it is also free and of rank at most d. Take $\beta \neq 0$ in I. Then I contains $\beta\alpha_1, \ldots, \beta\alpha_d$ where α_i is an integral basis given by Theorem 2.16. fin_gen_thm
Since these elements are also a $\mathbb{Q}$-basis of K, the rank of I is at least d. □

Example. Let $K = \mathbb{Q}(\sqrt{-5})$ and set

$$I_1 = (3, 1+\sqrt{-5}),\ I_2 = (3, 1-\sqrt{-5}),\ I_3 = (2, 1+\sqrt{-5}),\ \text{and}\ I_4 = (2, 1-\sqrt{-5}).$$

Then

$$I_1 \cdot I_2 = (9,\ 3(1+\sqrt{-5}),\ 3(1-\sqrt{5}),\ (1+\sqrt{-5})(1-\sqrt{-5})).$$

The last element is 6 and therefore $3 = 9 - 6$ is also in I. However all four generators are multiples of 3, therefore $I_1 \cdot I_2 = (3)$. Similarly $I_3 \cdot I_4 = (2)$. For $I_1 \cdot I_3 = (6, 3(1+\sqrt{-5}), 2(1+\sqrt{-5}), (1+\sqrt{-5})^2)$, the difference of the two middle terms shows that $1+\sqrt{-5}$ belongs to $I_1 \cdot I_3$ and all four generators are multiples of $1+\sqrt{-5}$; therefore $I_1 \cdot I_3 = (1+\sqrt{-5})$. Also $I_2 \cdot I_4 = (1-\sqrt{-5})$.

We can also describe the ideals as abelian groups. For instance $I_1 = (3, 1+\sqrt{-5})$ is generated as a group by 3, $3\sqrt{-5}$, $1+\sqrt{-5}$, and $(1+\sqrt{-5})\sqrt{-5} = -5+\sqrt{-5}$. Since $3\sqrt{-5} = -1\cdot 3 + 3(1+\sqrt{-5})$ and $-5+\sqrt{-5} = -2\cdot 3 + 1\cdot(1+\sqrt{-5})$, we have in fact $I_1 = 3\mathbb{Z} + (1+\sqrt{-5})\mathbb{Z}$ as an abelian group. One can also describe it as

$$I_1 = \left\{ a + b\sqrt{-5} \;\middle|\; a, b \in \mathbb{Z} \text{ with } a \equiv b \pmod 3 \right\}.$$

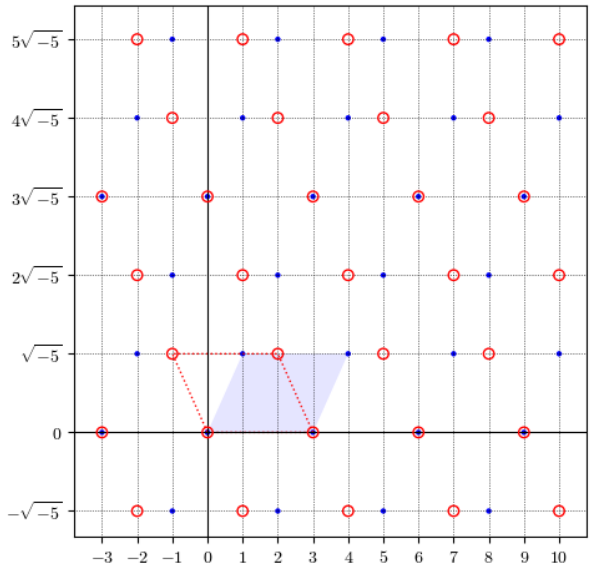
With the same method one obtains

$$I_2 = 3\mathbb{Z} + (1-\sqrt{-5})\mathbb{Z} = \left\{ a + b\sqrt{-5} \;\middle|\; a, b \in \mathbb{Z} \text{ with } a \equiv -b \pmod 3 \right\}$$

In the picture on the next page, the ideal I_1 is formed by the blue dots and I_2 by the red dots. Further

$$I_3 = I_4 = 2\mathbb{Z} + (1+\sqrt{-5})\mathbb{Z} = \left\{ a + b\sqrt{-5} \;\middle|\; a, b \in \mathbb{Z} \text{ with } a \equiv b \pmod 2 \right\}.$$

It was not at first obvious that I_3 and I_4 are equal. Even less that $(2) = I_3^2$ is the square of an ideal, despite the ring not containing $\sqrt{2}$.



◇

3.3 The norm of an ideal

Let K be a number field of degree d. Whenever we say I is an ideal in K, we will mean that it is an ideal of the ring of integers $\mathcal{O}_K$.

Lemma 3.4

If $\alpha \in I$, then $\mathrm{N}(\alpha) \in I$.

Proof. Writing $c_i \in \mathbb{Z}$ for the coefficients of the characteristic polynomial χ_α, we have

$$\mathrm{N}(\alpha) = -(-1)^d \cdot (\alpha^d + c_{d-1}\,\alpha^{d-1} + \cdots + c_1\alpha)$$

by Lemma 1.13 (char_poly_lem) as $\chi_\alpha(\alpha) = 0$. The right hand side belongs to $\alpha\,\mathcal{O}_K \subset I$. □

Lemma 3.5

quo_finite_lem

For any non-zero ideal I, the quotient ring $\mathcal{O}_K/I$ has finitely many elements.

Proof. Since $I \neq (0)$, we know that I contains an integer $a \in \mathbb{Z}$ by the previous lemma. Then $a\mathcal{O} \subset I$, which means that there is a surjective ring homomorphism

$$\mathcal{O}/a\mathcal{O} \to \mathcal{O}/I \qquad \beta + a\mathcal{O} \mapsto \beta + I$$

As an abelian group $\mathcal{O}/a\mathcal{O}$ is isomorphic to $\mathbb{Z}^d/a\mathbb{Z}^d \cong (\mathbb{Z}/a\mathbb{Z})^d$ which is finite. □

Definition 3.6. For a non-zero ideal I of $\mathcal{O}_K$, we set $\mathbb{N}(I) = \#\mathcal{O}_K/I$ and call it the **norm** of I. We also set $\mathbb{N}((0)) = 0$.

Example. In practice, it is possible to calculate the quotient ring $\mathcal{O}/I$. Let us do this slowly for the ideal $I = I_1 = (3, 1+\sqrt{-5})$ in $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. The ring itself is a quotient, namely $\mathbb{Z}[\sqrt{-5}] = \mathbb{Z}[X]/(X^2+5)$. Under the correspondence theorem 0.8, the ideal I corresponds to an ideal $\tilde{I}$ in $\mathbb{Z}[X]$ containing (X^2+5) obtained by taking the union of all cosets in I. Then $\tilde{I}$ contains 3, $1+X$ and X^2+5 and these three will generate $\tilde{I}$. The third isomorphism theorem 0.8 gives

$$\mathcal{O}/I \cong \mathbb{Z}[X]/\tilde{I} = \mathbb{Z}[X]/(3, 1+X, X^2+5).$$

To quotient by 3 means that we can reduce all coefficients of polynomials modulo 3 and we obtain

$$\mathcal{O}/I \cong \mathbb{Z}[X]/(3, X+1, X^2+5) \cong \mathbb{F}_3[X]/(X+1, X^2+5).$$

Alternatively, this is the third isomorphism theorem again with $\mathbb{Z}[X] \supset (3) \supset \tilde{I}$.

Next the ideal $(X+1)$ is the kernel of the evaluation at -1. Thus

$$\mathcal{O}/I \cong \mathbb{F}_3[X]/(X+1, X^2+2) \cong \mathbb{F}_3/((-1)^2+5) = \mathbb{F}_3/(6) = \mathbb{F}_3.$$

Alternatively, $X^2+2 = (X+1)(X+2)$ in $\mathbb{F}_3[X]$ shows that we can drop the second generator. This shows $\mathbb{N}(I_1) = 3$.

For the ideals $I_2 = (3, 1-\sqrt{-5})$ and $I_3 = (2, 1+\sqrt{-5})$, the same method gives $\mathbb{N}(I_2) = 3$ and $\mathbb{N}(I_3) = 2$. Actually, we have shown that in each case, the quotient was a field and hence these are maximal ideals and so prime ideals. ◇

Lemma 3.7

If $I = \alpha\mathcal{O}_K$ is principal then $\mathbb{N}(\alpha\mathcal{O}_K) = |\mathrm{N}(\alpha)|$.

Proof. We have seen one special case of this already: When $\alpha = a$ is an integer. In that case we saw that $\mathbb{N}(a\mathcal{O}) = (\#\mathbb{Z}/a\mathbb{Z})^d = |a|^d = |a^d|$.

In general, we use Lemma 2.4. Recall that $A = \mathcal{O}$ is a free figab group of rank $[K:\mathbb{Q}]$ and I is a subgroup of the same rank. If $\alpha_1, \ldots, \alpha_n$ is an integral basis, then $\beta_1 = \alpha\alpha_1, \ldots, \beta_n = \alpha\alpha_n$ is a $\mathbb{Z}$-basis of I. For every j, write $\beta_j = x_{1,j}\alpha_1 + \cdots + x_{n,j}\alpha_n$. Then the matrix $(x_{i,j})$ is exactly the matrix M_α of the map m_α in the basis $\alpha_1, \ldots, \alpha_n$. Lemma 2.4 implies that $\#\mathcal{O}/\alpha\mathcal{O} = |\det(x_{i,j})|$. Therefore $\mathbb{N}(\alpha\mathcal{O}) = |\det(M_\alpha)| = |\mathrm{N}(\alpha)|$. □

dim1_prop

Proposition 3.8

Any non-zero prime ideal in a number ring is a maximal ideal.

Proof. Let $(0) \neq \mathfrak{p}$ be a prime ideal in the number ring $\mathcal{O}$. We want to show that $\mathcal{O}/\mathfrak{p}$ is a field. Let $0 \neq x \in \mathcal{O}/\mathfrak{p}$. To say that $\mathfrak{p}$ is a prime ideal, means that the quotient ring has no non-zero zero-divisors. This implies that the map

$$\begin{aligned} \mathcal{O}/\mathfrak{p} &\to \mathcal{O}/\mathfrak{p} \\ y &\mapsto x \cdot y \end{aligned}$$

is injective. By Lemma 3.5, this is an injective map between finite groups of the same order; thus the map is also surjective. Now, the preimage of 1 is an inverse of x and hence $\mathcal{O}/\mathfrak{p}$ is a field. □

Definition 3.9. The quotient ring $\mathcal{O}_K/\mathfrak{p}$ for a non-zero prime ideal $\mathfrak{p}$ is called the **residue field** and we denote it by $\mathbb{F}_\mathfrak{p}$.

The following is a technical lemma that will be used later. It is the analogue to saying that any integer divides a product of prime numbers.

prod_in_lem

Lemma 3.10

Let I be a non-zero ideal in the number ring $\mathcal{O}_K$. Then there exist prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$ such that

$$\mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdots \mathfrak{p}_r \subset I.$$

Proof. Let I be a counter-example such that $\mathbb{N}(I)$ is minimal. Obviously I cannot be prime. Therefore there exists $\alpha, \beta \in \mathcal{O}_K$ such that $\alpha \cdot \beta \in I$ but neither α nor β belongs to I. Consider the ideals $J_1 = \alpha\mathcal{O}_K + I$ and $J_2 = \beta\mathcal{O}_K + I$. Since $\alpha \notin I$, we have $I \subsetneq J_1$ and hence $\mathbb{N}(J_1) < \mathbb{N}(I)$ as seen in an exercise. By the assumed minimality of I, there exist ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ such that $\mathfrak{p}_1 \cdots \mathfrak{p}_s \subset J_1$. Similarly there are prime ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_t$ such that $\mathfrak{q}_1 \cdots \mathfrak{q}_t \subset J_2$. Then

$$\mathfrak{p}_1 \cdots \mathfrak{p}_s \cdot \mathfrak{q}_1 \cdots \mathfrak{q}_t \subset J_1 \cdot J_2 = \alpha\beta\mathcal{O}_K + \alpha I + \beta I + I \cdot I \subset I$$

contradicts the assumption that I was a counter-example. □

3.4 Fractional ideals

We extend the notion of ideals. This is comparable to the passage from integers to rational numbers. Eventually we will define a group structure on ideals and that will need "ideals" bigger than $\mathcal{O}_K$.

Definition 3.11. A **fractional ideal** I in a number field K is a subset $I \subset K$ such that

- I is an additive subgroup of K;
- for all $\alpha \in \mathcal{O}_K$ and $\beta \in I$, also $\alpha\beta \in I$; and
- there is a finite set $\alpha_1, \ldots, \alpha_n$ such that $I = \alpha_1\mathcal{O}_K + \cdots + \alpha_n\mathcal{O}_K$.

We can write $I = (\alpha_1, \ldots, \alpha_n)$.

In fact the last condition implies the first two conditions. For those having seen the theory of modules, one could just ask that I is a finitely generated $\mathcal{O}_K$-module contained in K. Note that the first two conditions are alike for ideals; in particular if a fractional ideal is contained in $\mathcal{O}_K$ then it is a usual ideal. Conversely, every usual ideal is a fractional ideal by Lemma 3.3. "Usual" ideals are also called **integral ideals** when we need to be specific.

ideal_figab_lem

The last condition is needed to exclude subsets of K that are too big, like K itself or the set of all rational numbers whose denominator is a power of 2. For $K = \mathbb{Q}$ each fractional ideal is of the form $r\mathbb{Z}$ with r a rational number. For instance $\frac{2}{7}\mathbb{Z} = \{\ldots, -4/7, -2/7, 0, 2/7, 4/7, \ldots\}$ is a fractional ideal.

frac_ideals_lem

Lemma 3.12

Let I be a fractional ideal in K. Then there exists an algebraic integer $\delta \in \mathcal{O}_K$ such that δI is an integral ideal inside $\mathcal{O}_K$.

