MAT415: Algebraic Number Theory

Rishibh Prakash

Jan 2024

Contents

1 Preface

These notes are based on lectured delivered by Professor Jacob Tsimerman during the Winter semester of 2024.

2 Introduction

The main goal will be to understand the field of algebraic numbers. An algebraic number is a number that is the root of a polynomial with rational coefficients.

Recall a field is a set equipped with two operations $+$ and $\cdot$ where $(F, +, 0)$ and $(F^*, \cdot, 1)$ form commutative groups (where $F^* := F \setminus \{0\}$). The two operations are linked via the distributive law

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

Equivalently, a field is a commutative ring where every non-zero element is a unit. Some examples of fields are $\mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{Z}/p\mathbb{Z}($ for prime $p), \mathbb{Q}[\sqrt{2}]$.

2.1 Field Extensions

If E is a field and contains a subfield F then we say E is an *extesion (field)* of F. This is typically denoted E/F (note this is *not* a quotient!). Notice that since we can scale elements of E by elements of F (this is simply multiplication) we can in fact view E as a vector space over F. We call the dimension (as a vector space) of E over F the degree of the extension and denote if $[E : F]$. We say E is a finite extension if its degree (as an extension of E) is finite.

Example 2.1. $\mathbb{C}$ is a field extension of $\mathbb{R}$. In fact it has degree 2 so is a finite extension.

Example 2.2. $\mathbb{R}$ is a field extension of $\mathbb{Q}$. However, this extension is *not* finite (in fact the dimension of $\mathbb{R}$ over $\mathbb{Q}$ is not even countably infinite!).

Often we are working with polynomials over fields. Sometimes these polynomials are irreducible and the natural question we ask is whether there exists a (finite?) extension which contains a root. In fact the answer is yes and one can do so in a fairly simple way. Let $p(x)$ be an irreducible polynomial over F. Then $F[x]/(p(x))$ is a field (because $p(x)$ is irreducible) containing a copy of F (namely the images of the constant polynomials). The image of x in the quotient is a root of $p(x)$. In fact quotienting by irreducible polynomials will be the primary way we construct field extensions.

Definition 2.3 (Algebraic extensions)**.** Given an extension E/F we say $\alpha \in E$ is *algebraic* over F if one of the following equivalent conditions hold:

(i) There exists an irreducible polynomial $f(x) \in F[x]$ such that $f(\alpha) = 0$.

(ii) $F(\alpha)$ is a finite degree extension over F where $F(\alpha)$ is the (sub)field (of E) generated by α and E

We say E/F is an algebraic extension if every $\alpha \in E$ is algebraic over F.

Theorem 2.4 *The algebraic elements in E over F form a field.*

Proof. Given α, β algebraic over F, we want to show $\alpha^{-1}, \alpha+\beta$ and $\alpha\beta$ are algebraic over F. We will do so by considering $F(\alpha, \beta)$.

Since α, β are algebraic over F we know $[F(\alpha,\beta) : F(\alpha)]$ and $[F(\alpha) : F]$ are finite. Notice that

$$[F(\alpha,\beta) : F] \leq [F(\alpha,\beta) : F(\alpha)] \cdot [F(\alpha) : F]$$

This inequality holds because we construct a basis of $F(\alpha, \beta)$ over F by first finding a basis of the former field over $F(\alpha)$ and then find a basis of $F(\alpha)$ over F. Thus $\alpha^{-1}, \alpha+\beta, \alpha\beta$ are algebraic. □

Definition 2.5 (Algebraically closed fields)**.** A field F is said to be algebraically closed if every polynomial in $F[x]$ factors into linear factors. Equivalently every irreducible polynomial in $F[x]$ is linear.

Theorem 2.6 *Every field F has an algebraically closed extension. Moreover this extension can be chosen to be algebraic over F. In fact, such an extension is essentially unique since any two algebraic algebraically close extensions of F are isomorphic.*

Remark 2.7. The isomorphism at the end can be chosen to be an F-isomorphism so that when restricted to F, we get an isomorphism of F.

Given a field F, let $\overline{F}$ be the (unique) algebraic algebraically closed field extension of F. As suggested by the notation, we call $\overline{F}$ the algebraic closure of F.

3 Galois Theory

The motivation of Galois theory comes from the fact that often roots of polynomials are algebraically indistinguishable. For example any polynomial over $\mathbb{Q}$ with i as a root also has $-i$ as a root. In other words there is no way to canonically label one of the roots as i and the other one as $-i$, just algebraically. In fact we have the same issue with $\sqrt{2}$ and $-\sqrt{2}$ as well.

Theorem 3.1 *Let E/F is a field extension and $\alpha in E$. If $f(x)$ is a minimal polynomial of α over F then*

$$F(\alpha) \cong F[x]/(f(x))$$

Definition 3.2 (Conjugate elements)**.** Two elements α_1, α_2 are said to be conjugate is they satisfy the same minimal polynomial.

Theorem 3.3 *Let $\alpha_1, \alpha_2 \in \overline{F}$ be conjugate. Then there exists an F-automorphism $\phi : \overline{F} \to \overline{F}$ such that $\phi(\alpha_1) = \alpha_2$.*

This is what we mean when we say that conjugate elements are 'algebraically indistinguishable'.

Definition 3.4 (Normal extension)**.** An algebraic extension E/F is normal if any of the following equivalent conditions hold:

(i) E contains all the conjugates of α for every $\alpha \in F$.

(ii) The minimal polynomial of α factors into linear factors over E.

(iii) If $f(x)$ is an irreducible polynomial in $F[x]$ then f has a root in E if and only if f splits completely in E.

(iv) Every F-map $\phi : E \to \overline{F}$ sends E to E

Example 3.5. $\mathbb{C}/\mathbb{R}$ is a normal extension (in particular because $\mathbb{C}$ is algebraically closed).

Example 3.6. The extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not normal because although it contains a root of $x^3 - 2$ it does not contain all of them.

Theorem 3.7 *If E/F is an algebraic extension then every $\alpha \in F$ is contained in a finite normal extension E' over F.*

Proof. Let $\alpha_1, \ldots, \alpha_n$ be conjugates of α (in $\overline{F}$). Then $E' := F(\alpha_1, \ldots, \alpha_n)$ is the desired finite normal extension. □

Definition 3.8 (Separable extensions)**.** An algebraic extension E/F is *separable* if for all $\alpha \in E$ if $f(x)$ is a minimal polynomial of α then α has $\deg(F)$ different conjugates.
An equivalent formulation is to say that whenever E_0 is a subfield of E containing F (in other E_0 is an extension of F and E is an extension of E_0) the number of F-maps from E_0 to $\overline{F}$ is exactly $[E_0 : F]$.

Example 3.9. The extension $\mathbb{Q}[\sqrt{2}]/\mathbb{Q}$ is separable. Any element in $\mathbb{Q}[\sqrt{2}]$ is of the form $\alpha + \beta\sqrt{2}$ for $\alpha, \beta \in \mathbb{Q}$. If $\beta = 0$ then the element is a rational number and nothing needs to be checked (its minimal polynomial is the linear polynomial $x - \alpha$). If β is non-zero then a minimal polynomial is $(x - \alpha)^2 - 2\beta^2$. But this has two roots, namely $\alpha \pm \beta\sqrt{2}$.

Example 3.10. This is an example of a non-separable extension. Let $F := \mathbb{F}_p(t)$ be the field of all rational functions in t (which is to say all quotients of polynomials in t with non-zero denominators). The polynomial $f(x) = x^p - t$ is irreducible in $F[x]$. Thus we can take $E := F/(f(x))$. Let α be the image of x which is to say that α is a root of f. Then we know $E = \mathbb{F}_p(\alpha)$. However the minimal

polynomial of α, namely f itself, can be factored in E as

$$x^p - t = x^p - \alpha^p = (x - \alpha)^p$$

This shows the minimal polynomial has repeated roots and hence this extension is not separable.

As one can see above, we had to work a bit to find a non-separable extension. The following theorem shows why.

Theorem 3.11 *If char$(F) = 0$ or F is finite then all algebraic extensions E/F are separable.*

Remark 3.12. A field such that every finite extension is separable is called perfect.

Definition 3.13 (Galois extension)**.** A finite extension E/F is Galois if any of the following equivalent conditions hold

(i) E/F is separable and normal

(ii) $|\mathrm{Aut}(E/F)| = [E : F]$

(iii) $E \otimes_F \overline{F} \cong \prod_{[E:F]} \overline{F}$

Definition 3.14. If E/F is a Galois extension then we define its Galois group

$$\mathrm{Gal}(E/F) := \mathrm{Aut}(E/F) = \{\sigma : E \to E : \sigma \text{ is a field isomorphism such that } \sigma|_F = \mathrm{id}\}$$

Theorem 3.15 *(a) The map*

$$\{\textit{subgroups of Gal}(E/F)\} \to \{\textit{subfields of } E \textit{ containining } F\}$$
$$H \mapsto E^H := \{x \in E : h(x) = x \textit{ for every } h \in H\}$$

is an inclusion reversing bijection.

(b) Gal$(E/E^H) = H$ and E^H/F is Galois if and only if H is a normal subgroup of Gal(E/F). In this case Gal$(E^H/F) =$ Gal$(E/F)/H$

A simple example to consider are quadratic extensions.

Proposition 3.16 *If F is a field of characteristic different from 2 then any quadratic extension is Galois with Galois group $\mathbb{Z}/2\mathbb{Z}$.*

Proof. By completing the square, we see that if E/F is a quadratic extension then it is of the form

$E = F[x]/(x^2 - a)$ for a nonsquare $a \in F$. Then $E = \langle 1, x \rangle$ is an F-vector space with Galois group $\{\mathrm{id}, \sigma\}$ where $\sigma(1) = 1$ and $\sigma(x) = -x$. □

Example 3.17. Let $F = \mathbb{Q}$ and E be the splitting field of $x^3 - 2$. Notice that is a Galois extension (splitting fields are normal essentially by definition and its separable because $x^3 - 2$ has 3 distinct roots).
The fundamental theorem of Galois theory gives a correspondence between subfields of E (containing $\mathbb{Q}$) and subgroups of the Galois group. Let's see if we can use this correspondence to deduce the Galois group. A good first step is to determine the order of the Galois group. It is easy to see that a $\mathbb{Q}$-basis for E is $\{1, \theta, \omega, \theta^2, \omega\theta, \omega\theta^2\}$ where θ is a cube root of 2 (so $\theta^3 = 2$) and ω is a cube root of unity (so $\omega^3 = 1$). Therefore $|\mathrm{Gal}(E/\mathbb{Q})| = 6$.
There are only 2 groups of order 6: S_3 and C_6 (the cyclic group of order 6). In fact we claim that $\mathrm{Gal}(E/\mathbb{Q})$ cannot be C_6. In order to see this, consider the subfield $\langle 1, \theta, \theta^2 \rangle$ (if $\theta = \sqrt[3]{2}$ then this subfield is $\mathbb{Q}[\sqrt[3]{2}]$) which is not normal (as a field extension). Therefore $\mathrm{Gal}(E/\mathbb{Q})$ contains a non-normal subgroup so in particular could not be abelian. In other words, automorphisms of E fixing $\mathbb{Q}$ are exactly the isomorphisms that permute the cube roots of 2, namely $\theta, \omega\theta, \omega^2\theta$.

4 Traces and norms

Let E/F be a finite (separable) extension with $[E : F] = n$. Let $\alpha \in E$. Then we have an F-linear map on E given by multiplication by α

$$\begin{aligned} m_\alpha : E &\to E \\ \beta &\mapsto \alpha\beta \end{aligned}$$

We can then define the trace and norm of α using this map.

Definition 4.1 (Traces and norms)**.** Given $\alpha \in E$ we define

$$\begin{aligned} \mathrm{tr}_{E/F}(\alpha) &:= \mathrm{tr}_F(m_\alpha|_E) \\ \mathsf{nm}_{E/F}(\alpha) &:= \mathsf{det}_F(m_\alpha|_E) \end{aligned}$$

Example 4.2. Take $F = \mathbb{R}$ and $E = \mathbb{C}$. If we take $\alpha = i$ then m_α (with respect to the $1, i$ basis) is given by the matrix

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

Then $\mathrm{tr}_{\mathbb{C}/\mathbb{R}}(i) = 0$ and $\mathsf{nm}_{\mathbb{C}/\mathbb{R}}(i) = 1$.

Example 4.3. Take $F = \mathbb{Q}, E = \mathbb{Q}(\sqrt[3]{2})$ and $\alpha = 1 + \sqrt[3]{2}$. If we take $\alpha = 1 + \sqrt[3]{2}$ then m_α, with respect to the usual $1, \theta, \theta^2$ basis, is given by

$$\begin{pmatrix} 1 & 0 & 2 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

Then $\mathrm{tr}_{E/F}(\alpha) = 3$ and $\mathsf{nm}_{E/F}(\alpha) = 3$.

Lemma 4.4 *Let E, F as above. Let $M = F(\alpha)$. If $e := [E : M]$ then*

$$\mathrm{tr}_{E/F}(\alpha) = e \cdot \mathrm{tr}_{M/F}(\alpha)$$

Proof. Let $\beta_1, \ldots, \beta_e$ be an M-basis for E. Let $\phi : M^e \to E$ be an isomorphism of M-vector spaces given by $(m_1, \ldots, m_e) \mapsto \sum m_i \beta_i$ (this is exactly what it means to have an M-basis of E). Then since the trace commutes with ϕ we have

$$\begin{aligned}
\mathrm{tr}_{E/F}(m_\alpha) &= \mathrm{tr}_F(m_\alpha|_{M^e}) \\
&= \mathrm{tr}_F(m_\alpha|_{\oplus_1^e M}) \\
&= e \cdot \mathrm{tr}_F(m_\alpha|_M) \\
&= e \cdot \mathrm{tr}_{M/F}(\alpha)
\end{aligned}$$

The penultimate equality follows from the fact that M^e is just a direct sum of M e times. As m_α acts identically on each summand, the trace over the sum is exactly e times the trace on a single summand. □

Lemma 4.5 *Let $f(x) \in F[x]$ be a minimal polynomial of α over F. Then $f(x)$ is the characteristic polynomial of $m_\alpha|_M$ (where as before we have $M = F(\alpha)$).*

Proof. Let $g(x)$ be the characteristic polynomial of $m_\alpha|_M$. Then by the Cayley-Hamilton theorem we have $g(m_\alpha|_M) = 0$. On the other hand, it is a direct computation that $g(m_\alpha|_M) = m_{g(\alpha)}|_M$. This means that $0 = m_{g(\alpha)}|_M(1) = g(\alpha)$. Since g is monic and $\deg(f) = \deg(g)$, we conclude $f = g$. □

Corollary 4.6 *The eigenvalues of $m_\alpha|_M$ are exactly the conjugates of α in $\overline{F}$. In particular then,*

$$\mathrm{tr}_{M/F}(\alpha) = \sum_{i=1}^{[M:F]} \alpha_i$$

$$\mathit{nm}_{M/F}(\alpha) = \prod_{i=1}^{[M:F]} \alpha_i$$

where α_i are the conjugates of α.

We can verify the previous examples using this corollary.

Example 4.7. Suppose $E = \mathbb{C}, F = \mathbb{R}$ and $\alpha = i$. Then the (only) conjugate of α is $-i$. Therefore $\mathrm{tr}_{E/F}(\alpha) = i + (-i) = 0$ and $\mathrm{nm}_{E/F}(\alpha) = i \cdot (-i) = 1$.

Example 4.8. Suppose $E = \mathbb{Q}(\sqrt[3]{2})$ and $F = \mathbb{Q}$ with $\alpha = 1 + \sqrt[3]{2}$. The conjugates of α are $1 + \sqrt[3]{2}, 1 + \omega\sqrt[3]{2}$ and $1 + \omega^2\sqrt[3]{2}$ where ω is a cube root of unity (the conjugates of a sum are the sum of the conjugates). Then the trace is the sum of the conjugates is $3 + (1 + \omega + \omega^2)\sqrt[3]{2} = 3$ and

the norm is

$$\sqrt[3]{2}(1+\omega\sqrt[3]{2})(1+\omega^2\sqrt[3]{2}) = 3$$

Proposition 4.9 *Let E/M and M/F be separable field extensions with $\alpha \in E$. Then*

$$\mathrm{tr}_{M/F}\mathrm{tr}_{E/M}(\alpha) = \mathrm{tr}_{E/F}(\alpha)$$
$$nm_{M/F}nm_{E/M}(\alpha) = nm_{E/F}(\alpha)$$

Proof. Recall that we can find all the conjugates of α by considering all the field homomorphims that preserve the base field. To be preices, if $\overline{F}$ is the algebraic closure of F then the conjugates of α over M are $\{\phi(\alpha) : \phi \in Hom_M(E, \overline{F})\}$. Similarly, given $\beta \in M$ the conjugates of β over F are $\{\psi(\beta) : \psi \in Hom_F(M, \overline{F})\}$. Therefore

$$\mathrm{tr}_{E/M}(\alpha) = \sum_{\phi} \phi(\alpha)$$
$$\mathrm{tr}_{M/F}\mathrm{tr}_{E/M}(\alpha) = \sum_{\psi} \psi\left(\sum_{\phi} \phi(\alpha)\right)$$

We can extend each ψ (non-uniquely) to a homomorphim on E. Once we do such an extension we have

$$\begin{aligned}\mathrm{tr}_{M/F}\mathrm{tr}_{E/M}(\alpha) &= \sum_{\psi,\phi}(\psi\circ\phi)(\alpha)\\ &= \sum_{\rho\in Hom_F(E,\overline{F})} \rho(\alpha)\\ &= \mathrm{tr}_{E/F}(\alpha)\end{aligned}$$

The same argument works for the norms by replacing all the sums with products. □

Proof 2. We can give a second proof for the traces that is much more down to earth. We simply evaluate both sides of the equality with respect to some bases.

Let $a_1, \ldots, a_d$ be an F-basis for M and $b_1, \ldots, b_e$ be an M-basis for E. Then $\{a_i b_j\}$ form an F-basis for E. Suppose we have

$$\alpha b_i = \sum_{t=1}^{e} m_{i,t} b_t$$

for $m_{i,t} \in M$ so

$$\mathrm{tr}_{E/M}(\alpha) = \sum_{i=1}^{e} m_{i,i}$$

Now suppose

$$m_{i,i} a_j = \sum_{s=1}^{d} f_{j,s}^{(i,i)} a_s$$

with $f_{j,s}^{(i,i)} \in F$. Then

$$\mathrm{tr}_{M/F}(m_{i,i}) = \sum_{j=1}^{d} f_{j,j}^{(i,i)}$$

This means that

$$\begin{aligned}
\mathrm{tr}_{M/F}\mathrm{tr}_{E/M}(\alpha) &= \mathrm{tr}_{M/F}\left(\sum_{i=1}^{e} m_{i,i}\right) \\
&= \sum_{i} \mathrm{tr}_{M/F}(m_{i,i}) \\
&= \sum_{i}\sum_{j} f_{j,j}^{(i,i)}
\end{aligned}$$

Now we evaluate the right hand side with respect to the basis $\{b_i a_j\}$. Then we see

$$\begin{aligned}
\alpha b_i a_j &= \left(\sum_{t=1}^{e} m_{i,t} b_t\right) a_j \\
&= \left(\sum_{t=1}^{e} m_{i,t} a_j\right) b_t \\
&= \left(\sum_{t=1}^{e}\sum_{s=1}^{d} f_{j,s}^{(i,t)} a_s\right) b_t \\
&= \sum_{t=1}^{e}\sum_{s=1}^{d} f_{j,s}^{(i,t)} b_t a_s
\end{aligned}$$

Then the trace of $m_\alpha|_E$ over F is sum over the entries where $s = j$ and $t = i$. In other words,

$$\mathrm{tr}_{E/F}(\alpha) = \sum_{i,j}^{n} = f_{j,j}^{(i,i)}$$

which is exactly what we computed for the left hand side. □

5 Number Fields

We can now introduce the primary objects of study in this course.

Definition 5.1 (Number field)**.** A *number field* is a field F of characteristic 0 such that $[F : \mathbb{Q}] < \infty$. Equivalently a number field is a finite field extension of $\mathbb{Q}$.

These are the fields we really want to study. One way of understanding these fields is by looking at how the algebraic integers sit within them.

Definition 5.2 (Algebraic integer)**.** An element α in a number field F is called an algebraic integer if the minimal polynomial of α over $\mathbb{Q}$ has integer coefficients.

Lemma 5.3 *If $\alpha \in F$ then exists a positive integer n such that $n\alpha$ is an algebraic integer.*

Proof. Let $f(x)$ be the minimal polynomial of α. Let d be its degree. Then the minimal polynomial of $n\alpha$ is $n^d f(x/n)$. It is clear that $f(x/n) = 0$ for $x = n\alpha$. No polynomial of lower degree can have $n\alpha$ as a root since we could use that to find a polynomial of lower degree that has α as a 0.

If

$$f(x) = x^d + \sum_{i=1}^{d} c_i x^{d-i}$$

then

$$n^d f\left(\frac{x}{n}\right) = n^d \left(\frac{x^d}{n^d} + \sum_{i=1}^{d} c_i \frac{x^{d-i}}{n^{d-i}}\right)$$

Therefore once n^d is large enough to clear out the denominators of the c_i, all the coefficients will be integral. □

We also have other, arguably more useful, characterisations of algebraic integers.

Lemma 5.4 *Let F be a number field and $\alpha \in F$. Then the following are equivalent*

1. *α is an algebraic integer*
2. *$\mathbb{Z}[\alpha]$ is a finitely generated free abelian group*
3. *α is an element of a subring R of F, where R forms a finitely generated free abelian group with respect to addition*

Proof. (1) ⇒ (2). Let $d = \deg(f)$. Since f has integral coefficients, we conclude that $\alpha^d \in \langle 1, \alpha, \ldots, \alpha^{d-1} \rangle$ (where $\langle 1, \alpha, \ldots, \alpha^{d-1} \rangle$ is the abelian group/$\mathbb{Z}$-module generated by these elements). But this means all higher powers of α also lie in this finitely generated $\mathbb{Z}$-module. Therefore $\mathbb{Z}[\alpha] \subset \langle 1, \alpha, \ldots, \alpha^{d-1} \rangle$. The reverse inclusion is of course also true which means $\mathbb{Z}[\alpha] = \langle 1, \alpha, \ldots, \alpha^{d-1} \rangle$. Hence $\mathbb{Z}[\alpha]$ is finitely generated.

(2) ⇒ (3). Take $R = \mathbb{Z}[\alpha]$.

(3) ⇒ (1). Let $\beta_1, \ldots, \beta_n$ be a $\mathbb{Z}$-basis for R (such β_i exist because R is finitely generated and a free abelian group). Let $M := \mathbb{Q} \cdot R$, which is a subfield of F. We can consider m_α acting on M. Notice that $m_\alpha|_M$ is completely determined by how it acts on the β_i. Since $\alpha \in R$ and R is a ring, we know $\alpha\beta_i \in R$ for every i. Moreover since R is a finitely generated free abelian group, we know that $\alpha\beta_i$ can be expressed as an integral linear combinations of the $\beta_1, \ldots, \beta_n$. This is exactly saying that the matrix for $m_\alpha|_M$ with respect to the β_i basis has integer entries. Therefore the characteristic polynomial of $m_\alpha|_M$ has integral coefficients. By Gauss's lemma (recall that the characteristic polynomial is monic so is automatically primitive), this polynomial is irreducible over $\mathbb{Q}[x]$ if and only if it is irreducible over

$\mathbb{Z}[x]$. Since the minimal polynomial of α is a factor of the characteristic polynomial, this means that will also be integral. □

Corollary 5.5 *If α, β are algebraic integers then $\alpha + \beta$ and $\alpha\beta$ are algebraic integers.*

Proof. Since α, β are algebraic integers, we know by above that $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ are finitely generated free abelian groups. Let $a_1, \ldots, a_d$ and $b_1, \ldots, b_e$ be their respective $\mathbb{Z}$-bases. Then $\mathbb{Z}[\alpha, \beta] \subset \langle a_i b_j \rangle$ (and the reverse inclusion always holds) which means that $\mathbb{Z}[\alpha, \beta]$ is a finetely generated free abelian group. Since $\alpha + \beta$ and $\alpha\beta$ are contained in this ring by the third characterisation above, we conclude that they are also algebraic integers. □

We get a few immediate corollaries from this corollary.

Corollary 5.6 *The set of algebraic integers $\mathcal{O}_F$ forms a ring, called the ring of integers of F.*

Corollary 5.7 *If $\alpha \in \mathcal{O}_F$ then $\mathrm{tr}_{F/\mathbb{Q}}(\alpha)$ and $nm_{F/\mathbb{Q}}(\alpha)$ are integers.*

Proof. This is mostly evident from the proof of (3) ⇒ (1) in Lemma 5.4. Specifically, with respect to a basis for $\mathbb{Z}[\alpha]$ we know m_α has integer entries so its trace and determinant are also integers. □

In some simple cases, one can directly compute the ring of integers.

Example 5.8. Suppose $F = \mathbb{Q}(i)$ and we want to find $\mathcal{O}_F$. We know $\alpha \in F$ are of the form $a + bi$ for $a, b \in \mathbb{Q}$. If $b = 0$ then the minimal polynomial is $x - a$. This has integral coefficients if and only if a is an integer. In particular this means that integers are algebraic integers (phew!).
If $b \neq 0$ then the minimal polynomial of α is

$$(x - \alpha)(x - \overline{\alpha}) = x^2 - 2ax + (a^2 + b^2)$$

Hence in order for this to be an integral polynomial we need $2a \in \mathbb{Z}$ and $a^2 + b^2 \in \mathbb{Z}$. In fact we will show that a must be an integer due to the second constraint. Suppose $a = n/2$ for n some odd integer. As squares of integers are always congruent to 0 or 1 mod 4, we conclude the fractional part of $n^2/4$ is necessarily $1/4$. This means b^2 must have fractional part $3/4$ in order to have $n^2/4 + b^2$ be an integer. But this cannot happen as that would require the numerator of b^2 to be congruent to $3 \bmod 4$.
Therefore a must be an integer which forces b to be an integer as well. In this case, we therefore conclude that $\mathcal{O}_F = \mathbb{Z}[i]$.

The ring of integers is not always 'the obvious one' as the following example illustrates.

Example 5.9. Let $F = \mathbb{Q}(\sqrt{5})$. Then $\alpha \in F$ is of the form $a + b\sqrt{5}$ for $a, b \in \mathbb{Q}$. The case of $b = 0$ is the same as above. If $b \neq 0$ then the minimal polynomial of α is

$$(x - (a + b\sqrt{5}))(x - (a - b\sqrt{5})) = x^2 - 2ax + (a^2 - 5b^2)$$

Once again we need $2a$ to be an integer but this time we also have $a^2 - 5b^2 \in \mathbb{Z}$.

6 Lattices

Lattices will be a nice way of studying the ring of integers.