Conversely, every set of the form $\frac{1}{\delta}J$ with J an integral ideal and $\delta \in \mathcal{O}_K$ is a fractional ideal.

Proof. Take the finite set $\{\alpha_1, \ldots, \alpha_n\}$ such that $I = (\alpha_1, \ldots, \alpha_n)$. For each i there is a $d_i \in \mathbb{Z}$ by Corollary 2.12 (full_lattice_cor) such that $d_i\alpha_i \in \mathcal{O}_K$. Setting $\delta = d_1 \cdots d_n \in \mathbb{Z} \subset \mathcal{O}_K$ we obtain $\delta I \subset \mathcal{O}_K$.

Conversely, it is easy see that $\delta^{-1}J$ satisfies the condition of being a fractional ideal. □

As a consequence, fractional ideals are also free figab groups of rank $[K : \mathbb{Q}]$. The operations on integral ideals extend to fractional ideals: The product, sum and intersection of fractional ideals is a fractional ideal.

For any non-zero integral ideal I, we define

$$I^{-1} := \{\alpha \in K \mid \alpha \cdot I \subset \mathcal{O}_K\}$$

The notation as an inverse is in no way justified at this stage, but will become clear later.

inv_frac_lem

Lemma 3.13

For any non-zero integral ideal, the set I^{-1} is a fractional ideal with $I^{-1} \supset \mathcal{O}_K$.

Proof. First it is clear from the definition that $\mathcal{O} \subset I^{-1}$.

Pick a $\beta \in I$. Then for any $\alpha \in I^{-1}$, we have $\alpha\beta \in \mathcal{O}$ by definition. Therefore $\beta I^{-1} \subset \mathcal{O}$. It is easy to check that I^{-1} is an additive group and that multiplying an element in I^{-1} by an element in $\mathcal{O}$ is still in I^{-1}. Therefore βI^{-1} is an integral ideal and hence I^{-1} a fractional ideal by Lemma 3.12 (frac_ideals_lem). □

Example. Let $I = (3, 1 + \sqrt{-5})$ in $\mathcal{O} = \mathbb{Z}[\sqrt{-5}]$. Write $\alpha = x + y\sqrt{-5}$ with $x, y \in \mathbb{Q}$. To say that $\alpha \in I^{-1}$ is the same as to ask if $\alpha \cdot 3 \in \mathcal{O}$ and $\alpha(1 + \sqrt{-5}) \in \mathcal{O}$. This gives the following conditions:

$$3x \in \mathbb{Z}, \qquad 3y \in \mathbb{Z}, \qquad x - 5y \in \mathbb{Z}, \qquad \text{and} \qquad x + y \in \mathbb{Z}.$$

This is equivalent to $x = a/3$ and $y = b/3$ with integers a, b that satisfy $a - 5b \in 3\mathbb{Z}$ and $a + b \in 3\mathbb{Z}$. These two are the same condition. We find

$$I^{-1} = \left\{ \frac{a + b\sqrt{-5}}{3} \;\middle|\; a, b \in \mathbb{Z} \text{ and } a \equiv -b \pmod 3 \right\}$$

In fact, this is $\frac{1}{3}(3, 1 - \sqrt{-5})$. ◇

Lemma 3.14

Let $\mathfrak{p}$ be a non-zero prime ideal. Then $\mathfrak{p}^{-1} \supsetneq \mathcal{O}_K$.

Proof. Let $0 \neq \beta \in \mathfrak{p}$. By Lemma 3.10, there are prime ideals $\mathfrak{q}_1, \ldots \mathfrak{q}_m$ such that $\mathfrak{q}_1 \cdots \mathfrak{q}_m \subset \beta\mathcal{O}$. Among all such sets of prime ideals, we can choose one with m minimal. If all these prime ideals $\mathfrak{q}_i$ were different from $\mathfrak{p}$ then we could choose a $\alpha_i \in \mathfrak{q}_i \setminus \mathfrak{p}$ for each i and then $\alpha_1 \cdots \alpha_m$ would belong to $\mathfrak{p}$ which contradicts the primality of $\mathfrak{p}$. Renumbering if needed, we may assume $\mathfrak{q}_1 = \mathfrak{p}$.

By the minimality of m, the product $\mathfrak{q}_2 \cdots \mathfrak{q}_m$ is not contained in $\beta\mathcal{O}$. Pick γ inside this product, but not belonging to $\beta\mathcal{O}$. Then $\gamma\mathfrak{p} \subset \beta\mathcal{O}$, meaning that $\delta = \gamma/\beta$ belongs to $\mathfrak{p}^{-1}$ but δ is not in $\mathcal{O}$. □

Lemma 3.15

inv_tech_lem

Let $\mathfrak{p}$ be a non-zero prime ideal and let I be any non-zero integral ideal. Then $\mathfrak{p}^{-1} \cdot I \supsetneq I$.

Proof. Let $\delta \in \mathfrak{p}^{-1}$ which does not belong to $\mathcal{O}$ as constructed in the previous lemma. We write $I = (\beta_1, \beta_2, \ldots, \beta_r)$ for some $\beta_i \in \mathcal{O}_K$. We are done if we can show that there is a $1 \leqslant j \leqslant r$ such that $\delta\beta_j \notin I$.

To prove this we assume the contrary that $\delta\beta_j \in I$ for all j and aim to obtain a contradiction. For all j, we find $\gamma_{i,j} \in \mathcal{O}$ such that

$$\delta\beta_j = \sum_{i=1}^{r} \gamma_{i,j}\beta_i.$$

This means that δ is an eigenvalue for the matrix $\Gamma = (\gamma_{i,j})$ for the eigenvector $(\beta_1, \ldots, \beta_r)$. Therefore δ is a root of the characteristic polynomial χ_Γ in K. However, χ_Γ belongs to $\mathcal{O}[X]$ since $\gamma_{i,j} \in \mathcal{O}$ for all i and j. Proposition 2.18 implies that $\delta \in \mathcal{O}$, which is a contradiction. □

Example. Before we continue, we should stop to realise that the particular choice of ring matters a lot here. Consider the ideal $I = (2, 1 + \sqrt{-3})$ in the ring $A = \mathbb{Z}[\sqrt{-3}]$. Remember A is not the ring of integers of $\mathbb{Q}(\sqrt{-3})$.

We can describe the ideal I as the set of $a+b\sqrt{-3}$ with $a, b \in \mathbb{Z}$ and $a \equiv b \pmod 2$. The set I^{-1} is the set of all $x+y\sqrt{-3}$ with $x, y \in \mathbb{Q}$ and $2x, 2y, x-3y, x+y \in \mathbb{Z}$. This is equal to the set of all $\frac{1}{2}(u+v\sqrt{-3})$ with integers u, v such that $u \equiv v \pmod 2$. Hence $I^{-1} = \frac{1}{2}I$. However if $a + b\sqrt{-3} \in I$ and $(u + v\sqrt{-3})/2 \in I^{-1}$, then their product $(au - 3bv + (av + bu)\sqrt{-3})/2$ belongs to I because $au - 3bv \equiv av + bu \pmod 4$. In this ring, we have $I^{-1}I = I$. Urrrghh, the notation I^{-1} is certainly not a good choice this time. ◇

Lemma 3.16

prime_inverse_lem

Let $\mathfrak{p}$ be a non-zero prime ideal. Then $\mathfrak{p} \cdot \mathfrak{p}^{-1} = \mathcal{O}_K = (1)$.

This now justifies the notation $\mathfrak{p}^{-1}$ a little, though at this stage we do not know if this is the only fractional ideal with this property.

Proof. The previous lemma shows $\mathfrak{p}\mathfrak{p}^{-1} \supsetneq \mathfrak{p}$. From the definition all elements in $\mathfrak{p}\mathfrak{p}^{-1}$ are integral. Since $\mathfrak{p}$ is maximal by Proposition 3.8, we must have $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$. □

The previous lemmas lead to the following two theorem, which hold for the ring of integer in a number field, but not to other choices of rings as seen in the previous example.

ideal_group_thm

Theorem 3.17

The set of non-zero fractional ideals forms an abelian group under multiplication.

Proof. The identity element is $(1) = \mathcal{O}_K$. Lemma prime_inverse_lem 3.16 shows that all prime ideals admit an inverse in this group; we need to extend this to all fractional ideals.

First, let I be an integral ideal. Suppose that is it a non-invertible ideal of minimal norm. The ideal I is contained in a maximal ideal $\mathfrak{p}$. By Lemma inv_tech_lem 3.15, have $I \subsetneq \mathfrak{p}^{-1} \cdot I \subset \mathfrak{p} \cdot \mathfrak{p}^{-1} = \mathcal{O}_K$. Therefore $\mathfrak{p}^{-1}I$ is an integral ideal of norm strictly smaller than the norm of I. By the minimality of I, there is an inverse fractional ideal J such that $J\mathfrak{p}^{-1}I = \mathcal{O}_K$. This equality shows that $J\mathfrak{p}^{-1}$ is the inverse of I. Therefore all integral ideals have an inverse.

For a general fractional ideal I, there is a $\delta \in \mathcal{O}_K$ such that $I = \delta^{-1}J$ for an integral ideal J by Lemma frac_ideals_lem 3.12. Then the inverse of I is $\delta\, J^{-1}$. □

It will be shown later in an exercise that the inverse of I in this group is I^{-1} as defined before Lemma inv_frac_lem 3.13 for all integral ideals, not just prime ideals. As a consequence, we can now freely use implications like $I_1 I_2 = I_3 \Rightarrow I_1 = I_2^{-1} I_3$.

3.5 Factorisation of ideals into prime ideals

factorisation_thm

Theorem 3.18

Every non-zero ideal in $\mathcal{O}_K$ can be written in a unique way as a product of prime ideals.

Proof. Let I be the ideal of minimal norm that contradicts the theorem.

Existence: The ideal I is contained in a maximal ideal $\mathfrak{p}$. By Lemma inv_tech_lem 3.15, we know that $I \subsetneq \mathfrak{p}^{-1}I$. Together with the minimality of I, this imply that the ideal $\mathfrak{p}^{-1}I$ is the product of primes $\mathfrak{p}_1 \cdots \mathfrak{p}_r$. Therefore $I = \mathfrak{p}\mathfrak{p}^{-1}I = \mathfrak{p} \cdot \mathfrak{p}_1 \cdots \mathfrak{p}_r$ is also the product of primes.

Uniqueness: Suppose

$$I = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdot \mathfrak{q}_2 \cdots \mathfrak{q}_s$$

for prime ideals $\mathfrak{p}_i$ and prime ideals $\mathfrak{q}_j$. If $\mathfrak{p}_1 \neq \mathfrak{q}_j$ for all j, then we can pick $\alpha_j \in \mathfrak{q}_j \setminus \mathfrak{p}_1$ and reach a problem as $\alpha_1 \cdots \alpha_s \in I \subset \mathfrak{p}_1$ contradicts the primality of $\mathfrak{p}_1$. Therefore there is a j such that $\mathfrak{p}_1 = \mathfrak{q}_j$. By the minimality of I, the factorisations $\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_{j-1} \cdot \mathfrak{q}_{j+1} \cdots \mathfrak{q}_s$, must be equal (up to reordering). This implies that the factorisation of I is also unique. □

At this stage, this is not very practical to find the factorisation; even just to find a single prime ideal in it. Though this shouldn't be that surprising as factoring integers is also difficult.

Example. Back to our initial example of factoring 6 in $\mathbb{Z}[\sqrt{-5}]$. The ideals $\mathfrak{p}_1 = (3, 1+\sqrt{-5})$, $\mathfrak{p}_2 = (3, 1-\sqrt{-5})$, and $\mathfrak{p}_3 = (2, 1+\sqrt{-5})$ are prime ideals and

$$(6) = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3^2$$

is the prime factorisation of the principal ideal (6). ◇

frac_fac_cor

Corollary 3.19

Every non-zero fractional ideal can be written in a unique way as

$$I = \mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdots \mathfrak{p}_r \cdot \mathfrak{q}_1^{-1} \cdot \mathfrak{q}_2^{-1} \cdots \mathfrak{q}_s^{-1}$$

for prime ideals $\mathfrak{p}_i$ and $\mathfrak{q}_j$ such that $\mathfrak{p}_i \neq \mathfrak{q}_j$ for all i, j.

Proof. We can write $I = (\delta\mathcal{O}_K)^{-1} \cdot J$ for integral ideals J and $\delta\mathcal{O}_K$. Apply to both factorisation_thm Theorem 3.18 and then simplify the primes that appear in both until the list has no common factors anymore. □

divisibility_cor

Corollary 3.20: To contain is to divide

Let I and J be two non-zero fractional ideals. The following statements are equivalent:

(i) $I \subset J$
(ii) $IJ^{-1} \subset \mathcal{O}_K$
(iii) $I^{-1}J \supset \mathcal{O}_K$
(iv) $J \mid I$

In the last point we have extended the definition of divisibility to fractional ideals: $J \mid I$ means that there exists an integral ideal I' such that $I = J \cdot I'$. The following now justifies the earlier definitions of coprime ideals and prime ideals.

Corollary 3.21

Let I and J be two non-zero integral ideals.

(i) The ideal I is a prime ideal if and only if cannot be written as a product of two proper integral ideals.
(ii) The ideal I is a prime ideal if and only if $I \mid J \cdot J'$ implies $I \mid J$ or $I \mid J'$.
(iii) The ideal $I + J$ is the greatest common divisor of I and J.
(iv) (Coprime) I and J have no common prime factor in their factorisation if and only if $I + J = \mathcal{O}_K$.
(v) The ideal $I \cap J$ is the lowest common multiple of I and J.
(vi) If I and J are coprime, then $I \cap J = I \cdot J$.

Proof. The first two are direct consequences of the prime factorisation Theorem factorisation_thm 3.18.

Then $I + J$ is the smallest ideal containing both I and J. Using the "contain is divide" slogan, this is also the smallest ideal that divides I and J. That in turn is equal to the product of all the prime factors that the factorisation of the ideal I and J have in common, so the greatest common divisor in that sense.

It is now immediate that I and J have no common prime factor if and only if $I+J = \mathcal{O}$.

The ideal $I \cap J$ is the largest ideal contained in both I and J, that is, being divisible by both I and J. Again this is the lowest product of prime factors of I and J divisible by both I and J.

Finally, if I and J are coprime, then they do not have any prime factors in common and therefore the lowest common multiple is just the product. □

Digression

Computational algebraic number theory can calculate with these ideals and factorisations well:

```
sage: R.<X> = QQ[]
sage: K.<a> = NumberField(X^2-1087)
sage: I = K.ideal(15*a-494)     # creates a fractional ideal
sage: I.factor()
(Fractional ideal (7, a + 3))^2 * (Fractional ideal (11, a + 3))
sage: p = K.ideal(7,a+3)
sage: p.is_prime()
True
sage: p.norm()
7
sage: q = K.ideal(11,a+3)
sage: p+q
Fractional ideal (1)
sage: p^(-1)
Fractional ideal (1, 1/7*a + 4/7)
sage: I^(-1)*p*q
Fractional ideal (1, 1/7*a + 4/7)
```

3.6 The Chinese remainder theorem

Theorem 3.22

chinese_thm

Let I be a proper integral ideal with prime factorisation

$$I = \mathfrak{p}_1^{k_1} \cdot \mathfrak{p}_2^{k_2} \cdots \mathfrak{p}_r^{k_r}$$

where $\mathfrak{p}_i$ are distinct prime ideals. Then there exists a ring isomorphism

$$\mathcal{O}_K/I \to \mathcal{O}_K/\mathfrak{p}_1^{k_1} \times \mathcal{O}_K/\mathfrak{p}_2^{k_2} \times \cdots \times \mathcal{O}_K/\mathfrak{p}_r^{k_r}.$$

Proof. By induction on r; the case when $r = 1$ is trivial. Set $I = \prod_{i=1}^{r-1} \mathfrak{p}_i^{k_i}$ and $J = \mathfrak{p}_r^{k_r}$. Then I and J are coprime. The induction hypothesis and the Chinese remainder theorem general_crt_thm 0.9 for general rings prove the theorem. □

Lemma 3.23

Let $I_1, \ldots, I_m$ be pairwise coprime integral ideal and let $\alpha_1, \ldots, \alpha_m$ in $\mathcal{O}_K$. Then there exists $\alpha \in \mathcal{O}_K$ such that $\alpha \equiv \alpha_i \pmod{I_i}$ for all i.

Proof. This is just a reformulation that the map from $\mathcal{O}_K/\prod I_i$ to $\prod_i \mathcal{O}_K/I_i$ is surjective. □

The following proposition tells us that any ideal can be generated with one or two generators only. In this sense, all ideals are the greatest common divisor of two numbers, meaning of two principal ideals.

two_gen_prop

Proposition 3.24

Let I be a non-zero fractional ideal and let $0 \neq \alpha \in I$. Then there exists $\beta \in I$ such that $I = (\alpha, \beta)$.

Proof. Assume first that I is an integral ideal. Write $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ for the prime factors of (α). Since $(\alpha) \subset I$, we can write $I = \prod_{i=1}^m \mathfrak{p}_i^{k_i}$ for integers $k_i \geqslant 0$. For each i pick a β_i in $\mathfrak{p}_i^{k_i}$ which does not belong to $\mathfrak{p}_i^{k_i+1}$. The previous lemma gives a $\beta \in \mathcal{O}_K$ such that $\beta \equiv \beta_i \pmod{\mathfrak{p}^{k_i+1}}$ for all i.

Now $\beta \subset \prod \mathfrak{p}_i^{k_i} = I$ and (β) is not divisible by any higher power of $\mathfrak{p}_i$ than $\mathfrak{p}_i^{k_i}$. In other words $(\beta) \cdot I^{-1}$ is coprime to (α). Hence $(\beta) \cdot I^{-1} + (\alpha) = \mathcal{O}_K$, which shows that $(\beta) + \alpha I = I$. However, $I = (\beta) + \alpha\, I \subset (\beta) + (\alpha) \subset I$ implies that $(\alpha, \beta) = I$.

Finally, if I is not integral, then there is $\delta \in \mathcal{O}_K$ such that $J = \delta\, I$ is integral and $\delta\alpha \in I$. By the first part there is a $\beta \in \delta I$ such that $(\delta\alpha, \beta) = \delta\, I$ which yields $I = (\alpha, \delta^{-1}\beta)$. □

smooth_prop

Proposition 3.25

Let $\mathfrak{p}$ be a non-zero prime ideal and let $n > 0$. There is an isomorphism of abelian group from $\mathbb{F}_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$ to $\mathfrak{p}^n/\mathfrak{p}^{n+1}$.

Proof. Let α be any element in $\mathfrak{p}^n \setminus \mathfrak{p}^{n+1}$ and consider the map

$$\begin{aligned} \phi_\alpha \colon \mathcal{O}_K &\to \mathfrak{p}^n/\mathfrak{p}^{n+1} \\ \beta &\mapsto \alpha\beta + \mathfrak{p}^{n+1} \end{aligned}$$

which is a group homomorphism on the additive structures. It is clear that $\mathfrak{p} \subset \ker(\phi_\alpha)$. Conversely, let $\beta \in \ker(\phi_\alpha)$. Now $\alpha\beta \in \mathfrak{p}^{n+1}$ means $\mathfrak{p}^{n+1} \mid (\alpha)(\beta)$, but $\mathfrak{p}^{n+1} \nmid (\beta)$ implies $\mathfrak{p} \mid (\alpha)$ and so $\alpha \in \mathfrak{p}$. If we show that ϕ_α is surjective, then the first isomorphism theorem proves the proposition.

Note that $\mathfrak{p}^{n+1}$ and $\alpha\mathfrak{p}^{-n}$ are two coprime integral ideals. Let $\gamma \in \mathfrak{p}^n$. Use the Chinese remainder theorem to find $\delta \in \mathcal{O}_K$ such that $\delta \equiv \gamma \pmod{\mathfrak{p}^{n+1}}$ and $\delta \equiv 0 \pmod{\alpha\mathfrak{p}^{-n}}$. The first condition implies that $\delta \in \mathfrak{p}^n$ since $\gamma \in \mathfrak{p}^n$. Therefore $\delta \in \mathfrak{p}^n\alpha\mathfrak{p}^{-n} = \alpha\mathcal{O}_K$ which shows that $\delta/\alpha \in \mathcal{O}_K$ is such that $\phi_\alpha(\delta/\alpha) = \delta + \mathfrak{p}^n = \gamma + \mathfrak{p}^n$. □

It is a consequence of Corollary 3.19 frac_fac_cor that every non-zero fractional ideal can be written uniquely as $I \cdot J^{-1}$ with integral coprime ideals I and J. We extend the definition of the norm to fractional ideals by setting $\mathbb{N}(I \cdot J^{-1}) = \mathbb{N}(I)/\mathbb{N}(J) \in \mathbb{Q}$. If $I = \alpha\mathcal{O}_K$ for some $\alpha \in K$, we still have $\mathbb{N}(\alpha\mathcal{O}_K) = |\mathbb{N}(\alpha)|$.

norm_hom_prop

Proposition 3.26

For any two fractional ideals I and J, we have $\mathbb{N}(I \cdot J) = \mathbb{N}(I) \cdot \mathbb{N}(J)$. In other words, $\mathbb{N}$ is a group homomorphism from the group of non-zero fractional ideals to $\mathbb{Q}^\times$.

Proof. From the extended definition, it is clear that it is enough to prove the formula for integral ideals I and J. First, we need to show that $\mathbb{N}(\mathfrak{p}^k) = \mathbb{N}(\mathfrak{p})^k$ for any prime

ideal $\mathfrak{p}$. The case $k = 1$ is clear and we proceed by induction on k. The third isomorphism theorem 0.8 shows that $\mathcal{O}_K/\mathfrak{p}^k$ is the quotient of $\mathcal{O}_K/\mathfrak{p}^{k+1}$ by the subgroup $\mathfrak{p}^k/\mathfrak{p}^{k+1}$. Therefore $\mathbb{N}(\mathfrak{p}^{k+1}) = \mathbb{N}(\mathfrak{p}^k) \cdot \#\mathfrak{p}^k/\mathfrak{p}^{k+1}$. By the previous proposition, $\#\mathfrak{p}^k/\mathfrak{p}^{k+1} = \#\mathcal{O}_K/\mathfrak{p} = \mathbb{N}(\mathfrak{p})$ and by induction $\mathbb{N}(\mathfrak{p}^k) = \mathbb{N}(\mathfrak{p})^k$.

Next, if $I = \prod_{i=1}^m \mathfrak{p}_i^{k_i}$ is the prime factorisation of an integral ideal I with $\mathfrak{p}_i$ distinct prime ideals, then the Chinese remainder Theorem 3.22 proves that

$$\mathbb{N}(I) = \#\mathcal{O}_K/I = \#\prod_{i=1}^m \mathcal{O}_K/\mathfrak{p}_i^{k_i} = \prod \mathbb{N}(\mathfrak{p}_i)^{k_i}.$$

Now it is easy to prove the formula. □

4 Decomposition, ramification and embeddings

4.1 Decomposing primes

Let K be a number field with $\mathcal{O}_K$ its ring of integers. Let $\mathfrak{p}$ be a non-zero prime ideal. We know that $\mathbb{F}_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$ is a finite field.

Consider $\mathfrak{p} \cap \mathbb{Z}$. First this is an ideal of $\mathbb{Z}$ as it is the intersection of two abelian groups and multiplication by an integer will stay inside this intersection. If a, b are integers such that $ab \in \mathfrak{p} \cap \mathbb{Z}$, then $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$ since $\mathfrak{p}$ is a prime ideal. Therefore $\mathfrak{p} \cap \mathbb{Z}$ is a prime ideal in $\mathbb{Z}$.

Definition 4.1. If $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ for a prime ideal $\mathfrak{p}$ and a prime number p, we say that $\mathfrak{p}$ is **above** p and, likewise, we say that p is **below** $\mathfrak{p}$.

By the second isomorphism theorem, $\mathbb{Z}/p\mathbb{Z} = \mathbb{Z}/(\mathfrak{p} \cap \mathbb{Z})$ is isomorphic to $(\mathfrak{p} + \mathbb{Z})/\mathfrak{p} \subset \mathcal{O}_K/\mathfrak{p}$. Therefore $\mathbb{F}_p$ is a subfield of $\mathbb{F}_\mathfrak{p}$ or in our new terminology $\mathbb{F}_\mathfrak{p}$ is an extension of $\mathbb{F}_p$. As both are finite sets, the dimension $f_\mathfrak{p}$ of $\mathbb{F}_\mathfrak{p}$ as a $\mathbb{F}_p$-vector space is finite.

Definition 4.2. The dimension $f_\mathfrak{p} = [\mathbb{F}_\mathfrak{p} : \mathbb{F}_p]$ is called the **residue degree** or **residue class degree** of $\mathfrak{p}$ over p.

Lemma 4.3

$\mathbb{N}(\mathfrak{p}) = p^{f_\mathfrak{p}}$.

Proof. $\mathbb{N}(\mathfrak{p}) = \#\mathbb{F}_\mathfrak{p} = (\#\mathbb{F}_p)^{f_\mathfrak{p}} = p^{f_\mathfrak{p}}$. □

Note that the prime ideals $\mathfrak{p}$ above p are exactly the prime factors $\mathfrak{p}$ of $p\mathcal{O}$, since $\mathfrak{p} \mid (p)$ is equivalent to $(p) \subset \mathfrak{p}$. This shows that there are only finitely many prime ideals $\mathfrak{p}$ above p and we can write

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_{\mathfrak{p}_1}} \cdot \mathfrak{p}_2^{e_{\mathfrak{p}_2}} \cdots \mathfrak{p}_g^{e_{\mathfrak{p}_g}}$$

for some integer $e_{\mathfrak{p}_i} \geqslant 1$.

Definition 4.4. If $\mathfrak{p}$ is a prime ideal above p, then we call $e_\mathfrak{p}$ the **ramification index** of $\mathfrak{p}$ over p. The prime $\mathfrak{p}$ is called **unramified** if $e_\mathfrak{p} = 1$ and **ramified** otherwise.

Examples.

- In the field $\mathbb{Q}(\sqrt{-5})$, we have seen that $(3) = \mathfrak{p}_1\mathfrak{p}_2$ with $\mathfrak{p}_1 = (3, 1 + \sqrt{-5})$ and $\mathfrak{p}_2 = (3, 1 - \sqrt{-5})$. This is unramified.
- Instead, in the same field, $(2) = \mathfrak{p}_3^2$ with $\mathfrak{p}_3 = (2, 1 + \sqrt{-5})$. This is ramified with index 2.
- Let p be a prime and consider $K = \mathbb{Q}(\sqrt[n]{p})$. Since $p = \alpha^n$ for some $\alpha \in \mathcal{O}$, each prime ideal above p will be ramified with index a multiple of n.