Definition 6.1 (Lattice)**.** If V is a finite-dimensional $\mathbb{Q}$-vector space, then $L \subset V$ is a *lattice* if $L \cong \mathbb{Z}^{\dim_{\mathbb{Q}} V}$ as abelian groups.

Lemma 6.2 *$L \subset V$ is a lattice if and only if L is finitely generated (as an abelian group) and L contains a basis for V.*

Proof. Let $n = \dim_{\mathbb{Q}} V$. Suppose L is a lattice. We already know L is finitely generated since $L \cong \mathbb{Z}^n$. The isomorphism also implies there exist $\alpha_1, \ldots, \alpha_n$ such that $L = \langle \alpha_1, \ldots, \alpha_n \rangle_{\mathbb{Z}}$. In fact, we claim that $\alpha_1, \ldots, \alpha_n$ also form a basis for V. If this were not the case then there would be $\mathbb{Q}$-relations between them. But by clearing denominators we would get $\mathbb{Z}$-relations between them. But this contradicts the fact that the α_i form a $\mathbb{Z}$-basis for L.

Now we show the converse. So suppose L is finitely generated and L contains a basis for V. We want to show that L is in fact a free abelian group (of the appropriate rank). Let $\alpha_1, \ldots, \alpha_n$ be a basis for V in L and let $\beta_1, \ldots, \beta_m$ be generators for L. Since the α_j form a basis for every β_i we can find $c_{ij} \in \mathbb{Q}$ such that

$$\beta_i = \sum_{j=1}^{n} c_{ij} \alpha_j$$

Let N be the product of all the denominators of the c_{ij} (if you wish to be less wasteful you can take their LCM instead). Then each β_i is contained in

$$\beta_i \in \left\langle \frac{\alpha_1}{N}, \ldots, \frac{\alpha_n}{N} \right\rangle$$

Since this holds for all β_i we have

$$\langle \alpha_1, \ldots, \alpha_n \rangle \subset L \subset \left\langle \frac{\alpha_1}{N}, \ldots, \frac{\alpha_n}{N} \right\rangle$$

□

Recall that a bilinear form on a K-vector space V is a map $Q : V \times V \to K$ such that Q is (separately) linear in each component. We say Q is symmetric if $Q(x, y) = Q(y, x)$. Such forms are also sometimes called quadratic forms.

Example 6.3. If $V = K$ then muliplication itself is a (symmetric) bilinear form (in fact some sense every bilinear form can be understood as a product of some kind).

Example 6.4. Given a vector space V and $l \in V^*$, the map $Q(x, y) = l(x)l(y)$ is also a symmetric bilinear form.

Definition 6.5 (Discriminant (of a lattice))**.** Let V be a $\mathbb{Q}$-vector space of dimension n. Let $\alpha_1, \ldots, \alpha_n$ be a basis and $Q : V \times V \to \mathbb{Q}$ a bilinear form. Let L be the lattice generated by the α_i. Then we define the discriminant of L with respect to Q as $\det(Q(\alpha_i, \alpha_j))$ (i.e. take the determinant of the matrix formed by taking $Q(\alpha_i, \alpha_j)$ to be the (i, j) entry) and denote it $\text{Disc}_Q L$.

Lemma 6.6 *The discriminant $\text{Disc}_Q L$ is well-defined.*

Proof. This is essentially the same reason that the determinant of a linear map can be defined via its matrix with respect to some basis. Let $\{\beta_1, \ldots, \beta_n\}$ be another basis for L. Then we want to show that the discriminant remains well defined under this change of basis. Let M be the change of basis matrix. Notice that M has entries in the integers because we are working with bases of the abelian group L. Then

$$\begin{aligned}(Q(\beta_k, \beta_l))_{k,l=1}^n &= \left(Q\left(\sum_{i=1}^n c_{k,i}\alpha_i, \sum_{j=1}^n c_{l,j}\alpha_j\right)\right)_{k,l=1}^n \\ &= \left(\sum_{i,j=1}^n c_{k,i}c_{l,j}Q(\alpha_i, \alpha_j)\right)_{k,l=1}^n \\ &= M(Q(\alpha_k, \alpha_l))_{k,l=1}^n M^t\end{aligned}$$

Then $\det(Q^\beta) = \det(Q^\alpha)\det(M)^2$. Since $M \in GL(n, \mathbb{Z})$ we know $\det(M) = \pm 1$. □

Lemma 6.7 *Suppose $L_1 \supset L_2$ are lattices in V such that $[L_1 : L_2] = m$ (as abelian groups) then*

$$\text{Disc}_Q L_2 = m^2 \cdot \text{Disc}_Q L_1$$

Proof. We simply compute. Let $\alpha_1, \ldots, \alpha_n$ be a basis for L_1. Since L_2 is a sublattice, there are (integers) m_i so that $m_1\alpha_1, \ldots, m_n\alpha_n$ forms a basis for L_2.

$$\text{Disc}_Q(L_2) = \det\left((m_i m_j Q(\alpha_i, \alpha_j))_{i,j=1}^n\right) = \left(\prod_{i=1}^n m_i\right)^2 \det((Q(\alpha_i, \alpha_j))_{i,j=1}^n) = m^2 \text{Disc}_Q(L_1)$$

The first equality is a definition. In order to verify the second equality, recall scaling a row or column of a matrix by a matrix by a also scales the determinant by a. Notice that $(m_i m_j Q(\alpha_i, \alpha_j))$ is formed from $(Q(\alpha_i, \alpha_j))_{i,j=1}^n$ by scaling row i and column i by m_i. The determinant is scaled by m_i^2 for every i, giving the second equality. The penultimate equality follows form the fact that $\prod m_i = m$. One way to see this is to count the cosets of L_2 (this is, after all, exactly the index of L_2 in L_1). There are m_i cosets in the i-th direction so taking a product tells us how many 'fundamental domains of L_1' fit inside a single fundamental domain of L_2 (see Figure 1). □

Here are some examples and non-examples of lattices to keep in mind

1. $\mathbb{Z} \subset \mathbb{Q}$ is a lattice

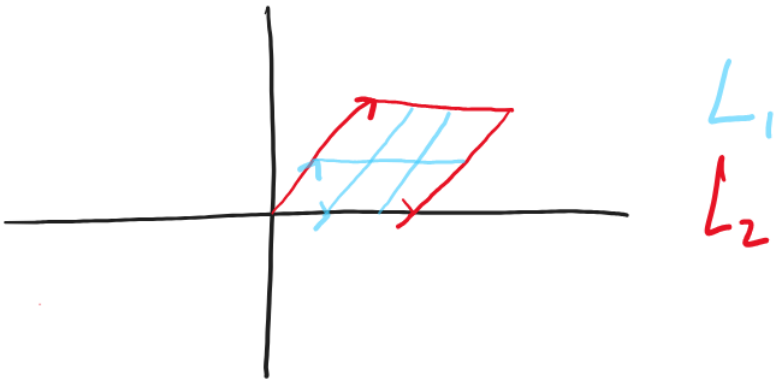

Figure 1: Example of lattice containing sublattice with $m_1 = 3$ and $m_2 = 2$

2. $\mathbb{Q} \subset \mathbb{Q}$ is not a lattice (as it is not finitely generated)
3. $\mathbb{Z}[1/p] \subset \mathbb{Q}$ for a prime p is not a lattice
4. $\langle 1/p_1, 1/p_2, \dots \rangle$ where $p_1, p_2, \dots$ form a sequence of primes is not a lattice

Definition 6.8. The trace pairing $\mathrm{tr}_{K/\mathbb{Q}} : K \times K \to \mathbb{Q}$ given by

$$\mathrm{tr}_{K/\mathbb{Q}}(x, y) = \mathrm{tr}_{K/\mathbb{Q}}(xy)$$

is a bilinear form on K.

Lemma 6.9 *The form $\mathrm{tr}_{K/\mathbb{Q}}$ is non-degenerate. In other words, for every $x \in K \setminus \{0\}$ there is some (non-zero) y such that $\mathrm{tr}_{K/\mathbb{Q}}(x, y) \neq 0$.*

Proof. The proof is quite easy. Since x is non-zero we can take $y = 1/x$ to get

$$\mathrm{tr}_{K/\mathbb{Q}}(x, y) = \mathrm{tr}_{K/\mathbb{Q}}(1) = \dim_{\mathbb{Q}}(K)$$

□

Although a fairly trivial lemma, it is important in view of the following result.

Lemma 6.10 *If V is an n-dimensional $\mathbb{Q}$-vector space and $Q : V \times V \to \mathbb{Q}$ is a non-degenerate quadratic form, then $\mathrm{Disc}_Q(L) \neq 0$ for any lattice $L \subset V$.*

Proof. Let $\psi_Q : V \to V^*$ be such that $(\psi_Q(x))(y) = Q(x, y)$ (one can think of $\psi_Q(x)$ as filling one of the components of Q so $\psi_Q(x) = Q(x, \cdot)$). Then

$$\begin{aligned} Q \text{ non degenerate} &\Leftrightarrow \forall x \in V \setminus \{0\} \exists y \in V \text{ such that } Q(x, y) \neq 0 \\ &\Leftrightarrow \forall x \in V \setminus \{0\} \psi_Q(x) \neq 0 \\ &\Leftrightarrow \psi_Q \text{ injective} \\ &\Leftrightarrow \psi_Q \text{ isomorphism} \end{aligned}$$

Let $\alpha_1, \ldots, \alpha_n$ be a basis for V and $\alpha_1^\vee, \ldots, \alpha_n^\vee$ its dual basis in V^*. Recall that given a basis and its dual we can express any $\varphi \in V^*$ with respect to this dual basis by $\varphi = \sum_j \varphi(a_j) a_j^\vee$. Thus taking $\varphi = \psi_Q(\alpha_i)$ we have

$$\psi_Q(\alpha_i) = \sum_{j=1}^{n} \psi_Q(\alpha_i)(\alpha_j)\alpha_j^\vee = \sum_{j=1}^{n} Q(\alpha_i, \alpha_j)\alpha_j^\vee$$

Therefore $(Q(\alpha_i, \alpha_j))_{i,j=1}^n$ is the matrix for $\psi_Q : V \to V^*$ with respect to the α_i and its dual basis. Since ψ_Q is an isomorphism this matrix must have non-zero determinant which is exactly saying that the discriminant of the lattice $L = \langle \alpha_1, \ldots, \alpha_n \rangle$ with respect to Q is non-zero. □

Finally we have the following proposition to justify the discussion of lattices and discriminants.

Proposition 6.11 *Let K be a number field. The ring of integer $\mathcal{O}_K$ forms a lattice in K.*

Proof. Let $\alpha_1, \ldots, \alpha_n$ be a $\mathbb{Q}$-basis for K. Recall we can scale each α_i (by an integer in fact) so that it lies in $\mathcal{O}_K$. Thus we can assume that $\alpha_1, \ldots, \alpha_n$ themselves lie in $\mathcal{O}_K$. This tells us that $\mathcal{O}_K$ definitely contains a basis of K. It remains to show that $\mathcal{O}_K$ is finitely generated.

Let $\alpha_1^\vee, \ldots, \alpha_n^\vee$ be the dual basis to $\alpha_1, \ldots, \alpha_n$. Since $\mathrm{tr}_{K/\mathbb{Q}}$ is a non-degenerate bilinear form, we know that $\psi_{\mathrm{tr}_{K/\mathbb{Q}}}$ defines an isomorphism from V to V^*. In particular then, there exist $\beta_1, \ldots, \beta_n$ such that β_i is sent to $\alpha_i^\vee$. This means that

$$\psi_{\mathrm{tr}_{K/\mathbb{Q}}}(\beta_i)(\alpha_j) = \delta_{ij}$$

which just means

$$\mathrm{tr}_{K/\mathbb{Q}}(\beta_i \alpha_j) = \delta_{ij}$$

Now suppose $\gamma \in \mathcal{O}_K$. Then since $\gamma\alpha_i \in \mathcal{O}_K$ so the trace of the product is integral for every i. On the other hand, we know $\beta_1, \ldots, \beta_n$ form a basis of K so $\gamma = \sum c_i \beta_i$ for some rational numbers c_i. We show that in fact the c_i must be integers. This is easy to do since the α_j essentially allow us to pick out the j-th component.

$$\mathbb{Z} \ni \mathrm{tr}_{K/\mathbb{Q}}(\gamma\alpha_j) = \mathrm{tr}_{K/\mathbb{Q}}\left(\sum_{i=1}^{n} c_i \beta_i \alpha_j\right) = \sum_{i=1}^{n} c_i \delta_{i,j} \alpha_j = c_j$$

This holds for all j so $\gamma \in \langle \beta_1, \ldots, \beta_n \rangle$. Thus we conclude

$$\langle \beta_1, \ldots, \beta_n \rangle \supset \mathcal{O}_K \supset \langle \alpha_1, \ldots, \alpha_n \rangle$$

But this means that $\mathcal{O}_K$ must also be isomorphic to $\mathbb{Z}^n$. Thus $\mathcal{O}_K$ is a lattice. □

Definition 6.12 (Discriminant of a number field)**.** The discriminant of a number field Disc_K (or sometimes simply D_K) is $\mathrm{Disc}_{\mathrm{tr}_{K/\mathbb{Q}}}(\mathcal{O}_K)$.

In fact the discriminant can be useful a tool for calculating the ring of integers.

Example 6.13. Let $K = \mathbb{Q}(\sqrt{7})$. We want to find the ring of integers which we know is a lattice. Consider the lattice $L = \langle 1, \sqrt{7} \rangle$. Since $1, \sqrt{7}$ are both algebraic integers, it follows that $L \subset \mathcal{O}_K$. The question becomes whether this containment is strict. If it is, then L is a sublattice of $\mathcal{O}_K$ and so by Lemma 6.7 we know

$$\mathrm{Disc}_{\mathrm{tr}_{K/\mathbb{Q}}} L = \mathrm{Disc}_{\mathrm{tr}_{K/\mathbb{Q}}}(\mathcal{O}_K) \cdot [\mathcal{O}_K : L]^2$$

In particular we can compute the left and hand side and consider the squares dividing it to restrict the possibilities for $[\mathcal{O}_K : L]$.
The trace pairing matrix with respect to the basis $\{1, \sqrt{7}\}$ is

$$\begin{pmatrix} 2 & 0 \\ 0 & 14 \end{pmatrix}$$

which has determinant 28. Therefore $\mathrm{Disc}_{\mathrm{tr}_{K/\mathbb{Q}}}(L) = 28$. The only squares dividing it are 1 and 4 which means $[\mathcal{O}_K : L] = 1$ or 2. Suppose the index is 2. Then the possibilities for $\mathcal{O}_K$ are

$$\left\langle 1/2, \sqrt{7} \right\rangle, \quad \left\langle 1, \frac{\sqrt{7}}{2} \right\rangle, \quad \left\langle 1, \frac{1+\sqrt{7}}{2} \right\rangle$$

(consider how you could parallelograms from the fundamental domain of L with 'half the area'. The notion of area is mostly for intuition here but we will make it more precise later!). However we can immediately rule out the first 2 since $1/2$ and $\sqrt{7}/2$ are not algebraic integers (notice the square of $\sqrt{7}/2$ si not an integer). For $\frac{1+\sqrt{7}}{2}$ we can see it satisfies $2x^2 - 2x - 3$ and thus its minimal polynomial is not integral. Therefore $[\mathcal{O}_K : L] = 1$ implying that $L = \mathcal{O}_K$.

Theorem 6.14 (Stickleberger) *If K is a number field with discriminant D_K then*

$$D_K \equiv 0, 1 \bmod 4$$

Proof. Let $\alpha_1, \ldots, \alpha_n$ be a basis for $\mathcal{O}_K$. Let $\{\sigma_1, \ldots, \sigma_n\} = \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$ (i.e. homomorphisms from K to $\mathbb{C}$ that fix $\mathbb{Q}$). Recall that the $\mathrm{tr}_{K/\mathbb{Q}}(\alpha)$ can also be found as the sum of the conjugates of α. But the σ_k exactly allow us to find the conjugates of α! Thus combining these things we get

$$\mathrm{tr}_{K/\mathbb{Q}}(\alpha_i \alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i \alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j) \tag{6.1}$$

Then consider the matrix

$$M := \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_n(\alpha_1) \\ \vdots & \ddots & \vdots \\ \sigma_1(\alpha_n) & \cdots & \sigma_n(\alpha_n) \end{pmatrix} = (\sigma_j(\alpha_i))_{i,j=1}^{n}$$

Then from (6.1) it follows that the trace pairing matrix (with respect to the α_i basis) is given by MM^t.

Therefore $D_K = \det(M)^2$. But we can compute $\det(M)$ directly to get

$$\begin{aligned}\det(M) &= \sum_{\tau \in S_n} \prod_i (-1)^\tau \sigma_i(\alpha_{\tau(i)}) \\ &= \underbrace{\sum_{\tau \in S_n} \prod_i \sigma_i(\alpha_{\tau(i)})}_{A} - 2 \underbrace{\sum_{\substack{\tau \in S_n \\ (-1)^\tau = -1}} \prod_i \sigma_i(\alpha_{\tau(i)})}_{B} \\ &= A - 2B\end{aligned}$$

Therefore $D_K = (A - 2B)^2$. Both A and B are algebraic integers since they are sums and products of algebraic integers. In fact A must be rational (and therefore an integer) since A is fixed by the Galois group. Then $D_K = A^2 - 4AB + 4B^2 = A^2 + 4(B^2 - AB)$. We know that $B^2 - AB$ is an algebraic integer since A and B are. Moreover, since $D_K \in \mathbb{Z}$ this means that $B^2 - AB$ is also a rational number. Therefore we conclude $B^2 - AB \in \mathbb{Z}$ allowing us to conclude that

$$D_K \equiv A^2 \bmod 4 \equiv 0, 1 \bmod 4$$

□

7 Ring of integers as Dedekind Domains

In this section, we show that the ring of integers form a Dedekind domain. There are 3 properties that Dedekind domains must satisfy. The first of these is integral closure.

Definition 7.1 (Integral closure)**.** Let R be an integral domain and K be its fraction field. Then $\alpha \in K$ is said to be integral over R if there exists a monic polynomial $f(x) \in R[x]$ such that $f(\alpha) = 0$. We say R is integrally closed in K if $\alpha \in K$ being integral implies that $\alpha \in R$.

Here are a few equivalent characterisations, analogous to what we had for algebraic integers.

Lemma 7.2 *Let R be an integral domain and α an element of its fractional field K. Then the following are equivalent:*

1. *α is integral over R*
2. *α is contained in a ring $S \subset K$ which is finitely generated over R*
3. *$R[\alpha]$ is a finitely generated R-module*

Example 7.3. As one might expect $\mathbb{Z}$ is integrally closed over its field of fractions $\mathbb{Q}$

Example 7.4. For a non-example, consider $R = \mathbb{Z}[2i]$. Its field of fractions is $K := \mathbb{Q}(i)$. In this case, R is not integrally closed over K because $i \in K$ is integral (it satisfies $x^2 + 1$) but $i \notin R$.

Theorem 7.5 *Let K be a number field. Then $\mathcal{O}_K$ is integrally closed in K.*

Proof. Let $\alpha \in K$ be integral over $\mathcal{O}_K$. Then by Lemma 7.2, we know that $\mathcal{O}_K[\alpha]$ is a finitely generated $\mathcal{O}_K$-module. But $\mathcal{O}_K$ itself is a finitely generated $\mathbb{Z}$-module so $\mathcal{O}_K[\alpha]$ is a finitely generated $\mathbb{Z}$-module. Therefore by Lemma 5.4, α is an algebraic integer. □

The second property that Dedekind domains have is that they are Noetherian.

Definition 7.6 (Noetherian Rings)**.** A ring R is Noetherian if every ascending chain of ideals stabilises. In other words, if

$$I_1 \subset I_2 \subset I_3 \subset \cdots$$

is a chain of ideals in R then there some $k \in \mathbb{Z}$ such that $I_k = I_{k+1} = I_{k+1} = \cdots$.

Lemma 7.7 *The ring of integers $\mathcal{O}_K$ is Noetherian.*

Proof. Let $I \subset \mathcal{O}_K$ be a non-zero ideal. Then I contains a basis for K as a $\mathbb{Q}$ vector space. This is because we know $\mathcal{O}_K$ contains a basis and then multiplying this basis by some $i \in I \setminus \{0\}$ gets us a basis for K in I as multiplication by a non-zero element maintains linear independence. Let $\beta_1, \ldots, \beta_n$ be this basis in I then. □

Definition 7.8 (Norm)**.** Given a non-zero $I \subset \mathcal{O}_K$, we define

$$\mathbf{Nm}(I) := [\mathcal{O}_K : I]$$

Lemma 7.9 *Every non-zero prime ideal in $\mathcal{O}_K$ is maximal.*

Proof. Let $P \subset \mathcal{O}_K$ be a non-zero prime ideal. Then $\mathcal{O}_K/P$ is an integral domain which is finite (as a set) due to the finite index. We know finite integral domains are fields so P must be maximal. □

Definition 7.10. A Dedekind domain R is an integral domain such thata

8 Fractional Ideals and Class Group

Definition 8.1 (Fractional ideal)**.** A fractional ideal in K is a subset $I \subset K$ such that I is finitely generated as an $\mathcal{O}_K$-module. Equivalently, I is a fractional ideal if it is an $\mathcal{O}_K$-module and is finitely generated over $\mathbb{Z}$.

Example 8.2. The simplest (and fundamental) example is with $K = \mathbb{Q}$. In this case we know that all the non-zero ideals are $\{n\mathbb{Z} : n \in \mathbb{Z}_{>0}\}$. Then given any $q \in \mathbb{Q}$, we see that $q\mathbb{Z}$ forms a fractional

idea. In fact more generally, if $I \subset \mathcal{O}_K$ is an ideal and $\alpha \in K^*$ then αI is a fractional ideal.

Remark 8.3. Throughout this section, it will be useful to think of ideals as actual integers and fractional ideals as actual fractions/rational numbers to orient yourself and get a sense for what is actually going on.

In fact every fractional ideal can be scaled version to form an actual (or integral) ideal (analogous to how one can always scale a rational number to get an integer).

Lemma 8.4 *If $I \subset K$ is a non-zero fractional ideal then there exists an ideal $J \subset \mathcal{O}_K$ and $\alpha \in K^*$ such that $I = \alpha J$.*

Proof. The proof follows more or less immediately from the fact that I is finitely generated as an $\mathcal{O}_K$ module and that any element of K can be scaled to form an algebraic integer.

By definition I is finitely generated as an $\mathcal{O}_K$ module, so let $\alpha_1, \ldots, \alpha_n$ be a finite set of generators. Each α_i can be written in the form $\alpha_i = c_i/d_i$ for $c_i, d_i \in \mathcal{O}_K$ (we know every element can be scaled to be an algebraic integer so we can take this quotient for the c_i, d_i. In fact the d_i can be taken to be actual integers, see Lemma 5.3). Take α to be the product of all the denominators so $\alpha = \prod d_i$. Then $J := \alpha I$ is an $\mathcal{O}_K$-module contained in $\mathcal{O}_K$. But this is exactly saying that J is an ideal. □

We have all the same operations with fractional ideals that we do with regular (or integral) ideals.

Lemma 8.5 *If I, J are fractional ideals then $I + J$, IJ and $I \cap J$ are all also fractional ideals, where recall*

$$\begin{aligned} I + J &:= \{i + j : i \in I, j \in J\} \\ IJ &:= \langle ij : i \in I, j \in J \rangle_{\mathcal{O}_K} \\ I \cap J &= \{i : i \in I \text{ and } i \in J\} \end{aligned}$$

Proof. There exist α_1, α_2 such that $\alpha_1 I$ and $\alpha_2 J$ are integral ideals of $\mathcal{O}_K$. But we can take $\alpha = \alpha_1 \alpha_2$ to get the same conclusion for αI and αJ. In other words, we can scale both I and J by the same element to get them to be actual ideals in $\mathcal{O}_K$. With this we are done since

$$\begin{aligned} I + J &= \alpha^{-1}(\alpha I + \alpha J) \\ IJ &= \alpha^{-2}(\alpha I \cdot \alpha J) \\ I \cap J &= \alpha^{-1}(\alpha I \cap \alpha J) \end{aligned}$$

□

To continue the theme that fractional ideals are just like fractions, notice how their addition is just like how addition of fractions works.

In the case where $K = \mathbb{Q}$, we see that the set of fractional ideals is $\{q\mathbb{Z} : q \in \mathbb{Q}_{>0}\}$ which interestingly forms a group (under multiplication of course). In fact this is the case more generally. This is particularly easy to see in the case where $\mathcal{O}_K$ is a PID.

Proposition 8.6 *Let K be a number field. Suppose $\mathcal{O}_K$ is a PID. Then*

1. *The set of non-zero fractional ideals I_K forms an abelian group (under multiplication).*
2. *Explicitly $I_K \cong K^*/\mathcal{O}_K^*$*

Proof. Define the map

$$\begin{aligned} \phi : K^* &\to I_K \\ \alpha &\mapsto \alpha\mathcal{O}_K \end{aligned}$$

Clearly ϕ preserves the multiplication since

$$\phi(\alpha\beta) = (\alpha\beta)\mathcal{O}_K = (\alpha\mathcal{O}_K)\cdot(\beta\mathcal{O}_K)$$

We also claim that ϕ is surjective. Let $I \subset K$ be a (non-zero) fractional ideal. Then we can find $\alpha \in K^*$ and $J \subset \mathcal{O}_K$ an ideal so that $I = \alpha J$. Since $\mathcal{O}_K$ is a PID there is some β so that $J = \beta\mathcal{O}_K$. But then $I = \alpha\beta\mathcal{O}_K$ which is to say $I = \phi(\alpha\beta)$.

Now we can show quite easily that I_K forms a group. Associativity is clear (it holds for ideal multiplication in general). The identity element is $\mathcal{O}_K$ itself. It only remains to show fractional ideals are invertible. Let $I \in I_K$. Let $\alpha \in K^*$ so that $I = \phi(\alpha)$. Take $J = \phi(\alpha^{-1})$. Then $IJ = \phi(\alpha)\phi(\alpha^{-1}) = \phi(1) = \mathcal{O}_K$.

In order to verify the second statement, we only need to compute the kernel of ϕ.

$$\begin{aligned} \ker(\phi) &= \{\alpha \in K^* : \phi(\alpha) = \mathcal{O}_K\} \\ &= \{\alpha \in K^* : \alpha\mathcal{O}_K = \mathcal{O}_K\} \\ &= \mathcal{O}_K^* \end{aligned}$$

□

Let us prove the statement in the more general case.

Theorem 8.7 *Let K be a number field. Then I_K forms an abelian group.*

Proof. As above, the only thing we need to check is the existence of inverses. Suppose we know that integral ideals have inverses. Then if $I = \alpha J$ with I a fractional ideal and J an integral ideal then $\alpha^{-1}J^{-1}$ is an inverse of I. So it suffices to show we can invert fractional ideals. Consider again the prototypical case of $K = \mathbb{Q}$ where if we know how to invert integers, we immediately know how to invert any other rational number as well.