◇

Proposition 4.5

For any prime number p, we have

$$\sum_{\mathfrak{p} \text{ above } p} e_{\mathfrak{p}} \cdot f_{\mathfrak{p}} = [K : \mathbb{Q}].$$

Proof. This is the combination of

$$\mathbb{N}(p\mathcal{O}_K) = \prod_{\mathfrak{p} \text{ above } p} \mathbb{N}(\mathfrak{p})^{e_{\mathfrak{p}}} = \prod_{\mathfrak{p}} p^{f_{\mathfrak{p}}\, e_{\mathfrak{p}}} = p^{\sum_{\mathfrak{p}} f_{\mathfrak{p}}\, e_{\mathfrak{p}}}$$

and

$$\mathbb{N}(p\mathcal{O}_K) = |\mathrm{N}(p)| = p^{[K:\mathbb{Q}]}.$$ □

4.2 Explicit decomposition

We will give a recipe how to calculate the factorisation of (p) for a prime number p in one important special case.

We will suppose that we are in the monogenic situation when

$$\mathcal{O}_K = \mathbb{Z}[\alpha]$$

for a specific α. (We will weaken this hypothesis later.) This is not true for all number fields, but we know it is for quadratic and cyclotomic fields for instance. Let $f = F_\alpha \in \mathbb{Z}[X]$ be the minimal polynomial of α, which is monic of degree $d = [K : \mathbb{Q}]$. Then $\mathcal{O}_K = \mathbb{Z}[X]/(f)$. The reduced polynomial in $\mathbb{F}_p[X]$ is denoted by $\bar{f}$.

Proposition 4.6

kummer_prop

With the above notation, factor $\bar{f}$ inside $\mathbb{F}_p[X]$ completely into monic irreducible polynomials

$$\bar{f}(X) = \prod_{i=1}^{g} \bar{f}_i(X)^{e_i}$$

with $\bar{f}_i$ pairwise coprime. For each i, pick a monic polynomial $f_i \in \mathbb{Z}[X]$ reducing to $\bar{f}_i$ and of the same degree as $\bar{f}_i$. Then the ideal

$$\mathfrak{p}_i = (p, f_i(\alpha)) = p\mathcal{O}_K + f_i(\alpha)\mathcal{O}_K$$

is prime and $\prod_{i=1}^{g} \mathfrak{p}_i^{e_i}$ is the prime factorisation of (p). Moreover $f_{\mathfrak{p}_i} = \deg \bar{f}_i$.

Proof. First, for all i, we have

$$\mathcal{O}_K/\mathfrak{p}_i \cong \mathbb{Z}[X]/(f, p, f_i) \cong \mathbb{F}_p[X]/(\bar{f}_i, \bar{f}) = \mathbb{F}_p[X]/(\bar{f}_i)$$

as $\bar{f}_i$ divides $\bar{f}$. Since the ring on the right hand side is a field, the ideal $\mathfrak{p}_i$ is a prime ideal. It contains p therefore it is above p. Moreover $\mathbb{N}(\mathfrak{p}_i) = p^{\deg(\bar{f}_i)}$ shows $\deg(f_i) = f_{\mathfrak{p}_i}$.

For any $i \neq j$, we can find polynomials u and v in $\mathbb{Z}[X]$ such that $\bar{u}\bar{f}_i + \bar{v}\bar{f}_j = 1$ in $\mathbb{F}_p[X]$. Hence there is a polynomial $g \in \mathbb{Z}[X]$ such that $u\, f_i + v\, f_j = 1 + p\, g$. The ideal $\mathfrak{p}_i + \mathfrak{p}_j$ contains $u(\alpha)\, f_i(\alpha) + v(\alpha)\, f_j(\alpha) - p\, g(\alpha) = 1$ showing that $\mathfrak{p}_i \neq \mathfrak{p}_j$.

Next we calculate, first with the usual manipulations from the third isomorphism theorem, then using the Chinese remainder theorem twice:

$$\frac{\mathcal{O}}{p\mathcal{O}} \cong \frac{\mathbb{Z}[X]}{(p,f)} \cong \frac{\mathbb{F}_p[X]}{(\bar{f})} \cong \prod_{i=1}^{g} \frac{\mathbb{F}_p[X]}{(\bar{f}_i^{e_i})} \cong \prod_{i=1}^{g} \frac{\mathcal{O}}{(p, f_i(\alpha)^{e_i})} \cong \prod_{i=1}^{g} \frac{\mathcal{O}}{\mathfrak{p}^{e_i}} \cong \frac{\mathcal{O}}{\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}}.$$

In particular, this shows that $\mathbb{N}(p) = \mathbb{N}(\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g})$. But also the element $p + \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$ in the last group gets mapped under these isomorphisms to $p + p\mathcal{O} = 0$. This shows that $p \in \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$ and hence $(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$. □

Digression

```
sage: R.<X> = QQ[]
sage: K.<a> = NumberField(X^7+X+1)
sage: K.ideal(7).factor()
(Fractional ideal (a^6 - 2*a^5 + a^4 + a + 1)) * (Fractional ideal
    (-a^6 + a^2 - a)) * (Fractional ideal (-a^6 - a - 2)) *  (
    Fractional ideal (-a^6 + a^5 - a^4))
sage: [(pp.ramification_index(), pp.residue_class_degree()) for pp
    in K.primes_above(7)]
[(1, 1), (1, 2), (1, 2), (1, 2)]    # (e_p,f_p)
sage: K.discriminant().factor()
-1 * 11 * 239 * 331
sage: K.primes_above(331)
[Fractional ideal (2*a^6 - 2*a^5 + a^4 + a^3 + a + 1),
 Fractional ideal (-2*a^5 + a^4 - 4*a^3 + a^2 - 3*a + 3),
 Fractional ideal (-10*a^6 + 3*a^5 - 7*a^4 + a^3 + 3*a^2 - 7*a - 9)
    ]
sage: [(pp.ramification_index(), pp.residue_class_degree()) for pp
    in _ ]
[(2, 1), (1, 2), (1, 3)]    # (e_p,f_p)
sage: Rp.<T> = GF(331)[]    # Polynomials over F_331
sage: Rp(K.polynomial()).factor()  # factor X^7+X+1 mod 331
(T + 277)^2 * (T^2 + 188*T + 203) * (T^3 + 251*T^2 + 84*T + 80)
```

Example. Let $K = \mathbb{Q}(\sqrt[3]{2})$. For ease of notation we will write $\alpha = \sqrt[3]{2}$. It is not obvious, but one can show that $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

We will start by calculating the factorisation of $p = 5$. The minimal polynomial is $f = X^3 - 2$, which we need to factor modulo 5. Running through all values modulo 5, we find that 3 is the only root of f modulo 5. Therefore $\bar{f} = (X-3)(X^2+3X+4)$ is the complete factorisation in $\mathbb{F}_5[X]$. We find that $(5) = \mathfrak{p}_1 \cdot \mathfrak{p}_2$ with $\mathfrak{p}_1 = (5, \alpha - 3)$ and $\mathfrak{p}_2 = (5, \alpha^2 + 3\alpha + 4)$. Let us check this

$$\begin{aligned}\mathfrak{p}_1 \cdot \mathfrak{p}_2 &= (25, 5(\alpha^2+3\alpha+4), 5(\alpha-3), (\alpha-3)(\alpha^2+3\alpha+4)) \\ &= (25, 5\alpha^2+15\alpha+20, 5\alpha-15, -5\alpha-10)\end{aligned}$$

Now $5\alpha^2 + 15\alpha + 20 = -(-5\alpha - 10)(\alpha + 1) + 10$ shows that $10 \in \mathfrak{p}_1\mathfrak{p}_2$ and also $25 - 2 \cdot 10$ is in it. As all generators above are clearly multiples of 5, we find as expected $\mathfrak{p}_1 \cdot \mathfrak{p}_2 = (5)$.

This shows that the prime 5 is not ramified and $f_{\mathfrak{p}_1} = 1$ while $f_{\mathfrak{p}_2} = 2$.

Next, we want to factor $p = 3$. The polynomial factors as $X^3 - 2 = (X+1)^3$ in $\mathbb{F}_3[X]$. Therefore $(3) = \mathfrak{p}^3$ with the prime ideal $\mathfrak{p} = (3, \alpha + 1)$. This time the prime is ramified and $f_\mathfrak{p} = 1$. Note that $\mathrm{N}(\alpha+1) = 3$, which also shows that $\mathfrak{p} = (\alpha+1)$ is a principal ideal. ◇

Corollary 4.7: Dedekind–Kummer theorem

Let K be a number field and let $\alpha \in \mathcal{O}_K$. Suppose p is a prime number such that p does not divide the order of the abelian group $\mathcal{O}_K/\mathbb{Z}[\alpha]$. Then the conclusion of Proposition 4.6 still holds for the factorisation of p in $\mathcal{O}_K$.

Proof. (Sketch only) The proposition calculates $\mathbb{Z}[\alpha]/(\mathfrak{p}_i \cap \mathbb{Z}[\alpha])$. This is isomorphic to $(\mathfrak{p}_i + \mathbb{Z}[\alpha])/\mathfrak{p}_i$. The latter is a subgroup of $\mathcal{O}_K/\mathfrak{p}_i$. By assumption, the index of this subgroup is coprime to p. Since both groups are groups whose order is a power of p, the index is 1. □

4.3 Ramification

Let K be a number field of degree d. Recall the definition of the codifferent:

$$\mathfrak{d} = \delta(\mathcal{O}_K) = \left\{ \alpha \in K \;\middle|\; \mathrm{Tr}(\alpha\beta) \in \mathbb{Z} \quad \forall \beta \in \mathcal{O}_K \right\}$$

Recall that if $\alpha_1, \ldots, \alpha_d$ is an integral basis of $\mathcal{O}_K$, write T for the matrix $(\mathrm{Tr}(\alpha_i\alpha_j)_{i,j})$. This matrix is invertible; its determinant is the discriminant Δ_K of K. Then for $x_i \in \mathbb{Q}$

$$x_1\alpha_1 + \cdots + x_d\alpha_d \in \mathfrak{d} \iff T(x_1, \ldots, x_d)^\intercal \in \mathbb{Z}^d.$$

Lemma 4.8

The codifferent is a fractional ideal.

Proof. By the additivity of the trace, $\mathfrak{d}$ is an abelian subgroup of K. If $\alpha \in \mathcal{O}_K$ and $\delta \in \mathfrak{d}$, then we claim that $\alpha\delta \in \mathfrak{d}$ because for all $\beta \in \mathcal{O}_K$ we have $\mathrm{Tr}(\delta\alpha\beta) \in \mathbb{Z}$ since $\alpha\beta \in \mathcal{O}_K$.

Finally, we have seen in the proof of Theorem 2.16 that $\delta(\mathcal{O}_K)$ is a free figab group of rank d. □

By the definition $\mathcal{O}_K \subset \mathfrak{d}$. Hence $\mathfrak{d}^{-1} \subset \mathcal{O}_K$.

Definition 4.9. The inverse of the codifferent is an integral ideal $\mathcal{D}$, called the **different** of K.

Proposition 4.10

The norm of the different is the absolute value of the discriminant Δ_K.

Proof. Let $\alpha_1, \ldots \alpha_d$ be an integral basis of $\mathcal{O}_K$. Consider the map $\eta\colon K \to \mathbb{R}^d$ sending $x_1\,\alpha_1 + \cdots + x_d\alpha_d$ to $T(x_1, \ldots, x_d)^\intercal$. The image of $\mathcal{O}_K$ is exactly $T\mathbb{Z}^d$; the image of $\mathfrak{d}$ is $\mathbb{Z}^d$. By Lemma 2.4, the size of the quotient $\mathbb{Z}^d/T\mathbb{Z}^d$ is $|\det(T)|$. Therefore

$$\mathbb{N}(\mathcal{D}) = \mathbb{N}(\mathfrak{d})^{-1} = \#\mathfrak{d}/\mathcal{O} = \#\mathbb{Z}^d/T\mathbb{Z}^d = |\det(T)| = |\Delta_K|.$$ □

diff_lem

Lemma 4.11

An integral ideal I divides the different $\mathcal{D}$ if and only if $\mathrm{Tr}(I^{-1}) \subset \mathbb{Z}$.

Proof. $I \mid \mathcal{D} \iff I \supset \mathcal{D} = \mathfrak{d}^{-1} \iff \mathfrak{d} \supset I^{-1} \iff \mathrm{Tr}(I^{-1}) \subset \mathbb{Z}$. □

Theorem 4.12

If a prime ideal $\mathfrak{p}$ is ramified then it divides the different.

Proof. Write $e \geqslant 1$ for the ramification index $e_\mathfrak{p}$ and p for the prime number below $\mathfrak{p}$. There is an integral ideal I such that $(p) = \mathfrak{p}^{e-1} \cdot I$. Now I is an ideal divisible by all prime factors of (p) and exactly once by $\mathfrak{p}$. If we can prove that $\mathrm{Tr}(p^{-1}I) \subset \mathbb{Z}$, then Lemma 4.11 will tell us that $(p^{-1}I)^{-1} = pI^{-1} = \mathfrak{p}^{e-1}$ divides $\mathcal{D}$.

Let $\alpha \in I$. Write $\bar{\alpha} = \alpha + (p)$ for its residue class in $\mathcal{O}_K/p\mathcal{O}_K$. Consider the multiplication m_α by $\bar{\alpha}$ from $\mathcal{O}_K/p\mathcal{O}_K$ to itself as a $\mathbb{F}_p$-linear map. Set $\bar{t} \in \mathbb{F}_p$ to be the trace of $m_{\bar{\alpha}}$. A matrix for $m_{\bar{\alpha}}$ can be obtained by reducing the matrix for m_α written in an integral basis. Therefore $\bar{t} = \mathrm{Tr}(\alpha) + p\mathbb{Z}$.