Step 1: Reduction to prime ideals

We claim that if $J \subset \mathcal{O}_K$ is a non-zero ideal, then there exist non-zero prime ideals $P_1, \ldots, P_m$ such that their product $P_1 \cdots P_m$ is contained in J.

If this is not the case, then by Noetheirality there exists a maximal J which does not have this property. Certainly J cannot be prime (if it were then we could take $m = 1$ and $P_1 = J$). Therefore J is not prime so there exists $\alpha, \beta \in \mathcal{O}_K \setminus J$ such that $\alpha\beta \in J$.

Consider $J_1 = (\alpha, J)$ and $J_2 = (\beta, J)$. By construction $J_1 \supsetneq J$ and $J_2 \supsetneq J$ but $J_1 J_2 \subset J$. Since J was maximal with respect to the above property, we know J_1, J_2 contain a product of primes. To be precise, there exist $Q_1, \ldots, Q_r$ and $Q_1', \ldots, Q_s'$ all prime such that

$$\prod Q_i \subset J_1, \quad \prod Q_j' \subset J_2$$

but then

$$\left(\prod Q_i\right)\left(\prod Q_j'\right) \subset J_1 J_2 \subset J$$

Step 2: Inverting prime ideals
Let $P \subset \mathcal{O}_K$ be a non-zero prime ideal. Define

$$P^- := \{\alpha \in K : \alpha P \subset \mathcal{O}_K\}$$

As you might imagine P^- will be the inverse to P but first, let's verify that P^- is a fractional ideal, i.e. a finitely generated $\mathcal{O}_K$-module. It is easy to see that P^- is an $\mathcal{O}_K$-module. Let $\beta \in \mathcal{O}_K$ and $\alpha \in P^-$. Then $(\alpha\beta)P = \alpha P \subset \mathcal{O}_K$ (closure of P^- under addition and additive inverses is similarly easy to check). In order to see that P^- is finitely generated (as an $\mathcal{O}_K$-module) it suffices to show it is contained in a finitely generated $\mathcal{O}_K$-module. By definition of P^- we know that for every $t \in P$ we have $tP^- \subset \mathcal{O}_K$. Then taking t to be non-zero we get $P^- \subset t^{-1}\mathcal{O}_K$ which is of course a finitely generated $\mathcal{O}_K$-module.

We naturally have $\mathcal{O}_K \subset P^-$ and $P \subset P \cdot P^- \subset \mathcal{O}_K$ which means that PP^- is an ideal in $\mathcal{O}_K$ (any R-module contained in the ring R is an ideal). Since prime ideals are maximal in Dedekind domains, we conclude that $P^-P = P$ or $P^-P = \mathcal{O}_K$. We will show that we cannot have the former.

Suppose we had $P^-P = P$. This forces $P^- = \mathcal{O}_K$. Let $r \in P^-$. If $P^-P = P$, then in particular multiplication by r defines a ring homomorphism from $P \to P$ which we can write out as a matrix with integer entries (thinking of P as a $\mathbb{Z}$-module). By Lemma 4.5 the minimal polynomial for r is the characteristic polynomial for this matrix which is in particular a monic polynomial with integer coefficients and r as a root. Thus r is an algebraic integer. Thus in order to have a contradiction, we simply need to show there exists $r \in P^- \setminus \mathcal{O}_K$. This will take some effort.

Take any non-zero β in P and consider the ideal $(\beta) = \beta\mathcal{O}_K$ generated by β. By *Step 1* above, we can find prime factors of (β). In other words, we can find prime ideals $P_1, \ldots, P_m$ so that $\prod P_i \subset (\beta)$. Let m be minimal with respect to this property (i.e. no product of less than m prime ideals lies in (β)).

Since β is in P, we know $(\beta) \subset P$. Then

$$\prod P_i \subset (\beta) \subset P$$

Primality of P immediately implies that one of the P_i must be P itself (this is analogous to the case of integers where if a prime divides a product of primes then it must appear in the product). If this were not the case then we could choose $a_i \in P_i \setminus P$ to get $\prod a_i \in P$ but this contradicts primality. Therefore, without loss of generality, we can assume $P_1 \subset P$ and since prime ideals are maximal we have $P_1 = P$. Since m above was chosen to be minimal, we know

$$\prod_{i=2}^{m} P_i \subsetneq (\beta)$$

Therefore we can choose $\gamma \in \prod_{i=2}^{m} P_i \setminus (\beta)$. Notice this means

$$\gamma P \subset P \cdot \prod_{i=2}^{m} P_i = \prod_{i=1}^{m} P_i \subset (\beta) = \beta \cdot \mathcal{O}_K$$

Rearranging this we get $(\gamma\beta^{-1})P \subset \mathcal{O}_K$ which is to say $\gamma\beta^{-1} \in P^-$. But also $\gamma\beta^{-1} \notin \mathcal{O}_K$ since we chose γ to lie outside $(\beta) = \beta\mathcal{O}_K$. This concludes Step 2.

Step 3: Inverting (integral) ideals

Suppose not every ideal is invertible. Then (by Noetherirality) there is a maximal ideal J which is not invertible. Let P be a maximal (hence prime) ideal containing J. By above we know that P has an inverse P^-. Consider P^-J. We know $1 \in P^-$ (indeed P^- contains all of $\mathcal{O}_K$) so $P^-J \supset J$. Either $P^-J = J$ or, P^-J is strictly bigger and so, by maximality of J, it has an inverse.

We know there exists $r \in P^- \setminus \mathcal{O}_K$ which means that $rJ \not\subset J$ (if it was then multiplication by r would be a $\mathbb{Z}$-homomorphism so by the same argument as above would force r to be in the ring of intgers). Therefore P^-J cannot be J. Thus P^-J has an inverse Q. This means QP^- is an (so the) inverse of J since

$$\mathcal{O}_K = Q(P^-J) = (QP^-)J$$

□

With the previous theorem we actually get unique factorisation of ideals.

Corollary 8.8 *Every (non-zero) integral ideal $J \subset \mathcal{O}_K$ is a finite product of prime ideals.*

Proof. As we've done before, suppose the statement does not hold and take J to be a maximal ideal so that it cannot be expressed as a product of prime ideals. Let P be the maximal (equivalently, prime) ideal containing it (clearly J itself cannot be prime). Then $J = (JP^-)P$. We know from above that JP^- is an ideal strictly containing J so JP^- can be expressed as a product of primes but this means that J can be expressed as a product of primes. □

Theorem 8.9 *Every non-zero integral ideal factors uniquely as a product of prime ideals (up to the usual shenanigans of reordering).*

Proof. The proof runs the same as in the usual integer setting.

Suppose

$$\prod_{i=1}^{m} P_i = \prod_{j=1}^{r} Q_j$$

with P_i, Q_j non-zero prime ideals. Suppose $\min\{m, r\}$ is minimal with respect to having different factorisation. Notice we have

$$P_1 \supset \prod_{i=1}^{m} P_i = \prod_{j=1}^{r} Q_j$$

thus primality of P_1 implies that it contains at least one of the Q_j (if not we could take $a_j \in Q_j \setminus P_1$ to get $\prod a_j$ to lie in P_1 despite none of the terms lying in P_1). Without loss of generality we can assume

$j = 1$ and since prime ideals are maximal we conclude $P_1 = Q_1$. Then we can multiply both sides of the equation above by $P^-(= Q^-)$ to get

$$\prod_{i=2}^{m} P_i = \prod_{j=2}^{r} Q_j$$

But this contradicts minimality of $\min\{m, r\}$. □

With all this theory being built up, it is useful to work with some examples to see it in action.

Example 8.10. Consider $K = \mathbb{Q}(\sqrt{-6})$. In this case, one can calculate that $\mathcal{O}_K = \mathbb{Z}[\sqrt{-6}]$. This ring is a standard example of where the 'classic' unique factorisation statement does not hold since

$$2 \cdot 3 = 6 = -\sqrt{-6} \cdot \sqrt{-6}$$

but $\sqrt{-6}$ does not divide 2 or 3 and neither 2 nor 3 divide $\sqrt{-6}$. The 'problem' is that the ideals generated by these elements are not prime. Indeed we see that

$$(2, \sqrt{-6})(2, \sqrt{-6}) = (4, 2\sqrt{-6}, -6) = (2)$$

where for the last equality, the inclusion $\subset$ is clear (all the generators are multiples of 2) and to see $\supset$ note that $2 = -(4 + (-6))$. Similarly we have $(3, \sqrt{-6})^2 = (3)$. Therefore

$$(6) = (2)(3) = (2, \sqrt{-6})^2 (3, \sqrt{-6})^2$$

is the prime decomposition of the ideal (6).
As a bonus we have, basically, computed the inverses of $(2, \sqrt{-6})$ and $(3, \sqrt{-6})$. Notice

$$\left(\frac{1}{2}\right)(2, \sqrt{-6})(2, \sqrt{-6}) = \left(\frac{1}{2}\right)(2) = (1)$$

Therefore

$$(2, \sqrt{-6})^{-1} = \left(\frac{1}{2}\right)(2, \sqrt{-6}) = \left(1, \frac{\sqrt{-6}}{2}\right)$$

and similarly

$$(3, \sqrt{-6})^{-1} = \left(1, \frac{\sqrt{-6}}{3}\right)$$

It's also useful to keep counterexamples in mind where things don't work out to appreciate how things can go wrong. Here we see why it is important that we work with ideals of $\mathcal{O}_K$ (or, slightly more generally, with ideals of Dedekind domains).

Example 8.11. Consider $K = \mathbb{Q}(i)$ and $R = \mathbb{Z}[2i] := \{a + bi : a \in \mathbb{Z}, b \in 2\mathbb{Z}\}$. In this case, we will show that the 'fractional ideals' of R could not form a group. Consider $I = (2, 2i)_R$ and $J = (2)_R$. It is clear that J is properly contained in I (for example $2i \notin J$). However

$$I^2 = (4, 4i, -4) = (4, 4i) = I \cdot J$$

Thus we don't even have cancellation of ideals so we certainly could not form a group from the ideals.

Definition 8.12. If I, J are non-zero ideals, we say $I|J$ (read "I divides J") if there exists an ideal $M \subset \mathcal{O}_K$ such that $IM = J$.
Given two ideals I, J, their greatest common divisor (GCD) is an ideal D such that $D|I$ and $D|J$ and if D' is any other ideal dividing both I and J then $D'|D$. Their lowest common multiple (LCM) is an ideal M such that $I|M$, $J|M$ and if M' is any other ideal satisfying this then $M'|M$.

Lemma 8.13 *The GCD and LCM of non-zero ideals exists and*

$$\mathit{GCD}(I, J) = I + J$$
$$\mathit{LCM}(I, J) = I \cap J$$

Remark 8.14. The main idea is to note that the divisibility relation is equivalent to containment.

$$I|J \Leftrightarrow I \supset J$$

Proof. Suppose $I|J$. Then there exists M such that $J = IM \subset I$. Conversely suppose $I \supset J$. Then $JI^- \subset II^{-1} = \mathcal{O}_K$. Therefore JI^{-1} is an ideal in $\mathcal{O}_K$ so we can write $M = JI^{-1}$ to get $J = IM$.

Then since $I \cap J \subset I, J \subset I + J$, it's certainly true that $I + J$ is a divisor of I and J and that both I, J divide $I \cap J$. Suppose $D|I$ and $D|J$. Then $D \supset I$ and $D \supset J$. Then $D \supset I + J$ (since D is an ideal) so $D|I + J$. Similarly if $I|M$ and $J|M$ then $I \supset M$ and $J \supset M$ so $I \cap J \supset M$ so $I \cap J|M$. □

Remark 8.15. Another way to find the GCD and LCM of ideals is to use their prime factor decomposition as one would with integers. To be precise, if

$$I = \prod_{i=1}^{n} P_i^{e_i}, \quad J = \prod_{i=1}^{n} P_i^{f_i}$$

with $e_i, f_i \geq 0$ and P_i distinct prime ideals of $\mathcal{O}_K$, then

$$\mathrm{GCD}(I, J) = \prod_{i=1}^{n} P_i^{\min\{e_i, f_i\}}, \quad \mathrm{LCM}(I, J) = \prod_{i=1}^{n} P_i^{\max\{e_i, f_i\}}$$

Lemma 8.16 *Suppose I, J are fractional ideals. Then $I \supset J$ if and only if $JI^{-1} \subset \mathcal{O}_K$.*

Proof. Suppose $I \supset J$. Then $JI^{-1} \subset II^1 = \mathcal{O}_K$. Running this in reverse gets us the other direction (this requires cancellation which is possible since I_K is a group). Alternatively, note that $J = I \cdot (JI)^{-1} \subset I \cdot \mathcal{O}_K = I$. □

Corollary 8.17 *For all $I, J \in I_K$, we have*

$$I \cdot J = (I + J) \cdot (I \cap J)$$

Proof. The statement is easy to see for integral ideals. We note that

$$I \cdot J = \mathsf{GCD}(I, J) \cdot \mathsf{LCM}(I, J)$$

This can be seen by writing the GCD and LCM in terms of the prime decomposition of I and J.

Now suppose I, J are fractional ideals. Then we can find $\alpha \in K^*$ and (integral) ideals $I', J' \subset \mathcal{O}_K$ such that $I = \alpha I'$ and $J = \alpha J'$. Then

$$IJ = \alpha^2 I'J' = \alpha^2(I' + J') \cdot (I' \cap J') = (\alpha I' + \alpha J')(\alpha I' \cap \alpha J') = (I + J) \cdot (I \cap J)$$

□

We also have (unique) factorisation of fractional ideals.