Because all prime factors of (p) divide I, there is a power I^N of I such that $(p) \mid I^N$. Hence $\alpha^N \in (p)$. As $\bar{\alpha}^N = 0$ the map $m_{\bar{\alpha}}$ is nilpotent. Such a matrix has minimal and characteristic polynomial equal to a power of X, which shows that its trace $\bar{t}$ is zero. It follows that $\mathrm{Tr}(\alpha) \in p\mathbb{Z}$ and so $\mathrm{Tr}(p^{-1}\alpha) \in \mathbb{Z}$. □

Corollary 4.13

Only finitely many primes p have a ramified prime above them; they are among the divisors of the discriminant Δ_K.

One can push this a little further: The ramified primes are, in fact, exactly the prime divisors of the different. Our proof shows that the exponent of $\mathfrak{p}$ in the factorisation of $\mathfrak{d}$ is $e_\mathfrak{p} - 1$ unless p divides $e_\mathfrak{p}$, which is called "wild ramification".

Digression

Hilbert can be credited to connect these topics to Galois theory. Suppose $K/\mathbb{Q}$ is a Galois extension with group G and $\mathfrak{p}$ is a prime ideal above the prime number p. One can show that the ramification indices and the residue degrees are equal for all primes above p. Furthermore, there is a subgroup $D_\mathfrak{p} \leqslant G$ called the decomposition group and a smaller subgroup $I_\mathfrak{p} \leqslant D_\mathfrak{p}$ called the inertia subgroup. The order of $I_\mathfrak{p}$ is $e_\mathfrak{p}$ and the order of $D_\mathfrak{p}$ is $e_\mathfrak{p} \cdot f_\mathfrak{p}$. Frobenius constructed interesting elements in $D_\mathfrak{p}/I_\mathfrak{p}$, which are helpful for calculating Galois groups of number fields.

4.4 Real and complex embeddings

embedding_subsec

Let $K = \mathbb{Q}(\alpha)$ be a number field of degree d and let $f = F_\alpha$ be the minimal polynomial of α. Recall that $f \in \mathbb{Q}[X]$ is an irreducible polynomial.

The fundamental theorem of algebra states that f factors into linear factors in $\mathbb{C}[X]$. Consider the solutions $z_1, \ldots, z_d$ to $f = 0$ in $\mathbb{C}$. If any two roots were equal, say $z_i = z_j$,

then $f'(z_j) = 0$ and we would have a common factor between f and $f' \in \mathbb{Q}[X]$. But that is impossible as f is irreducible.

If $z_i \notin \mathbb{R}$, then the complex conjugate of z_i is also a root. We may arrange the solution such that $z_1, \ldots, z_r$ are the real solutions and $z_{r+1}, \bar{z}_{r+1}, \ldots, z_{r+s}, \bar{z}_{r+s}$ are the non-real complex roots. That is there are r real roots and s pairs of complex conjugates roots. We have $r + 2s = d$. The couple (r, s) is called the **signature** of K.

For each $0 \leqslant i \leqslant d$, we define a map $\sigma_i \colon K \to \mathbb{C}$ by

$$\sigma_i(x_0 + x_1\alpha + \cdots + x_{d-1}\alpha^{d-1}) = x_0 + x_1 z_i + \cdots + x_{d-1} z_i^{d-1}$$

with $x_0, \ldots, x_{d-1}$ in $\mathbb{Q}$.

Lemma 4.14

Tha maps $\sigma_i \colon K \to \mathbb{C}$ are injective ring homomorphism.

Proof. The evaluation-at-z_i map $\mathbb{Q}[X] \to \mathbb{C}$ is known to be a ring homomorphism. The kernel of this map consists of all polynomials g such that $g(z_i) = 0$. But these are all the multiples of $f = F_\alpha$ as that is the minimal polynomial of this algebraic number. The first isomorphism theorem gives us an injective ring homomorphism from $\mathbb{Q}(\alpha) = \mathbb{Q}[X]/(F_\alpha)$ to $\mathbb{C}$. This is the map σ_i. □

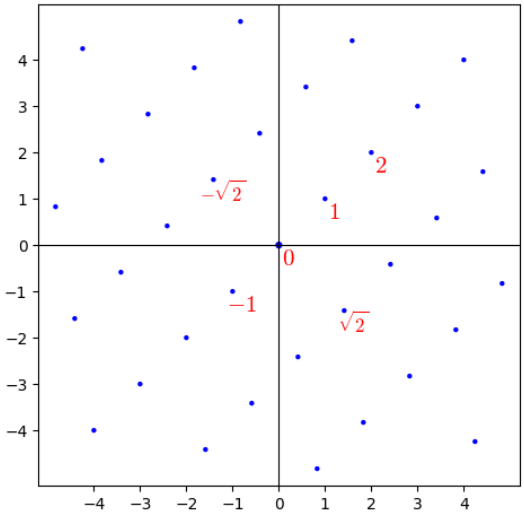
We can view the images $\sigma_i(K)$ as a concrete realisation of the abstract number field as a subfield of $\mathbb{C}$. It is not hard to show that these are actually all ring homomorphisms from K to $\mathbb{C}$.

We can put all the embeddings into one map:

$$\sigma \colon K \to \mathbb{C}^d \qquad \beta \mapsto (\sigma_1(\beta), \sigma_2(\beta), \ldots, \sigma_d(\beta))$$

Examples.

- For the real quadratic field $\mathbb{Q}(\sqrt{D})$ with a squarefree $D > 1$, we get two solutions to $X^2 - D = 0$ in $\mathbb{R}$ and so two embeddings σ_1 and σ_2. For instance, when $D = 2$, we could pick $\sigma_1(a + b\sqrt{2}) = a + 1.414\ldots b$ and $\sigma_2(a + b\sqrt{2}) = a - 1.414\ldots b$. An integer $n \in \mathbb{Z}$ is sent to (n, n), so the image of $\mathbb{Q}$ under σ lies in the diagonal of $\mathbb{R}^2$ and $n\sqrt{D}$ maps to points on the anti-diagonal $y = -x$.



- For an imaginary quadratic field, the image of σ is in $\mathbb{C}^2$. For instance for $\mathbb{Q}(i)$, the image of the rational numbers are again on the diagonal $(z,z) \in \mathbb{C}^2$, instead elements of the form $b\,i$ are sent to the line parametrised by $(z,\bar{z})$ in $\mathbb{C}^2$.
- The signature of the field $\mathbb{Q}(\sqrt[3]{7})$ is $(r,s) = (1,1)$: There is a unique real number $z_1 \approx 1.913$ whose cube is 7. The other two solutions to $X^3 - 7 = 0$ are $z_2 \approx -0.956 + 1.657\,i$ and $z_3 = \overline{z_2}$.
- The signature of the p-th cyclotomic field for an odd prime p is $r = 0$ and $s = (p-1)/2$ since there are no real roots to $X^p - 1$ other than 1.
- The minimal polynomial of $\sqrt{7-\sqrt{3}}$ is $X^4 - 14X^2 + 46$ which gives a number field of degree 4. Since $7 > \sqrt{3}$ in $\mathbb{R}$, all four solutions are in $\mathbb{R}$, namely ± 2.955 and ± 2.295. The signature is $(4,0)$.

◇

norm_emb_lem

Lemma 4.15

For all $\beta \in K$, we have

$$\mathrm{Tr}_K(\beta) = \sum_{i=1}^{d} \sigma_i(\beta) \qquad \text{and} \qquad \mathrm{N}_K(\beta) = \prod_{i=1}^{d} \sigma_i(\beta).$$

For an integral basis $\alpha_1, \ldots, \alpha_d$, set S to be the complex matrix $(\sigma_i(\alpha_j))$. Then $\det(S)^2 = \Delta_K$.

Proof. For two elements β and γ of K, we have $\sigma(\beta\gamma) = \sigma(\beta)\sigma(\gamma)$. This shows that $\sigma(m_\beta(\gamma)) = L_\beta\,\sigma(\gamma)$ where L_β is the diagonal matrix with entries $\sigma_i(\beta)$ on the diagonal. Therefore the trace and determinant of m_β are equal to the trace and determinant of L_β; this gives the formulas for $\mathrm{Tr}(\beta)$ and $\mathrm{N}(\beta)$.

The i,j-th entry of the matrix $S^\intercal S$ is equal to

$$\sum_{k=1}^{d} \sigma_k(\alpha_i)\sigma_k(\alpha_j) = \sum_{k=1}^{d} \sigma_k(\alpha_i\alpha_j) = \mathrm{Tr}(\alpha_i\alpha_j)$$

which means $S^\intercal S = T$. Therefore $\det(S)^2 = \det(S^\intercal S) = \det(T) = \Delta_K$. □

Example. Consider $K = \mathbb{Q}(\sqrt{-5})$ with the integral basis $\alpha_1 = 1$ and $\alpha_2 = \sqrt{-5}$. The two embeddings are $\sigma_1(a+\sqrt{-5}) = a + 2.236i\,b$ and $\sigma_1(a+\sqrt{-5}) = a - 2.236i\,b$. Their sum and product are $2a$ and $a^2 + 5b^2$, respectively, which we recognise as the trace and norm in this field. The matrix S is equal to

$$\begin{pmatrix} 1 & 2.236i \\ 1 & -2.236i \end{pmatrix}$$

whose determinant is $-4.472i$. Its square is indeed equal to $-20 = \Delta_{\mathbb{Q}(\sqrt{-5})}$. Note however that S does not have real or rational coefficients, while $T = S^\intercal S$ has integer coefficients. Also S and its determinant depend on the choice of the integral basis (for instance swapping 1 and $\sqrt{-5}$ changes both), while $\det(T)$ is invariant under any such change. ◇

Later, we will need a real analogue of this. Arrange the roots again so that $z_1, \ldots, z_r$ are the real roots. The maps $\sigma_1, \ldots, \sigma_r$, corresponding to the real solutions $z_1, \ldots z_r$, are called the **real embeddings** $K \to \mathbb{R}$ as their image is inside $\mathbb{R}$. The non-real

roots give s pairs of **complex embeddings** $(\sigma_{r+i}, \bar{\sigma}_{r+i})$: The embedding for the root $\bar{z}_i$ sends $\beta \in K$ to $\overline{\sigma_i(\beta)}$.

Consider the map $\tau\colon K \to \mathbb{R}^d$ given by

$$\tau(\beta) = \Big(\sigma_1(\beta), \dots, \sigma_r(\beta), \mathrm{Re}(\sigma_{r+1}(\beta)), \mathrm{Im}(\sigma_{r+1}(\beta)), \dots \mathrm{Re}(\sigma_{r+s}(\beta)), \mathrm{Im}(\sigma_{r+s}(\beta))\Big)$$

The image $\tau(\mathcal{O}_K)$ of the ring of integers is spanned by $\tau(\alpha_1)$, …, $\tau(\alpha_d)$ for an integral basis α_1, …, α_d. Write $F = \{\sum_i t_i \tau(\alpha_i) \mid 0 \leqslant t_i < 1\} \subset \mathbb{R}^d$. We call $v = \mathrm{Vol}(F)$ the covolume of $\tau(\mathcal{O}_K)$.

covol_lem

Lemma 4.16

The covolume v is equal to $2^{-s}\sqrt{|\Delta_K|}$.

Proof. The volume of F is the absolute value of the determinant of the real matrix $\tilde{S}$ whose i-th column is $\tau(\alpha_i)$ by Lemma 2.4.

Start with the matrix S from the previous proof. As we do not care about the sign, we may swap rows freely. We can assume the row i and $i+1$ contain the vectors $\sigma_i(\alpha_j)$ and $\bar{\sigma}_i(\alpha_j)$, respectively. Add row $i+1$ to row i to get $2\,\mathrm{Re}(\sigma_i(\alpha_j))$ in row i. Take away half of row i from row $i+1$ so that the latter becomes $-i\,\mathrm{Im}(\sigma_i(\alpha_j))$. Therefore $\det S = \pm(-i)^s 2^s \det \tilde{S}$. Finally $v = |\det \tilde{S}| = 2^{-s}|\det S| = 2^{-s}\sqrt{|\Delta_K|}$ by the previous lemma. □

Examples.

- The image of τ for $\mathbb{Q}(\sqrt{2})$ is the same as for σ. The set F is the parallellogramme spanned by the vectors $(1,1)$ and $(1.414, -1.414)$. Its area is equal to $2.828 = \sqrt{|\Delta_{\mathbb{Q}(\sqrt{2})}|}$.
- For the imaginary quadratic field $\mathbb{Q}(\sqrt{-5})$ instead τ and σ are different. The matrix $\tilde{S}$ is
$$\begin{pmatrix} \mathrm{Re}(1) & \mathrm{Re}(2.236i) \\ \mathrm{Im}(1) & \mathrm{Im}(2.236i) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 2.236 \end{pmatrix}.$$
The set F is the parallellogramme spanned by its column vectors; its area is equal to $2.236 = \frac{1}{2}\sqrt{|\Delta_{\mathbb{Q}(\sqrt{-5})}|}$.

◇

Digression

It may seem strange that we put prime factorisations and embeddings into one chapter, but there is a reason. In modern number theory, the embeddings are called the "primes at infinity". There is a unique prime at ∞ for $\mathbb{Q}$. In the field $\mathbb{Q}(\sqrt{2})$ this ∞ factors into two primes $\sigma_1\,\sigma_2$.

Conversely, it is also possible to view prime ideals as embeddings. Instead of sending K to real or complex fields, one embedds it into finite extensions of the p-adic numbers from [Further Number Theory]. The unifying view is given by the topological theory of absolute values $|\cdot|_{\mathfrak{p}}$ and $|\cdot|_{\sigma_1}$.

5 The class group

5.1 Ideal classes

Let K be a number field. We have seen in Theorem 3.17 that the set of non-zero fractional ideals forms an abelian group I_K under ideal multiplication.

A special subset of ideals is the set of principal ideals, i.e., fractional ideals of the form $\alpha\mathcal{O}_K$ for some $\alpha \in K^\times$. It is not hard to see that these principal ideals form a subgroup P_K of I_K.

Definition 5.1. The quotient group I_K/P_K is called the **class group** $\mathrm{Cl}(K)$ of K.

An element in this group is called an ideal class. The class containing the ideal I is denoted by $[I] = I \cdot P_K$. These are all ideals of the form αI for $\alpha \in K^\times$. Two ideal I and J are in the same class if and only if IJ^{-1} is principal.

The following result justifies why the class group measure the failure of unique factorisation in $\mathcal{O}_K$.

Proposition 5.2

The ring $\mathcal{O}_K$ admits unique factorisation of elements as products of irreducible elements (ufd) if and only if $\mathrm{Cl}(K)$ is trivial (pid).

Recall that, in a unique factorisation domain (ufd), the factorisation into irreducible elements is up to reordering and two irreducibles are not distinguished if their fraction is a unit.

Proof. $\Leftarrow$: Let $\alpha \in \mathcal{O}_K$. Factor (α) into a product of prime ideals by Theorem 3.18. By assumption all these prime ideals are principal and we can pick a generator for each of them. Therefore $(\alpha) = \prod_{i=1}^m (\pi_i)$ with not necessarily distinct prime ideals (π_i). The elements π_i must be irreducible as otherwise (π_i) cannot be prime. We find a unit $u \in \mathcal{O}_K$ and $\alpha = u \cdot \prod_{i=1}^m \pi_i$ shows that α can be factored into irreducibles. Since the factorisation into prime ideals is unique, this factorisation into irreducibles is also unique.

$\Rightarrow$: Let I be an integral ideal and let $0 \neq \alpha \in I$. By assumption $\alpha = \prod_i \pi_i$ for irreducible elements π_i. Again the ideals $\mathfrak{p}_i = (\pi_i)$ must be prime ideals as otherwise we could factor the element π_i. Since $I \mid (\alpha) = \prod_i \mathfrak{p}_i$, the ideal I is a product of some of these prime ideals; but since they are principal so is I. □

5.2 Geometry of numbers

The "geometry of numbers" is a topic in euclidean geometry which is useful in number theory.

We first need a few definitions. Recall that a subset of $\mathbb{R}^n$ is **compact** if it is bounded and closed in the real topology. We say that a subset X is **symmetric with respect to 0** if $\mathbf{x} \in X$ implies $-\mathbf{x} \in X$. Finally a set $X \subset \mathbb{R}^n$ is **convex** if, for any $\mathbf{x}, \mathbf{y} \in X$ the segment $\{t\mathbf{x} + (1-t)\mathbf{y} \mid 0 \leqslant t \leqslant 1\}$ also belongs to X.

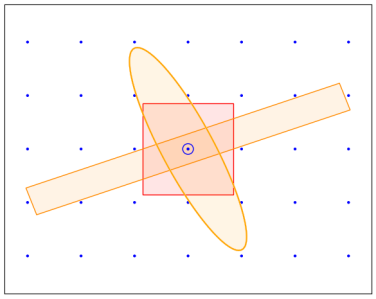
Examples.

- The set $\{(x_1, \ldots, x_n) \in \mathbb{R}^n \mid -1 \leqslant x_i \leqslant 1 \ \forall i\}$ is a (hyper)-cube that is compact, convex and symmetric with respect to $\mathbf{0}$.
- The closed ball of radius $r > 0$ is another example. That stays true even if we take a non-standard metric in $\mathbb{R}^n$, like the set $\{(x_1, \ldots, x_n) \in \mathbb{R}^n \mid \sum_i |x_i| \leqslant r\}$.

$\diamond$

A **lattice** $A \subset \mathbb{R}^n$ is a figab group that contains a basis of $\mathbb{R}^n$. Suppose A is generated by the basis $\mathbf{a}_1, \ldots, \mathbf{a}_n$ The fundamental domain $F = \{\sum x_i \mathbf{a}_i \mid 0 \leqslant x_i < 1\} \subset \mathbb{R}^n$ contains exactly one element of each coset of $\mathbb{R}^n/A$ as seen in the proof of Lemma 2.4. coker_det_lem We call $\mathrm{coVol}(A) := \mathrm{Vol}(F)$ the **covolume** of A.

We try to fit a large convex, symmetric set X around $\mathbf{0}$ in such a way as not to contain any non-zero elements of A. As in the picture with $A = \mathbb{Z}^2 \subset \mathbb{R}^2$.



minkowski_lem

Lemma 5.3

Let A be a figab subgroup of $\mathbb{R}^n$ containing a basis of that vector space and let X be a compact, convex subset of $\mathbb{R}^n$ which is symmetric with respect to $\mathbf{0}$. If $\mathrm{Vol}(X) > 2^n \cdot \mathrm{coVol}(A)$, then X contains a non-zero element from A.

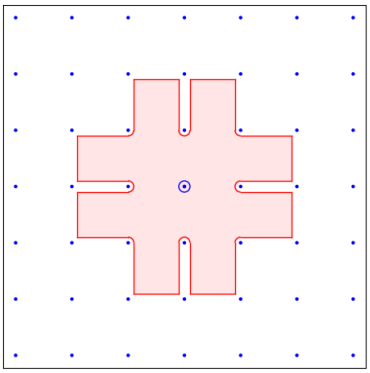
Proof. Let $\frac{1}{2}X$ denote the set $\{\mathbf{x}/2 \mid \mathbf{x} \in X\}$. Consider the map $\Phi\colon \frac{1}{2}X \to \mathbb{R}^n/A$ sending $\mathbf{x}/2$ to its coset $\mathbf{x}/2 + A$. If Φ were injective then

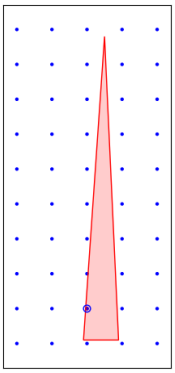
$$\mathrm{coVol}(A) = \mathrm{Vol}(F) \geqslant \mathrm{Vol}(\tfrac{1}{2}X) = \frac{1}{2^n}\mathrm{Vol}(X)$$

which contradicts the assumption.

Since Φ is not injective, there exists $\mathbf{x} \neq \mathbf{y} \in X$ such that $\mathbf{x}/2 + A = \mathbf{y}/2 + A$. By symmetry of X, the vector $-\mathbf{y}$ is also in X. As X is convex, the point $\frac{1}{2}\mathbf{x} + \frac{1}{2}(-\mathbf{y}) \in X \cap A$. $\square$

The following two pictures should convince you that the conditions "convex" and "symmetric" are needed for the conclusion to hold.





5.3 Finiteness of the class group

bounded_ideals_lem

Lemma 5.4

Given $B > 0$, there are only finitely many integral ideals I with $\mathbb{N}(I) < B$.

Proof. It is enough show that there are only finitely many ideals I with $\mathbb{N}(I) = n$ for any $n > 0$. If I is such an ideal, then, by definition $\#\mathcal{O}_K/I = n$. By Lagrange's Theorem, $n \cdot (1 + I) = 0 + I$ and this shows that $n \in I$. Thus $I \mid (n)$. But there are only finitely many divisors of the ideal (n). □

class_group_thm

Theorem 5.5

Let K be a number field. The class group $\mathrm{Cl}(K)$ is finite.

Proof. Let I be a fractional ideal. We aim to find an integral ideal in the same class as I with small norm. Such an ideal is of the form αI and we look for an $\alpha \in K^\times$. To make αI integral means $\alpha \in I^{-1}$.

We start by picking $\varepsilon > 0$ and picking a convex, compact set Y which is symmetric with respect to $\mathbf{0}$. Write A for the image of $\mathcal{O}_K$ under the map $\tau\colon K \to \mathbb{R}^d$ from Section 4.4. Lemma 4.16 shows that A is a lattice as its covolume is $v > 0$. Write B for the image of I^{-1}. Since $B/A \cong I^{-1}/\mathcal{O}_K \cong \mathcal{O}_K/I$ has $\mathbb{N}(I)$ elements, we have $\mathrm{coVol}(B) \cdot \mathbb{N}(I) = v$. Let

$$\lambda = (2+\varepsilon) \cdot \sqrt[d]{\frac{\mathrm{coVol}(B)}{\mathrm{Vol}(Y)}}$$

and use if to scale $X = \lambda Y$, which is still convex, compact and symmetric. By construction

$$\mathrm{Vol}(X) = \lambda^d \cdot \mathrm{Vol}(Y) = (2+\varepsilon)^d \cdot \mathrm{coVol}(B) > 2^d \cdot \mathrm{coVol}(B)$$

and this allows us to apply Lemma 5.3. This guarantees the existence of $\mathbf{0} \neq \mathbf{x} \in X \cap B$. As it is in B there is an α in I^{-1} with $\mathbf{x} = \sigma(\alpha)$.

Let $\tilde{\mathrm{N}}\colon \mathbb{R}^d \to \mathbb{R}$ be the function defined by

$$\tilde{\mathrm{N}}(\mathbf{x}) = x_1 \cdot x_2 \cdots x_r \cdot (x_{r+1}^2 + x_{r+2}^2) \cdot (x_{d-2}^2 + x_{d-1}^2).$$

It satisfies $\tilde{\mathrm{N}}(\lambda \mathbf{y}) = \lambda^d \tilde{\mathrm{N}}(\mathbf{y})$. As $\alpha \in K$, then Lemma 4.15 says that

$$\mathrm{N}(\alpha) = \prod_{i=1}^{d} \sigma_i(\alpha) = \tau_1(\alpha) \cdot \tau_2(\alpha) \cdots \tau_r(\alpha) \cdot |\sigma_{r+1}(\alpha)|^2 \cdots |\sigma_{r+s}(\alpha)|^2 = \tilde{\mathrm{N}}(\tau(\alpha)) = \tilde{\mathrm{N}}(\mathbf{x}).$$

The function $|\tilde{N}|$ must have a maximum M on the compact set Y.

$$\begin{aligned} \mathbb{N}(\alpha I) =& |\mathrm{N}(\alpha)| \cdot \mathbb{N}(I) = \lambda^d \cdot |\tilde{N}(\mathbf{x}/\lambda)| \cdot \mathbb{N}(I) \\ &\leqslant (2+\varepsilon)^d \cdot \frac{\mathrm{coVol}(B)}{\mathrm{Vol}(Y)} \cdot M \cdot \mathbb{N}(I) = (2+\varepsilon)^d \cdot \frac{M}{\mathrm{Vol}(Y)} \cdot v \end{aligned}$$

This final expression does no longer depend on I, only on Y and ε.

Therefore each ideal class contains at least one integral ideal of norm bounded by that constant. By Lemma 5.4 there are only finitely many such ideals. □

Definition 5.6. The order of $\mathrm{Cl}(K)$ is called the **class number** h_K of K.

5.4 Explicit calculation

Theorem 5.5 proves that $\mathrm{Cl}(K)$ is finite. We can turn the proof into an actual algorithm to calculate this group and its order.

Two steps will be needed. First, we need an explicit bound B such that all ideal classes contain an integral ideal of norm less than B. The second step is to find all ideals below this bound and to understand which are principal.

The proof of the theorem showed that we can take

$$B = 2^d \frac{M}{\mathrm{Vol}(Y)} \cdot v = 2^{r+s} \frac{M}{\mathrm{Vol}(Y)} \cdot \sqrt{|\Delta_K|}.$$

Well, the proof had an $\varepsilon > 0$ in it, too, but since the statement holds for all $\varepsilon > 0$ we may ignore it.

The factor $M/\mathrm{Vol}(Y)$ depends on the choice of Y. We get a better bound the larger we can make Y while keeping $M = \max_{\mathbf{y}\in Y} |\tilde{N}(\mathbf{y})|$. Therefore a good choice of Y is a convex set of maximal volume inside the set defined by $\tilde{N}(\mathbf{x}) \leqslant 1$.

A good choice for a general number field is the set of all $\mathbf{x} \in \mathbb{R}^d$ satisfying

$$|x_1| + |x_2| + \cdots + |x_r| + 2\sqrt{x_{r+1}^2 + x_{r+2}^2} + \cdots + 2\sqrt{x_{d-2}^2 + x_{d-1}^2} \leqslant 1.$$

It can be shown that this is convex and that $M = d^{-d}$ using the inequality between the geometric and arithmetic means. The tedious calculation of the volume of this set is left to the ones with an interest in multiple integrals. The result from this choice is the so-called Minkowski bound:

$$B = \left(\frac{4}{\pi}\right)^s \frac{d!}{d^d} \sqrt{|\Delta_K|}$$

The second task is to enumerate all ideals of norm less than B. For this it is sufficient to find all prime ideals of norm less than B, which can be obtained by factoring all $p\mathcal{O}_K$ for prime numbers below p. Once we have the list, we need to determine for each ideal if it is principal and, if not, if it belongs to a class of an ideal that we have found earlier.