Proposition 8.18 *Let I be a fractional ideal. Then we can write*

$$I = \prod_{i=1}^{n} P_i^{e_i}$$

where P_i are prime ideals and e_i are integers. Moreover this decomposition is unique (up to the usual reordering stuff).

Proof. Existence of such a decomposition is easy to see. Let α be such that αI is an integral ideal. Then

$$I = \alpha I \cdot (\alpha)^{-1}$$

and we can decompose both terms into a product of primes.

In order to see uniquness, suppose

$$\prod_{i=1}^{n} P_i^{e_i} = \prod_{i=1}^{n} P_i^{f_i}$$

with P_i prime ideals and e_i, f_i integers (we are allowing some to be 0). Let N be such that $N+e_i, N+f_i \geq 0$ for all i. Then multiplying both sides by $\prod_{i=1}^{n} P_i^N$ we get

$$\prod_{i=1}^{n} P_i^{e_i+N} = \prod_{i=1}^{n} P_i^{f_i+N}$$

Both sides are now integral ideals so by uniqueness in this case we conclude $e_i + N = f_i + N$ for all i. □

Corollary 8.19 (Chinese Remainder Theorem) *Let $I = \prod_{i=1}^{n} P_i^{e_i}$ be an ideal with P_i distict prime ideals and e_i positive integers. Then*

$$\phi : \mathcal{O}_K/I \to \prod_{i=1}^{n} \mathcal{O}_k/P_i^{e_i}$$

given by the natural map is an isomorphism.

Remark 8.20. The map is given by $[x]_I \mapsto ([x]_{P_1^{e_1}}, [x]_{P_2^{e_2}}, \ldots, [x]_{P_n^{e_n}})$. This is well-defined because $I \subset P_i^{e_i}$ for all i.

Proof. Consider the map $\widetilde{\phi} : \mathcal{O}_K \to \prod \mathcal{O}_K/P_i^{e_i}$. We claim that this map is onto and its kernel is I.

In order to see that this map is onto it suffices to show that elements of the form $([0], \ldots, [1], \ldots, [0])$ can be lifted since these generate the target space as an $\mathcal{O}_K$-module. Let E_i denote such elements (i.e. E_i has $[1]$ in the i-th component and $[0]$ everywhere else). We will show how to lift E_1 and the argument for the remaining E_i is analogous.

Define $J := \prod_{j=2}^{n} P_j^{e_j}$. Notice that $P_1^{e_1}$ is relatively prime to J so

$$P_1^{e_1} + J = \mathsf{GCD}(P_1^{e_1}, J) = \mathcal{O}_K$$

Therefore there exist $\beta \in P_1^{e_1}, \gamma \in J$ such that $\beta + \gamma = 1$. Then $\phi(\gamma) = E_1$. In other words, $[\gamma]_{P_1^{e_1}} = [1]_{P_1^{e_1}}$ since the difference of the representatives lies in $P_1^{e_1}$. □

We take some time to explore the properties of ideal norms. Recall in Definition 7.8 we defined the norm of an ideal I as the index $[\mathcal{O}_K : I]$.

Theorem 8.21 *Let K be a number field and I, J non-zero ideal in $\mathcal{O}_K$. Then*

$$\mathbf{Nm}(IJ) = \mathbf{Nm}(I)\mathbf{Nm}(J)$$

Proof. We will prove this lemma using 2 claims:

Claim 1: The statement holds when I and J are relatively prime, i.e. when $\mathsf{GCD}(I, J) = \mathcal{O}_K$.

Claim 2: The statement holds when $I = P$ is prime and $J = P^n$.

Notice that these two claims along with prime decomposition of I, J allows us to conclude the statement for all ideals. In particular if $I = \prod_{i=1}^{n} P_i^{e_i}$ then

$$\begin{aligned} \mathbf{Nm}(I) &= \prod_{i=1}^{n} \mathbf{Nm}(P_i^{e_i}) && \text{(by claim 1)} \\ &= \prod_{i=1}^{n} \mathbf{Nm}(P_i)^{e_i} && \text{(by claim 2)} \end{aligned}$$

Proof of Claim 1. By definition $\mathbf{Nm}(IJ)$ is the index of the ideal IJ (viewed as a subgroup) in $\mathcal{O}_K$. This is exactly the cardinality of $\mathcal{O}_K/IJ$. Then coprimeness of I, J implies, using the Chinese Remainder Theorem, that

$$\mathcal{O}_K/IJ \cong \mathcal{O}_K/I \oplus \mathcal{O}_K/J$$

Therefore

$$\underbrace{|\mathcal{O}_K/IJ|}_{\mathbf{Nm}(IJ)} = \underbrace{|\mathcal{O}_K/I|}_{\mathbf{Nm}(I)} \cdot \underbrace{|\mathcal{O}_K/J|}_{\mathbf{Nm}(J)}$$

Proof of Claim 2. This statement takes a bit more work to prove. We want to show that $\mathbf{Nm}(P^n) = \mathbf{Nm}(P)^n$. Notice that this statement is slightly easier to prove if P is a principal ideal. There are a few different ways of proving the statement in this setting but one way that generalises quite nicely is to consider the map

$$\begin{aligned} \phi : \mathcal{O}_K &\to (p)/(p^2) \\ \alpha &\mapsto [p\alpha] \end{aligned}$$

Clearly this map is onto and primality implies that its kernel is exactly (p). So $\mathcal{O}_K/(p) \cong (p)/(p^2)$. In fact we can consider the same map on (p^n) for $n \geq 1$

$$\begin{aligned} \phi : (p^n) &\to (p^{n+1})/(p^{n+2}) \\ \alpha &\mapsto [p\alpha] \end{aligned}$$

Once again primality implies the kernel is (p^{n+1}) so $(p^n)/(p^{n+1}) \cong (p^{n+1})/(p^{n+2})$. Notice this means that

$$|\mathcal{O}_K/(p)| = \left|(p)/(p^2)\right| = \cdots = \left|(p^n)/(p^{n+1})\right|$$

Now we can just combine all this information using the third isomorphism theorem (repeatedly). The theorem gives us

$$\begin{aligned} |\mathcal{O}_K/(p^n)| &= |\mathcal{O}_K/(p)| \cdot |(p)/(p^n)| \\ &= |\mathcal{O}_K/(p)| \cdot \left|(p)/(p^2)\right| \cdot \left|(p^2)/(p^n)\right| \\ &\vdots \\ &= |\mathcal{O}_K/(p)| \cdot \left|(p)/(p^2)\right| \cdot \left|(p^2)/(p^3)\right| \cdots \left|(p^{n-1})/(p^n)\right| \\ &= |\mathcal{O}_K/(p)|^n \end{aligned}$$

Of course not every (prime) ideal is principal so we still need to consider how to deal with those ideals. But notice the main thing we used above was the map $\phi : P^n \to P^{n+1}/P^{n+2}$ (for $n \geq 0$) and that its kernel was exactly P^{n+1}. With some work, such a map is not too hard to find and in fact can be made to look exactly like ϕ above, i.e. multiplication by a single element. Let $\pi \in P \setminus P^2$. Then exactly one factor of P appears in the factorisation of (π), i.e. $(\pi) = PQ$ where P and Q are coprime ideals (i.e. $GCD(P, Q) = (1)$). Then we define

$$\begin{aligned} \phi : P^n &\to P^{n+1}/P^{n+2} \\ \alpha &\mapsto [\pi\alpha] \end{aligned}$$

We claim that the kernel of ϕ is exactly P^{n+1}. In order to see this suppose $[\pi\alpha] = 0$ in the quotient which is exactly saying $(\pi\alpha) \subset P^{n+2}$ so $P^{n+2} \mid (\pi\alpha) = (\pi)(\alpha) = PQ(\alpha)$. Therefore $P^{n+1} | Q \cdot (\alpha)$ and since Q is relatively prime to P we must have $P^{n+1} | (\alpha)$ so $\alpha \in P^{n+1}$.

Therefore with this map the exact same argument as with the principal ideal case hold. In fact this is a general technique that one might use to move arguments on principal ideals to general ideals in Dedekind domains. □

We can naturally extend the notion of norms to fractional ideals.

Definition 8.22. Let I be a fractional ideal. Then we can write $I = AB^{-1}$ for some integral ideals A, B (we can do so by Proposition 8.18). Then we define

$$\mathbf{Nm}(I) = \frac{\mathbf{Nm}(A)}{\mathbf{Nm}(B)}$$

This extension of the norm has many of the properties that you would expect.

Proposition 8.23 *The norm for fractional ideals satisfies the following properties:*

1. *The norm is well defined. If $AB^{-1} = CD^{-1}$ then $AD = BC$ and so $\mathbf{Nm}(A)\mathbf{Nm}(D) = \mathbf{Nm}(B)\mathbf{Nm}(C)$*
2. *The norm is multiplicative for fractional ideals as well.*
3. *If $I \supset J$ then $\mathbf{Nm}(J) = \mathbf{Nm}(I)[I : J]$*

We have two notions of norm: one for ideals and one for elements of the number field itself. The two notions agree when they should.

Lemma 8.24 *Let $\alpha \in \mathcal{O}_K \setminus \{0\}$. Then*

$$\mathbf{Nm}((\alpha)) = \left|nm_{K/\mathbb{Q}}(\alpha)\right|$$

Proof. Notice by definition $\mathbf{Nm}((\alpha)) = |\mathcal{O}_K/\alpha\mathcal{O}_K|$. We can write this out in a nice way. Since $\alpha\mathcal{O}_K$ is free abelian group (i.e. a $\mathbb{Z}$-module) contained in a free abelian group $\mathcal{O}_K$, there exists a basis $\{\beta_1, \ldots, \beta_n\}$ of $\mathcal{O}_K$ such that $\{d_1\beta_1, \ldots, d_n\beta_n\}$ form a basis of $\alpha\mathcal{O}_K$ for some $d_1, \ldots, d_n \in \mathbb{Z}$ (this is by the classification of finitely generated abelian groups or, if you prefer, the structure theorem for finitely generated modules over PIDs). Therefore the index $[\mathcal{O}_K : \alpha\mathcal{O}_K]$ is exactly $\prod d_i$ (see Figure 1 to convince yourself).

Now consider the map m_α

$$\begin{aligned} m_\alpha : K &\to K \\ \beta &\mapsto \alpha\beta \end{aligned}$$

We want to work out the determinant of this map so in principle we should try to work out the matrix of this map and then do the usual determinant calculations. However we know that $\{d_1\beta_1, \ldots, d_n\beta_n\}$ is also a basis for the image of m_α. This means that, up to a sign, the determinant of m_α is the same of the linear map defined by $\beta_i \to d_i\beta_i$. The determinant of this map is of course $\prod d_i$. Thus we get

$$\mathbf{Nm}((\alpha)) = \prod d_i = \left|\mathsf{nm}_{K/\mathbb{Q}}(\alpha)\right|$$

□

From this the result for fractional ideals follows.

Corollary 8.25 *If $\alpha \in K^*$ then*

$$\mathbf{Nm}(\alpha\mathcal{O}_K) = \mathit{nm}_{K/\mathbb{Q}}(\alpha)$$

Proof. Simply scale α so it lies in $\mathcal{O}_K$ and then use the previous lemma. Norms are multiplicative so we get the statement. □

9 Real and complex embeddings

Definition 9.1. We say $L \subset \mathbb{R}^n$ is a *lattice* if

1. $L \cong \mathbb{Z}^n$ as an abelian group
2. L contains an $\mathbb{R}$-basis for $\mathbb{R}^n$

When dealing with lattices of $\mathbb{Q}$-vector spaces we only needed the first condition. However when going to $\mathbb{R}$-vector spaces the second condition is a necessary addendum as the following counterexample demonstrates

Example 9.2. Consider $L = \left\langle (1,0), (\sqrt{2},0) \right\rangle_{\mathbb{Z}} \subset \mathbb{R}^2$. Then L is indeed isomorphic to $\mathbb{Z}^2$ (as an abelian group) but clearly should not be a lattice.

Clearly what is going wrong above is that the subset is not discrete and you have points in L that are arbitrarily close together. One feels that if this is not the case then we should have a lattice. The following theorem shows exactly this.

Theorem 9.3 *Let $L \subset \mathbb{R}^n$ be isomorphic to $\mathbb{Z}^n$. Then the following are equivalent:*

1. *L is a lattice*
2. *$L \subset \mathbb{R}^n$ is discrete*
3. *There is some $M > 0$ so that for all $\ell \in L \setminus \{0\}$ we have $|\ell| > M$*

Proof. (2) $\Rightarrow$ (3). This follows immediately by applying discreteness to the point $0 \in L$. In particular by discreteness there is some $\delta > 0$ so that $B_\delta(0) \cap L = \{0\}$ so we can take $M = \delta$.

(3) $\Rightarrow$ (2). The third condition is basically discreteness at 0 and its fairly easy to deduce discreteness around all other points by translation. Let $\ell \in L$ and let $\ell' \in B_M(\ell) \cap L$. Since $L \cong \mathbb{Z}^n$ we know $\ell' - \ell \in L$ and since $|\ell' - \ell| < M$ we conclude $\ell' - \ell = 0$.

(1) $\Rightarrow$ (3). If L is a lattice then it contains a basis $\{e_1, \dots, e_n\}$ of $\mathbb{R}^n$. Let $\{f_1, \dots, f_n\}$ be the standard basis and let ϕ be the vector space isomorphism taking f_i to e_i. Then $\mathbb{Z}^n \subset \mathbb{R}^n$ is sent to L under this isomorphism. Notice that ϕ is not only an isomorphism but also a homeomorphism. Therefore since $\mathbb{Z}^n \subset \mathbb{R}^n$ is discrete so is its image L.