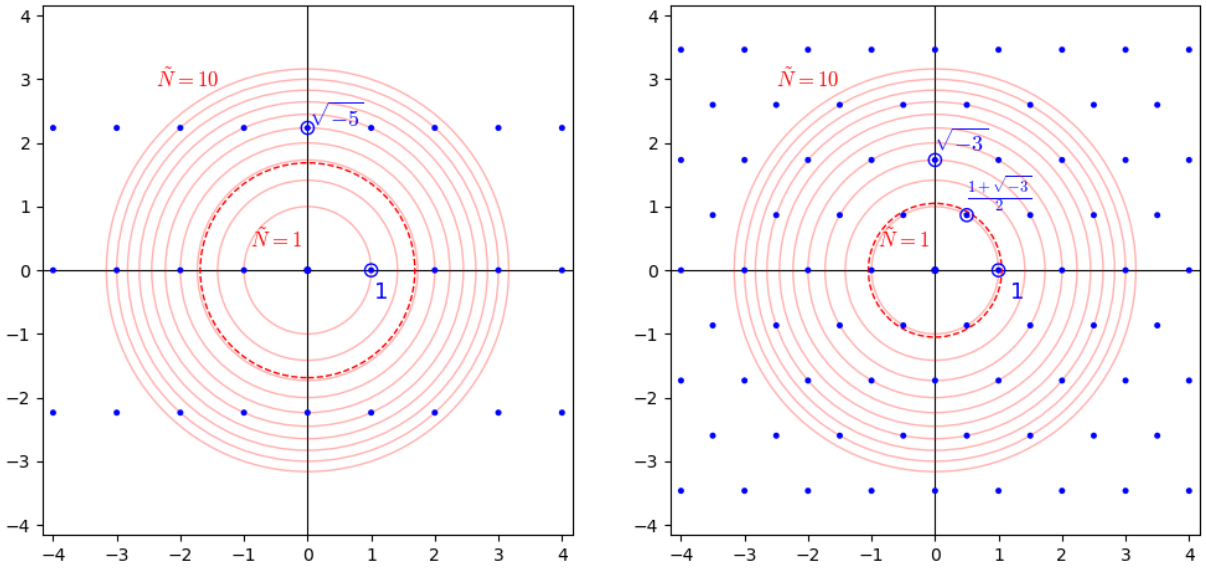
5.4.1 Example of an imaginary quadratic field

We return to our favourite example $K = \mathbb{Q}(\sqrt{-5})$. The ring of integers is $\mathbb{Z}[\sqrt{-5}]$ and the discriminant is -20. We have seen that covolume is $v = \sqrt{5} \approx 2.236$. As Y we take the circle of radius 1; it has volume π. The function $\tilde{N}$ is $\tilde{N}(x, y) = x^2 + y^2$. Therefore the maximum M is exactly 1 and we see that our choice of Y is optimal. The bound is

$$B = 2^2 \frac{1}{\pi} \sqrt{5} \approx 2.847.$$

As a result, we only have to look for ideals of norm at most 2. There is a unique ideal of norm 1, namely $\mathcal{O}_K$ and that represents the trivial class in the class group. We factored (2) already as $(2) = \mathfrak{p}^2$ with $\mathfrak{p} = (2, 1 + \sqrt{-5})$. Therefore $\mathfrak{p}$ is the unique ideal of norm 2. We have already seen that this ideal cannot be principal. It is of order 2 in the class group as $\mathfrak{p}^2$ is principal. Conclusion: $\mathrm{Cl}(\mathbb{Q}(\sqrt{-5}))$ is a cyclic group of order 2.

In general, for an imaginary quadratic number field, the method above gives the Minkowski bound of $B = \frac{2}{\pi}\sqrt{|\Delta_K|}$. This is equal to $4/\pi\sqrt{-D}$ if $D \equiv 2$ or 3 modulo 4 and equal to $2/\pi\sqrt{-D}$ id $D \equiv 1 \pmod 4$.



These two pictures represent the case $\mathbb{Q}(\sqrt{-5})$ discussed before and the case $\mathbb{Q}(\sqrt{-3})$. The dotted circle is the limit given by the Minkowski bound.

Digression

It was already conjectured by Gauss that there are only finitely many imaginary quadratic fields with class number 1: Namely $\mathbb{Q}(\sqrt{-D})$ for D in the list 1, 2, 3, 7, 11, 19, 43, 67, and 163. This was proven by Heegner (though that proof was only accepted after rework by Birch and Stark) using elliptic curves and by Baker using transcendence theory.

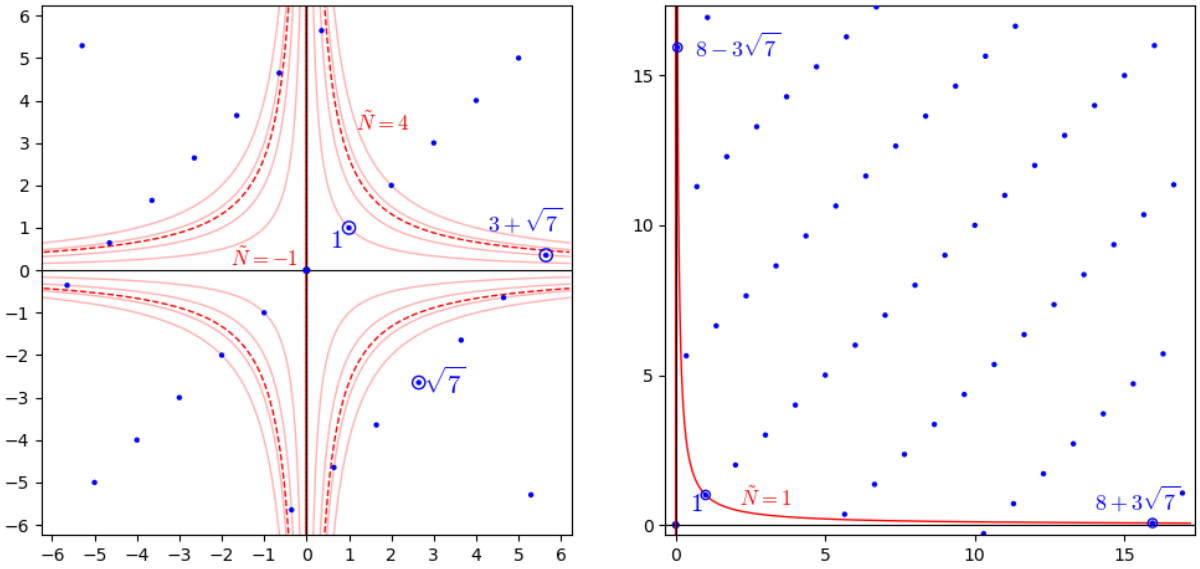
D	1	2	3	5	6	7	10	11	13	14	15	17	19	21	22
$h_{\mathbb{Q}(\sqrt{-D})}$	1	1	1	2	2	1	2	1	2	4	2	4	1	4	2
D	23	26	29	30	31	33	34	35	37	38	39	41	42	43	46
$h_{\mathbb{Q}(\sqrt{-D})}$	3	6	6	4	3	4	4	2	2	6	4	8	4	1	4

5.4.2 Example of a real quadratic field

Let us take $K=\mathbb{Q}(\sqrt{7})$. The ring of integers is $\mathbb{Z}[\sqrt{7}]$ with discriminant $\Delta_K=28$. Write $\sqrt{7.}\approx 2.646>0$ for the unique positive real square root of 7. The map τ sends $a+b\sqrt{7}$ to $(a+b\sqrt{7.}, a-b\sqrt{7.})$. The covolume is $v=\sqrt{28}=2\sqrt{7.}$ The extended norm map is now $\tilde{N}(x,y)=x\cdot y$. The set of points with $|\tilde{N}(x,y)|=1$ is now formed by two hyperbolas going through $(1,1)$. The largest convex set Y inside is the slanted square of points (x,y) such that $|x|+|y|\leqslant 2$. The volume of Y is 8 and $M=1$. The bound is therefore $B=2^2\frac{1}{8}2\sqrt{7.}=\sqrt{7.}\approx 2.646$.

Again, we only have to look for ideals of norm 2. If we will find a principal ideal of norm 2, then its generator α will have norm 2. This means $\alpha=a+b\sqrt{7}$ with $\mathrm{N}(\alpha)=a^2-7b^2=2$. Luckily we can spot a solution $a=3$ and $b=1$. Therefore $\mathfrak{p}=(3+\sqrt{7})$ is an ideal of norm 2. However $\alpha^2=16+6\sqrt{7}=2(8+3\sqrt{7})$ and $\mathrm{N}(8+3\sqrt{7})=64-9\cdot 7=1$ shows that $8+3\sqrt{7}$ is a unit. Therefore $\mathfrak{p}^2=(2)$ and we have already the full factorisation of (2). We can conclude that the class number of K is 1.

In general for real quadratic fields, the above slanted square gives the Minowski bound of $B = \frac{1}{2}\sqrt{\Delta_K}$.



Digression

Unlike for the imaginary case where the class numbers grow (slowly) with $|\Delta_K|$, the class numbers of real quadratic fields stay much smaller. Yet, it is not know if there are infinitely many real quadratic fields with class number 1.

D	2	3	5	6	7	10	11	13	14	15	17	19	21	22	23
$h_{\mathbb{Q}(\sqrt{D})}$	1	1	1	1	2	1	1	1	2	1	1	1	1	1	2
D	26	29	30	31	33	34	35	37	38	39	41	42	43	46	47
$h_{\mathbb{Q}(\sqrt{D})}$	1	1	2	1	1	2	2	1	1	2	1	2	1	1	1

5.4.3 Example for cyclotomic fields

To show that these calculations very soon fail to be practical, consider the field $K = \mathbb{Q}(\zeta_{23})$, the 23-rd cyclotomic field. The ring of integers is $\mathbb{Z}[\zeta_{23}]$ and the discriminant is $\Delta_K = -23^{21}$. The Minkowski bound evaluates to $B = 9324406.48$, which leaves us factoring more than a quarter of a million primes. The computer can still do this and produce the result $h_K = 3$. A generator for the class group is given by the prime ideal $\mathfrak{p} = (47, \zeta_{23} - 21)$ of norm 47.

p	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53
$h_{\mathbb{Q}(\zeta_p)}$	1	1	1	1	1	1	1	3	8	9	37	121	211	655	4889
p	59		61		67		71		73		79		83		
$h_{\mathbb{Q}(\zeta_p)}$	41241		76301		853513		3882809		11957417		100146415		13379363737		

Digression

Already Kummer found a surprising link between the class number of cyclotomic fields and Bernoulli numbers. For instance, he showed that p divides the class number of $\mathbb{Q}(\zeta_p)$ if and only if a Bernoulli numbers B_{2k} with $1 \leqslant k \leqslant (p-3)/2$ has its numerator divisible by p. The first p with this property is $p = 37$ where $B_{32} = -37 \cdot 208360028141/510$ and $h_{\mathbb{Q}(\zeta_{37})} = 37$. Iwasawa found an even deeper connection between these class groups and the values of the Riemann zeta function, which is now part of Iwasawa Theory.

5.5 Examples of diophantine equations

An important application of algebraic number theory concerns diophantine equations, i.e., the resolution of polynomial equations in integer variables. A first example in [Further Number Theory] uses the unique factorisation in the Gaussian integers $\mathbb{Z}[\sqrt{-1}]$ to explain which prime are the sum of two squares. Deliberately, we pick two rather more difficult examples to illustrate the power of the method.

Theorem 5.7

ell_thm

The only integer solutions to $y^2 = x^3 - 13$ are $(x, y) = (17, 70)$ and $(17, -70)$.

For those who studied [Elliptic Curves] they will know this as such a curve. The set of rational solution is infinite; for instance

$$\left(\tfrac{85289}{19600},\ \pm\tfrac{22858837}{2744000}\right) \quad \text{and} \quad \left(\tfrac{148751276257}{61459863921}, \pm\tfrac{16535372234548510}{15236576324519031}\right)$$

are the next smallest such solutions.

Crucial for the proof of the theorem is the following fact.

Lemma 5.8

The class group of $\mathbb{Q}(\sqrt{-13})$ is cyclic of order 2.

Proof. The Minkowski bound is $4\sqrt{13}/\pi \approx 4.59$. We need to factor the primes 2 and 3 only. First $(2) = \mathfrak{p}^2$ with $\mathfrak{p} = (2, 1 + \sqrt{-13})$. If $\mathfrak{p}$ were principal, we could find $a, b \in \mathbb{Z}$ with $a^2 + 13b^2 = \pm 2$. The negative sign is impossible as the left hand side is non-negative. Then $b = 0$ as otherwise the left hand side would be too big. However $a^2 = 2$ has no solution in $\mathbb{Z}$.

The ideal (3) is a prime ideal and it is principal. Therefore we have shown the lemma. □

Proof of Theorem ell_thm *5.7.* Let (x, y) be an integral solution to $y^2 = x^3 - 13$.

Suppose y is odd. Then $x^3 = y^2 + 13 \equiv 1 + 13 \equiv 2 \pmod 4$. But that is impossible as it would imply that x is even and then $x^3 \equiv 0 \pmod 4$. Hence y is even.

Suppose y is divisible by 13. Then 13 divides $y^2 = x^3 - 13$; this implies that $13 \mid x$. This gives a contradiction as 13^2 will divide y^2 while $x^3 - 13 \equiv -13 \pmod{13^2}$. Hence 13 does not divide y.

Now write

$$x^3 = y^2 + 13 = (y - \sqrt{-13}) \cdot (y + \sqrt{-13}).$$

Let I be the ideal $(y+\sqrt{-13})$ and $J=(y-\sqrt{-13})$ in $\mathbb{Z}[\sqrt{-13}]$. We wish to show that I and J are coprime. First $2\sqrt{-13}$ belongs to $I+J=(y+\sqrt{-13}, y-\sqrt{-13})$ as it is the difference of the two generators. Therefore $I+J$ divides $(\sqrt{-13})\mathfrak{p}^2$ with $\mathfrak{p}=(2,1+\sqrt{-13})$. Since y is even $y+\sqrt{-13}$ does not belong to $\mathfrak{p}$, which shows that $\mathfrak{p}$ does not divide $I+J$. Since y is not divisible by 13, the element $y+\sqrt{-13}$ is not in $(\sqrt{-13})$. Hence $I+J=\mathbb{Z}[\sqrt{-13}]$.