(3) $\Rightarrow$ (1). This is the most non-trivial implication. We will show the contrapositive. So suppose L does not contain a basis of $\mathbb{R}^n$. We will show there exists points in L that are arbitrarily close to 0.

Since L does not contain a basis, it lives in an $(n-1)$-dimensional subspace of $\mathbb{R}^n$. Let $\psi : \mathbb{R}^{n-1} \to \mathbb{R}^n$ map into this subspace. To be precise, ψ is a linear injective map so that $L \subset \psi(\mathbb{R}^{n-1})$ (in principle L might live in an even small dimensional space than $\mathbb{R}^{n-1}$ but in that case we simply take the domain of ψ to be smaller. The argument is easily modified.). Let $f_i = \psi^{-1}(e_i)$. Let $A = \max_i\{|f_i|\}$. For any $B \in \mathbb{Z}$ we can consider

$$S := \left\{ \sum_{i=1}^{n} a_i f_i : a_i \in \mathbb{Z} \text{ such that } -B \leq a_i \leq B \right\}$$

Notice that $|S| = (2B+1)^n$ and $S \subset B_{nAB}(0)$ the ball of radius nAB in $\mathbb{R}^{n-1}$ centered at 0. The volume of $B_{nAB}(0)$ is strictly less than the volume of $B_{nAB+1}(0)$ which in turn is some constant multiple of $(nAB+1)^{n-1}$. The key point is that $|S|$ grows faster than the volume (as we allow $B \to \infty$). This will force points to occur arbitrarily close.

To make things more concrete, suppose we place balls of radius $0 < \delta < 1$ around all the points in S. Then the total volume over all these ball is $C_{n-1}|S|\delta^{n-1}$ where C_{n-1} is the volume of the unit ball. All of these balls are contained in $B_{nAB+1}(0)$ and if all of these balls were disjoint we would have

$$C_{n-1}(2B+1)^n\delta^{n-1} < C_{n-1}(nAB+1)^{n-1} \tag{9.1}$$

However

$$\frac{nAB+1}{(2B+1)^{n/(n-1)}} \to 0$$

as $B \to \infty$. Thus by choosing B sufficiently large we can find a $\delta > \frac{nAB+1}{(2B+1)^{n/(n+1)}}$ arbitrarily small so that the inequality in (9.1) is flipped. For such δ, the δ-balls around the points in S cannot all be disjoint so there must be some $s_1, s_2 \in S \subset L$ so that $|s_1 - s_2| < 2\delta$. Since δ can be taken to be arbitrarily small, we are done. □

9.1 Embedding map

Definition 9.4. Let K be a number field of degree n. Let r_1 be the number of real embeddings of K (i.e. the number of homomorphisms $\sigma : K \to \mathbb{R}$ that fix $\mathbb{Q}$) and $2r_2$ the number of 'non-real complex' embeddings (i.e. the number of homomorphisms $\sigma : K \to \mathbb{C}$ that achieves non-real values at some points). This quantity is always going to be even because such maps always come in complex conjugate pairs. The quantities we are going to be most interested in are r_1 and r_2.

Example 9.5.

1. $K = \mathbb{Q}(\sqrt{2})$ then $r_1 = 2$ and $r_2 = 0$
2. $K = \mathbb{Q}(\sqrt{-1})$ then $r_1 = 0$ and $r_2 = 1$
3. $K = \mathbb{Q}(\sqrt[3]{2})$ then $r_1 = 1$ and $r_2 = 1$

Then we can define

$$\begin{aligned} \sigma : K &\hookrightarrow \mathbb{R}^{r_1} \oplus \mathbb{C}^{r_2} \\ k &\mapsto (\sigma_1(k), \dots, \sigma_{r_1}(k), \tau_1(k), \dots, \tau_{r_2}(k)) \end{aligned}$$

where σ_i are the real embeddings and τ_j are 'non-real complex' embeddings. You should think of σ as encoding all the different ways that the number field K (which is somewhat of an abstract object) can be 'realised'.

Example 9.6. Consider the first example above, $K = \mathbb{Q}(\sqrt{2})$. In this case σ is defined by

$$\begin{aligned} \sigma : \mathbb{Q}(\sqrt{2}) &\to \mathbb{R}^2 \\ a + b\sqrt{2} &\mapsto (a + b\sqrt{2}, a - b\sqrt{2}) \end{aligned}$$

For the second example the map σ is given by

$$\begin{aligned} \sigma : \mathbb{Q}(\sqrt{-1}) &\to \mathbb{C} \\ a + b\sqrt{-1} &\to a + bi \end{aligned}$$

This might be seem a bit silly when written like this but the point is that on the left we are thinking of $a + b\sqrt{-1}$ as just some rational linear combinations of 1 and $\sqrt{-1}$ (something like a formal sum) while on the right we are thinking of this as an actual complex number. To emphasise this distinction, I wrote $\sqrt{-1}$ as i on the right.
Notice also in this case, there are 2 choices for σ. We could have equally well defined it by its complex conjugate $a + b\sqrt{-1} \mapsto a - bi$. Since such maps always come in complex conjugate pairs, we only keep track of one of them.
For the final example, σ could be defined as

$$\begin{aligned} \sigma : \mathbb{Q}(\sqrt[3]{2}) &\to \mathbb{R} \times \mathbb{C} \\ a + b\sqrt[3]{2} &\mapsto (a + b\sqrt[3]{2}, a + be^{2\pi i/3}\sqrt[3]{2}) \end{aligned}$$

Once again, we have two choice for σ by taking the complex conjugate of the second entry.

Proposition 9.7 *$\sigma(\mathcal{O}_K)$ is a lattice*

Proof. We already know $\mathcal{O}_K \cong \mathbb{Z}^n$ and σ is an isomorphism onto its image. So we only need to show $\sigma(\mathcal{O}_K)$ contains an $\mathbb{R}$-basis of $\mathbb{R}^{r_1} \oplus \mathbb{C}^{r_2} \cong \mathbb{R}^n$. We will do so by showing σ has non-zero determinant.

Let $\alpha_1, \dots, \alpha_n$ be a $\mathbb{Z}$ basis for $\mathcal{O}_K$ (and hence also a $\mathbb{Q}$-basis for K). With respect to this basis the

matrix for σ is given by

$$\sigma = \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_{r_1}(\alpha_1) & \tau_1(\alpha_1) & \cdots & \tau_{r_2}(\alpha_1) \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\alpha_n) & \cdots & \sigma_{r_1}(\alpha_n) & \tau_1(\alpha_n) & \cdots & \tau_{r_2}(\alpha_n) \end{pmatrix}$$

This is an $n \times (r_1 + r_2)$ matrix. Ideally we would like a square matrix and its easy to do so with our usual identifications of $\mathbb{C}$ with $\mathbb{R}^2$ via the real and imaginary parts of a complex number. Then the matrix becomes

$$\begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_{r_1}(\alpha_1) & \mathrm{Re}(\tau_1(\alpha_1)) & \mathrm{Im}(\tau_1(\alpha_1)) & \cdots & \mathrm{Re}(\tau_{r_2}(\alpha_1)) & \mathrm{Im}(\tau_{r_2}(\alpha_1)) \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \sigma_1(\alpha_n) & \cdots & \sigma_{r_1}(\alpha_n) & \mathrm{Re}(\tau_1(\alpha_n)) & \mathrm{Im}(\tau_1(\alpha_n)) & \cdots & \mathrm{Re}(\tau_{r_2}(\alpha_n)) & \mathrm{Im}(\tau_{r_2}(\alpha_n)) \end{pmatrix}$$

which has non-zero determinant if and only if σ does.

By performing column operations we can get τ_j and $\overline{\tau_j}$ along the columns. This gives us the matrix

$$N = \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_{r_1}(\alpha_1) & \tau_1(\alpha_1) & \overline{\tau_1}(\alpha_1) & \cdots & \tau_{r_2}(\alpha_1) & \overline{\tau_{r_2}}(\alpha_1) \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \sigma_1(\alpha_n) & \cdots & \sigma_{r_1}(\alpha_n) & \tau_1(\alpha_n) & \overline{\tau_1}(\alpha_n) & \cdots & \tau_{r_2}(\alpha_n) & \overline{\tau_{r_2}}(\alpha_n) \end{pmatrix}$$

Let us relabel $(\sigma_1, \ldots, \sigma_n) := (\sigma_1, \ldots, \sigma_{r_1}, \tau_1, \overline{\tau}_1, \ldots, \tau_{r_2}, \overline{\tau}_{r_2})$ so that now the σ_i are simply all the embeddings of K. This means that

$$N = \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_n(\alpha_1) \\ \vdots & \ddots & \vdots \\ \sigma_1(\alpha_n) & \cdots & \sigma_n(\alpha_n) \end{pmatrix}$$

It suffices to show that N has non-zero determinant.

Now notice that

$$\begin{aligned} NN^T &= (\sigma_1(\alpha_i)\sigma_1(\alpha_j) + \cdots + \sigma_n(\alpha_i)\sigma_n(\alpha_j))_{i,j=1}^n \\ &= \left(\mathrm{tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j)\right)_{i,j=1}^n \end{aligned}$$

Taking determinants on both sides, we get that $\det(N)^2$ is the discriminant of K. We know the discriminant of a number field is never zero (combine Lemma 6.9 and Lemma 6.10). □

9.2 Volumes

Recall what a volume form is.

Definition 9.8 (Volume form)**.** Suppose V is a real n-dimensional vector space. Then a volume form ω is simply a (non-zero) top form on V. More concretely,

$$\omega = c dx_1 \wedge \cdots \wedge dx_n$$

for $c \neq 0$.

Let $L \subset V$ be a lattice. Then we know that as (topological) groups we have $V/L \cong \mathbb{R}^n/\mathbb{Z}^n \cong (S^1)^n$. Let ω be a volume form on V. Then we define the *covolume* of L by

$$cov(L) := vol(V/L) := \left| \int_{V/L} \omega \right|$$

where ω descends to a form on V/L as it is translation invariant. In practical terms, the covolume of L is simply the area/volume of a fundamental parallelopiped.

Lemma 9.9 *If $L' \supset L$ then $cov(L) = cov(L') \cdot [L' : L]$.*

Proof. Let $\pi : V/L \to V/L'$ be the natural projection (notice this is well-defined since representatives in the domain differ by elements of L and since $L \subset L'$ in particular they differ by elements of L'). Notice that by construction is π is $[L' : L]$-to-one (this is essentially the definition of index. This statement may become more convincing by considering an example, e.g. $V = \mathbb{R}$, $L' = 2\mathbb{Z}$ and $L = 4\mathbb{Z}$). This map π lets us take the volume form on V/L and move it to V/L' but it necessarily comes with the $[L' : L]$ factor. □

Remark 9.10. It may seem slightly confusing that 'bigger' lattices have smaller volumes. If you think through everything it of course makes sense (a lattice L' is bigger than L if it contains it but that means that L' is more dense (i.e. the points are closer together) and hence must have a smaller volume), but nevertheless takes some getting used to.

Another simple observation we can make is

Lemma 9.11 *If $T : V \to V$ is linear and $L \subset V$ is a lattice then $cov(T(L)) = cov(L) \cdot |\det T|$.*

Proof. This is a simple application of the change of variables formula

$$cov(T(L)) = \left| \int_{T/V(L)} \omega \right| = \left| \int_{V/L} T^*\omega \right| = |\det(T)| \left| \int_{V/L} \omega \right| = |\det(T)|\, cov(L)$$

□

In order to apply these results about volume forms to our previous discussion, we need to choose a volume form on $\mathbb{R}^{r_1} \oplus \mathbb{C}^{r_2}$. On the copies of $\mathbb{R}$ we choose the standard volume form dx and on the copies of $\mathbb{C}$ we choose $2dx \wedge dy$ (where $\mathbb{C}$ is identified with $\mathbb{R} \oplus \mathbb{R}$ as usual. Here we take twice the usual volume on $\mathbb{C}$ since each copy of $\mathbb{C}$ corresponds to two embeddings.). With this choice we get the following lemma

Lemma 9.12

$$cov(\sigma(\mathcal{O}_K)) = \sqrt{|D_K|}$$

Proof. We essentially did this calculation in the proof of Proposition 9.7. □

10 Class Group

The class group is an important object for studying rings of integers and measures to some extent how far the ring is from being a PID.

Definition 10.1 (Class Group)**.** Let I_K be the group of non-zero fractional ideals of a number field K. Let $P_K \subset I_K$ be the group of principal fractional ideals (i.e. $P_K = \{\alpha\mathcal{O}_K : \alpha \in K^*\}$). Then the class group of K is

$$\mathbf{Cl}(K) := I_K/P_K$$

A highly non-trivial fact about the class group is that it is always finite (which is to say rings of integers are never 'too far' from being PIDs). Once we know this the class group will prove to be an important invariant and will be relatively easy to compute, at least for some cases (You get a bound for how big the class group could be and then you can just check all the possibilities in finite time). A key tool in proving finiteness is Minkowski's Theorem.

Lemma 10.2 (Minkowski's Theorem) *Let V be an n-dimensional real vector space equipped with a volume form. Let $L \subset V$ be a lattice. Let $S \subset V$ be a set that is convex, bounded, closed and symmetric about the origin (i.e. $x \in S \Rightarrow -x \in S$). Then if $vol(S) \geq 2^n cov(L)$ then $S \cap (L \setminus \{0\})$ is non-empty. In other words, S necessarily contains a non-zero point of L.*

Remark 10.3. What you want to say is that if a set is big enough, it must contain at least two points of the lattice. The problem is of course this might not be true if you're set has a very weird shape. So instead we need to impose some regularity conditions on the sets (this is where the convexness, compactness, symmetry, etc. come it) in which case the statement becomes true.