If the prime ideal factorisation of (x) is $\mathfrak{p}_1^{a_1}\cdot\mathfrak{p}_g^{a_g}$, then $IJ=(x)^3=\mathfrak{p}_1^{3a_1}\cdots\mathfrak{p}_g^{3a_g}$. As I and J are coprime, $I=I'^3$ for some ideal $I'\mid(x)$. If I' were non-principal, its class would have order 2, so $[I']=[I']^3=[I]$ but I is principal. Hence I' is principal, say $I'=(a+b\sqrt{-13})$.

The only units in the ring $\mathbb{Z}[\sqrt{-13}]$ are 1 and -1. We have

$$\pm1\cdot(a+b\sqrt{-13})^3=y+\sqrt{-13}$$

for some integers a and b. Expanding the left hand side we obtain two equations:

$$\begin{aligned}\pm(a^3-3\cdot13\,ab^2)&=y\\ \pm(3\,a^2b-13\,b^3)&=1\end{aligned}$$

The second equation implies that $b=\pm1$ since it is a factors as $b(3a^2-13b^2)=\pm1$. This equation becomes $3a^2-13=\pm1$. Since 14 is not divisible by 3, it must be $3a^2=12$ and therefore $a=\pm2$. The first of the two equation above now shows $y=\pm a(a^2-39b^2)=\pm2(4-39)=\pm70$. Then $x^3=70^2+13=17^3$ which concludes the proof. □

quad_thm

Theorem 5.9

There are no integer solutions to $x^2-79y^2=-3$.

Again this equation has plenty of rational solutions, like $(x,y)=(\frac{4}{5},\frac{1}{5})$ and $(289,\frac{2}{3})$. From [Elliptic Curves] or [Algebraic Geometry] you might know to parametrise all rational solutions on that conic. A consequence of this, the equation has solutions modulo every integer $m>1$. This is why this is not so easy to solve.

Proof. Suppose there exists an integral solution (x,y). The equation can be written as $\mathrm{N}(x+y\sqrt{79})=-3$ with the norm from the field $\mathbb{Q}(\sqrt{79})$. Therefore $x+y\sqrt{79}$ is a generator of an ideal of norm 3. The factorisation of (3) is $\mathfrak{pq}$ with $\mathfrak{p}=(3,1+\sqrt{79})$ and $\mathfrak{q}=(3,1-\sqrt{79})$. By changing the sign of y if necessary, we may assume that $x+y\sqrt{79}$ generates $\mathfrak{p}$.

Consider $\beta=17+2\sqrt{79}$. Its norm is $\mathrm{N}(\beta)=17^2-4\cdot79=-27$. Since $\beta=5\cdot3+2\cdot(1+\sqrt{79})$ it belongs to $\mathfrak{p}$, but $\beta\equiv17+2\equiv1\pmod{\mathfrak{q}}$ shows that it is not in $\mathfrak{q}$. We conclude that $(\beta)=\mathfrak{p}^3$.

There is a unit $\varepsilon\in\mathcal{O}^\times$ such that

$$(x+y\sqrt{79})^3=\varepsilon\cdot(17+2\sqrt{79}).\qquad(\text{🌥})$$ daggereq

We have to determine the units in our ring. Searching for a and b between -100 and 100, the only solution to $a^2-79b^2=\pm1$ are those corresponding to ±1 and $\pm80\pm9\sqrt{79}$. Let $\eta=80+9\sqrt{79}\in\mathcal{O}^\times$; then $\eta^{-1}=80-9\sqrt{79}$.

Next we consider the composite map

$$\lambda\colon\ \mathbb{Q}(\sqrt{79})^\times \xrightarrow{\ \sigma\ } \mathbb{R}^\times \times \mathbb{R}^\times \xrightarrow{(x,y)\mapsto(\log|x|,\log|y|)} \mathbb{R}^2$$

where σ is given by the two real embeddings $\sigma = (\sigma_1, \sigma_2)$. As σ is a ring homomorphism, $|\cdot|$ is multiplicative and $\log$ of a product is the sum of the logs, this map λ is a group homomorphism from the multiplicative group $\mathbb{Q}(\sqrt{79})^\times$ to the additive group $\mathbb{R}^2$. The unit group $\mathcal{O}^\times$, consisting exactly of the elements of norm 1 in $\mathcal{O}$, is first sent by σ into the hyperbolas given by $xy = \pm 1$ and then by the logarithmic map to the line $x + y = 0$. The image $\lambda(\mathcal{O}^\times)$ is a subgroup contained in this line $y = -x$. On this line we know the image of $\pm 1 \in \mathcal{O}^\times$, which is $\lambda(1) = (0, 0)$, and the images of η and η^{-1}, which are roughly at $(5.075, -5.075)$ and $(-5.075, 5.075)$. From our systematic search, we can deduce that there are no other images of $\mathcal{O}^\times$ between the point $\lambda(\eta)$ and $\lambda(1)$. Therefore, $\lambda(\mathcal{O}^\times)$ is the cyclic group generated by $\lambda(\eta)$. We can deduce that

$$\mathcal{O}^\times = \Big\{(-1)^v \cdot \eta^n \ \Big|\ n \in \mathbb{Z},\ v \in \{0, 1\}\Big\}.$$

The unit ε in equation (daggereq) must be of that form. Since $-1 = (-1)^3$, we can change the sign of our unknown x and y to reduce to the case that $\varepsilon = \eta^n$ for some integer n. Further we can divide $x + y\sqrt{79}$ by ε or its inverse to reduce to the case that n is either 1, 0 or -1.

First case $n = 0$: this gives $(x + y\sqrt{79})^3 = 17 + 2\sqrt{79}$. Expanding the cube, we obtain two equations:

$$x^3 + 3 \cdot 79\, xy^2 = 17$$
$$3\, x^2 y + 79\, y^3 = 2$$

The first equation tells us that x divides 17, which means $x = \pm 1$ or $x = \pm 17$, and the second that y divides 2, giving $y = \pm 1$ or ± 2. This leaves 16 cases to check. However the values of $\mathrm{N}(x + y\sqrt{79})$ for them are -315, -78, -27, or 210. Therefore there are no solutions in this first case.

The second case is

$$(x + y\sqrt{79})^3 = (80 + 9\sqrt{79})(17 + 2\sqrt{79}) = 2782 + 313\sqrt{79}.$$

The same expansion as in the first case, gives us that y divides 313 and x divides 2782. Now there are 64 cases resulting in 16 different norm but all far away from the desired -3.

The final case is $(x + y\sqrt{79})^3 = (80 - 9\sqrt{79})(17 + 2\sqrt{79}) = -62 + 7\sqrt{79}$. This time x divides -62 and y divides 7. Once again none of the 32 possibilities for (x, y) give an element of norm -3.

Therefore there are no integer solutions to the equation $x^2 - 79y^2 = -3$. □

Proposition 5.10

The class group of $\mathbb{Q}(\sqrt{79})$ is cyclic of order 3 and the unit group is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$ with generators -1 and $\eta = 80 + 9\sqrt{79}$.

Proof. The statement about the units was part of the proof of the previous theorem.

The Minkowski bound for this field is about 8.89. We have already factored the ideal (3) and found two primes $\mathfrak{p}$ and $\mathfrak{q}$. A generator must have norm ± 3. In the previous theorem, we have ruled out -3. Note that $x^2 - 79y^2 = 3$ has no solution modulo 4, which excludes also generators of norm $+3$. Therefore $\mathfrak{p}$ and $\mathfrak{q}$ are non-principal ideals. Since $\mathfrak{p}^3$ is principal, $[\mathfrak{p}]$ and $[\mathfrak{q}] = [\mathfrak{p}]^{-1} = [\mathfrak{p}]^2$ are two elements of order 3 in the class group.

Our aim now is to factor also the other small primes and check that we do not find any new classes. Writing $\alpha = \sqrt{79}$, the factorisations are

p	2	3	5	7
(p)	$(2, 1+\alpha)^2$	$(3, 1+\alpha)(3, 1-\alpha)$	$(5, 2+\alpha)(5, 2-\alpha)$	$(7, 3+\alpha)(7, 3-\alpha)$

To find possible generators, we best calculate plenty of norms $a^2 - 79b^2$ of elements with small coordinates:

$a \setminus b$	1	2	3
1	$-2 \cdot 3 \cdot 13$	$-3^2 \cdot 5 \cdot 7$	$-2 \cdot 5 \cdot 71$
2	$-3 \cdot 5^2$	$-2^3 \cdot 3 \cdot 13$	$-7 \cdot 101$
3	$-2 \cdot 5 \cdot 7$	-307	$-2 \cdot 3^3 \cdot 13$
4	$-3^2 \cdot 7$	$-2^2 \cdot 3 \cdot 5^2$	$-5 \cdot 139$
5	$-2 \cdot 3^3$	$-3 \cdot 97$	$-2 \cdot 7^3$
6	-43	$-2^3 \cdot 5 \cdot 7$	$-3^3 \cdot 5^2$
7	$-2 \cdot 3 \cdot 5$	$-3 \cdot 89$	$-2 \cdot 331$
8	$-3 \cdot 5$	$-2^2 \cdot 3^2 \cdot 7$	-647
9	2	$-5 \cdot 47$	$-2 \cdot 3^2 \cdot 5 \cdot 7$
10	$3 \cdot 7$	$-2^3 \cdot 3^3$	$-13 \cdot 47$
11	$2 \cdot 3 \cdot 7$	$-3 \cdot 5 \cdot 13$	$-2 \cdot 5 \cdot 59$
12	$5 \cdot 13$	$-2^2 \cdot 43$	$-3^4 \cdot 7$
13	$2 \cdot 3^2 \cdot 5$	$-3 \cdot 7^2$	$-2 \cdot 271$
14	$3^2 \cdot 13$	$-2^3 \cdot 3 \cdot 5$	$-5 \cdot 103$
15	$2 \cdot 73$	$-7 \cdot 13$	$-2 \cdot 3^5$

One spots here that the element $9 + \sqrt{79}$ has norm 2, which means that the unique prime ideal $(2, 1 + \sqrt{79})$ above 2 must be principal.

Then the element $2 + \sqrt{79}$ has norm $-3 \cdot 5^2$. As it is not divisible by 5, the ideal $(2 + \sqrt{79})$ must factor into a prime above 3 times the square of a prime $\mathfrak{q}_5$ above 5. As a consequence $\mathfrak{q}_5$ cannot be principal, but it lies in either the class $[\mathfrak{p}]$ or $[\mathfrak{p}]^2$. It follows that both ideals above 5 are non-principal ideals in either $[\mathfrak{p}]$ or $[\mathfrak{p}]^2$.

The same argument can be used with $4 + \sqrt{79}$, which generates an ideal that factors into a square of an ideal above 3 times and ideal above 7. Therefore also the two ideal above 7 are non-principal, but already in one of the two classes discovered before.

This now proves that the class group of K is $\{[1],\ [\mathfrak{p}],\ [\mathfrak{p}]^2\}$. □

From looking at the table above, one can deduce further interesting information. For instance $5 + \sqrt{79}$ divided by $9 + \sqrt{79}$ will be an element of norm 27; it is $-17 + 2\sqrt{79}$, which how the element used in the proof of Theorem 5.9 was found. Given that there are plenty of elements in this list whose norm has only prime factors below 10, we can find further relations. For instance $(9 + \sqrt{79}) \cdot (10 + \sqrt{79})/(11 - \sqrt{79})$ is an element of norm 1; since it is equal to $80 + 9\sqrt{79}$, which is in $\mathcal{O}$, we have found a unit.

The hard work to show that the class group was non-trivial happened in Theorem quad_thm 5.9. This cannot be avoided: Any non-principal ideal, like $(5, 2+\sqrt{79})$ gives rise to a diophantine equation which is hard to solve, like $x^2 - 79y^2 = 5$.

Digression

The map λ in the proof of Theorem quad_thm 5.9 is used for all number fields to determine the group of units $\mathcal{O}_K^\times$. The result is known as Dirichlet's unit theorem which states that this group is a figab group isomorphic to a finite group times $r+s-1$ copies of $\mathbb{Z}$. Kummer recounted that Dirichlet found the idea to the proof of this fundamental theorem during a concert in the Sistine Chapel.

5 References

baker [1] Alan Baker. *Transcendental number theory*. Cambridge Math. Library. George Green Library QA247.5 BAK. Cambridge University Press, Cambridge, 2022, p. 169.

cohen [2] Henri Cohen. *A course in computational algebraic number theory*. Vol. 138. Graduate Texts in Mathematics. George Green Library QA247 COH. Springer-Verlag, Berlin, 1993, p. 534.

marcus [3] Daniel A. Marcus. *Number fields*. Second Edition. Universitext. George Green Library QA247 MAR. Springer, Cham, 2018, p. 203.

mi [4] James S. Milne. 'Algebraic Number Theory'. Lecture Notes, available at https://www.jmilne.org/math/CourseNotes/ant.html. 2020.

siksek [5] Samir Siksek. 'MA3A6 Algebraic Number Theory'. Lecture Notes, available at https://samirsiksek.github.io/siksek.github.io/index.html. 2018.

stewart [6] Ian Stewart and David Tall. *Algebraic number theory and Fermat's last theorem*. Third. George Green Library QA247 STE. A K Peters, Ltd., Natick, MA, 2002, p. 313.

swi [7] H. P. F. Swinnerton-Dyer. *A brief guide to algebraic number theory*. Vol. 50. London Mathematical Society Student Texts. George Green Library QA247 SWI. Cambridge University Press, Cambridge, 2001, p. 146.