Proof. We consider 2 cases. When $vol(S)$ is strictly greater than $2^n cov(L)$ and when it is equal. Let's start with the former case. In this case we have $vol(S/2) = 2^{-n}vol(S) > cov(L)$. Consider the projection $\pi : S/2 \to V/L$. Notice that this is locally a volume-preserving homeomorphism. However π can certainly not be injective, as we conclude by simply comparing the volumes of the domain and codomain. Thus there exist $s_1 \neq s_2 \in S/2$ such that $\pi(s_1) = \pi(s_2)$. This means that

$$L \ni s_1 - s_2 = \frac{2s_1 - 2s_2}{2}$$

Notice that $2s_1$ and $-2s_2$ are in S (by symmetry of S) so convexity of S implies that $(2s_1 - 2s_2)/2$ is also in S.

Suppose $vol(S) = 2^n cov(L)$. For $0 < \epsilon \leq 1$ we can consider $S_\epsilon := (1+\epsilon)S$. This has volume strictly greater than $2^n cov(L)$ so by above we know $S_\epsilon \cap (L \setminus \{0\})$ is non-empty. Taking $\epsilon = 1/n$, we form a sequence $\{a_n\}$ of points in $S_1 \cap (L \setminus \{0\})$ which is a compact set. Thus we find a converging subsequence the limit of which must lie in $S \cap (L \setminus \{0\})$ by construction (we can also phrase this argument in a slightly different way: $S_{1/n} \cap (L \setminus \{0\})$ is a sequence of compact sets satisfying the finite intersection property. Since they all live in $S_1 \cap (L \setminus \{0\})$ which is compact, the intersection $\bigcap_n S_{1/n} \cap (L \setminus \{0\})$ is non-empty). □

Now we can prove the main theorem.

Theorem 10.4 *Given a number field K, its class group $\mathbf{Cl}(K)$ is finite.*

Proof. We will show there exists $A > 0$ such that every ideal class in the class group has a representative which is an integral ideal of norm at most A.

Let $\sigma : K \hookrightarrow V := \mathbb{R}^{r_1} \oplus \mathbb{C}^{r_2}$ be the embedding of K. Then we know that $cov(\sigma(\mathcal{O}_K)) = |D_K|^{1/2}$. Then if $I \subset \mathcal{O}_K$ is an integral ideal then $cov(\sigma(I)) = cov(\sigma(\mathcal{O}_K))[\mathcal{O}_K : I] = |D_K|^{1/2} \mathbf{Nm}(I)$. This implies that the identity $cov(\sigma(I)) = |D_K|^{1/2} \mathbf{Nm}(I)$ in fact holds for all $I \in I_K$. Why? Recall that if $I \in I_K$ then there exists $\alpha \in K^*$ so that αI is an integral ideal. Let's see how both sides scale with multiplication by α. On the right hand side we gain a factor of $\mathbf{Nm}((\alpha)) = \mathrm{nm}_{K/\mathbb{Q}}(\alpha)$. On the left hand side, using the fact that σ is a homomorphism we get $cov(\sigma(\alpha I)) = cov(\sigma(\alpha)\sigma(I))$. Viewing multiplication by $\sigma(\alpha)$ as a linear map on V, we see that its determinant is $\mathrm{nm}_{K/\mathbb{Q}}(\alpha)$. Therefore by Lemma 9.11, both sides scale by the same amount so can be cancelled out, preserving the equality.

Now we properly begin. Let $I \in I_K$ arbitrary and let S be a convex, bounded, symmetric, closed subset of V. Define

$$\lambda := \left(\frac{2^n cov(I^{-1})}{vol(S)} \right)^{1/n}$$

so that $vol(\lambda S) = 2^n cov(I^{-1})$ (for example you could take a closed ball centered at the origin of appropriate radius). Consider the map ϕ on S given by

$$(x_1, \ldots, x_{r_1}, z_1, \ldots, z_{r_2}) \mapsto |x_1| \cdots |x_{r_1}| \, |z_1|^2 \cdots |z_{r_2}|^2$$

This is obviously continuous so has a maximum M by compactness of S. Notice that given $\alpha \in K$ such that $\sigma(\alpha) \in S$, we have $\phi(\sigma(\alpha)) = \left|\mathrm{nm}_{K/\mathbb{Q}}(\alpha)\right|$ since the norm of an element is simply the product of its conjugates which is essentially exactly what ϕ computes.

While we may not be able to find such an α for S (since S may not contain any elements of the lattice $\sigma(\mathcal{O}_K)$), we can find such an α for λS as given by Minkowski's Theorem. So fix some non-zero $\alpha \in \sigma(I^{-1}) \cap \lambda S$ and observe that $\mathrm{nm}_{K/\mathbb{Q}}(\alpha) \leq M\lambda^n$ (notice that $\phi(\lambda x) = \lambda^n \phi(x)$). Then with this α we have

$$\begin{aligned}
\mathbf{Nm}(\alpha I) &= \mathbf{Nm}(I)\mathbf{Nm}((\alpha)) \\
&\leq \mathbf{Nm}(I) M \lambda^n \\
&= M\mathbf{Nm}(I) \cdot \frac{2^n cov(I^{-1})}{vol(S)} \\
&= M\mathbf{Nm}(I) \cdot \frac{2^n |D_K|^{1/2} \mathbf{Nm}(I^{-1})}{vol(S)} \\
&= \frac{M 2^n |D_K|^{1/2}}{vol(S)}
\end{aligned}$$

Notice that the final quantity is independent of I. Therefore every element of $\mathbf{Cl}(K)$ has a representative that is an *integral ideal* (notice $\alpha I \subset \mathcal{O}_K$ since $\alpha \in I^{-1}$) that has norm at most $M 2^n |D_K|^{1/2} vol(S)^{-1}$. □

We now have a bound for the norm of a representative but we can refine it further by choosing S appropriately. In fact what one finds is that the optimal S is

$$S := \{(x_1, \ldots, x_{r_1}, z_1, \ldots, z_{r_1}) : |x_1| + \cdots + |x_{r_1}| + 2|z_1| + \cdots + 2|z_{r_2}| \leq 1\}$$

Using this S we get the following corollaries

Corollary 10.5 *Every element of $\mathbf{Cl}(K)$ has an integral representative J such that*

$$\mathbf{Nm}(J) \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |D_k|^{1/2}$$

Proof. This is exactly what we did in the proof above. Given an ideal I, we found α so that αI has norm at most $M 2^n |D_K|^{1/2} / \text{vol}(S)$. By using S as above, we get a corresponding bound on M which gives the statement above. □

The right hand side of the inequality is called the *Minkowski bound*.

Corollary 10.6

$$|D_K|^{1/2} \geq \frac{n^n}{n!} \left(\frac{\pi}{4}\right)^{r_2}$$

Proof. Use the previous corollary with the fact that $1 \leq \mathbf{Nm}(J)$ for any ideal J. □

The previous corollary shows that in particular the discriminant of a field extension is always strictly greater than 1.

Using factorisation into prime ideals we get

Corollary 10.7 *The class group $\mathbf{Cl}(K)$ is generated by prime ideals of norm at most $\left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |D_K|^{1/2}$*

Thus we would like to find prime ideals of some norm and the following lemma highlights a way of finding candidates.

Lemma 10.8 *If $Q \subset \mathcal{O}_K$ is a prime ideal, then $Q | p\mathcal{O}_K$ for some prime integer p. In this case, we have $\mathbf{Nm}(Q) = p^d$ for some $1 \leq d \leq [K : \mathbb{Q}]$.*

Proof. If $Q \subset \mathcal{O}_K$ is prime then $Q \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$. Since $Q \subset \mathcal{O}_K$ has finite index, $Q \cap Z \subset \mathbb{Z}$ has finite index. Thus in particular $Q \cap \mathbb{Z} \neq \{0\}$. Therefore $Q \cap \mathbb{Z} = p\mathbb{Z}$ for some prime integer p. Therefore $p \in Q$ and so $Q \supset p\mathcal{O}_K$ which is equivalent to saying $Q \mid p\mathcal{O}_K$. Notice that the norm of the latter ideal is $p^{[K:\mathbb{Q}]}$ so $\mathbf{Nm}(Q)$ is also a power of p by multiplicativity of norms. □

This essentially gives an algorithm for finding generators of the class group. By Corollary 10.7, we only need to find prime ideals of some bounded norm. If such prime ideals exist then they must divide $p\mathcal{O}_K$ for some prime p. So by considering factors of $p\mathcal{O}_K$ we can find all possible candidates for generators of the class group. Then it amounts to finding the relations between. We do a few examples below.

Example 10.9. Consider $K = \mathbb{Q}(\sqrt{-3})$. This is a quadratic extension. In this case we know that $D_K = -3$ and $O_K = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ (since $-3 \cong 1 \bmod 4$).
In this case then the Minkowski bound is

$$\left(\frac{4}{\pi}\right)^1 \cdot \frac{2^2}{2!} \cdot \sqrt{3} < \frac{4}{3} \cdot \frac{1}{2} \cdot \sqrt{3} < 2$$

In particular this means that every element of $\mathbf{Cl}(K)$ has an integral representative of norm at most 1. The only ideal of norm 1 is $\mathcal{O}_K$ itself. Hence every (fractional) ideal in K differs from $\mathcal{O}_K$ only by a principal ideal so itself must be principal as well. In other words, $|\mathbf{Cl}(K)| = 1$

Example 10.10. For a less trivial example, consider $K = \mathbb{Q}(\sqrt{-6})$. Then $\mathcal{O}_K = \mathbb{Z}[\sqrt{-6}]$ and $D_K = -24$. Then the Minkowski bound is

$$\left(\frac{4}{\pi}\right)^1 \cdot \frac{2^2}{2!} \cdot \sqrt{24} < \frac{4}{3} \cdot \frac{1}{2} \cdot 5 < 4$$

The only primes less than 4 are 2 and 3. This means $\mathbf{Cl}(K)$ is (possibly) generated by prime factors of $2\mathcal{O}_K$ and $3\mathcal{O}_K$. Factorising ideals simply amounts to looking at ideals that sit over them. We can find these by studying the ideal structure after we quotient them out. To make this more concrete, first notice that $\mathbb{Z}[\sqrt{-6}] = \mathbb{Z}[x]/(x^2+6)$ where the "=" is given by the isomorphism which sends x to $\sqrt{-6}$. Then

$$\mathcal{O}_K/2\mathcal{O}_K = \mathbb{Z}[x]/(x^2+6)/(2) = \mathbb{F}_2[x]/(x^2)$$

In the right hand side, we have the prime ideal (x) hence its lift back to $\mathcal{O}_K$, namely $(2, x)$, is also prime and a factor of $2\mathcal{O}_K$. Since the isomorphism is given by identifying x and $\sqrt{-6}$ more concretly we are saying that $(2, \sqrt{-6})$ is a prime factor of $2\mathbb{Z}[\sqrt{-6}]$.
Now we want to know what power of $(2, \sqrt{-6})$ sits inside $2\mathbb{Z}[\sqrt{-6}]$. We could try to work this out directly but the calculation is a lot easier to do in the quotient above. Notice that the $(x)^2 = 0$ in $\mathbb{F}_2[x]/(x^2)$. Pulling this information back what we get is $(2, x)^2 = 0$ in $\mathbb{Z}[x]/(x^2+6)$ which is to say

$$(2, \sqrt{-6})^2 = 2\mathbb{Z}[\sqrt{-6}]$$

Thus $Q_2 := (2, \sqrt{-6})$ is the unique prime ideal dividing $2\mathcal{O}_K$ and hence is a (possible) generator for $\mathbf{Cl}(K)$. We will need to check that it is not principal before we can be certain that it is a generator, but assuming it is, the above computation also tells us that this generator has order 2 since its square is a principal ideal.
Now we factorise $3\mathcal{O}_K$. Repeating the same steps as above we get

$$\mathcal{O}_K/3\mathcal{O}_K = \mathbb{Z}[x]/(x^2+6)/(3) = \mathbb{F}_3[x]/(x^2)$$

Thus as before we conclude $Q_3 := (3, \sqrt{-6})$ is the unique factor dividing $3\mathcal{O}_K$ and

$$Q_3^2 = (3, \sqrt{-6})^2 = 3\mathcal{O}_K$$

Therefore we have 2 potential generators for the class group Q_2, Q_3. We need to check that they are non-trivial in the class group (i.e. non-principal) and then determine the relations between Q_2 and Q_3.
It is easy to see that Q_2 and Q_3 are non-principal. For example Q_2 has norm 2 (as an ideal. One way to see this is to use the multiplicativity of norms with respect to $Q_2^2 = (2)$ where the right hand side is norm 4) and the norm of any $\alpha = m + n\sqrt{-6}$ is $m^2 + 6n^2$. But there are no integer solutions to $m^2 + 6n^2 = 2$. The same argument applies to Q_3 which has 3. Now we need to determine the relations between Q_2 and Q_3. Let's begin by computing their product.

$$Q_2Q_3 = (2, \sqrt{-6})(3, \sqrt{-6}) = (6, 2\sqrt{-6}, 3\sqrt{-6}, -6) = (\sqrt{-6})$$

Therefore Q_2Q_3 is trivial in the class group. This means that $[Q_2] = [Q_2]^{-1} = [Q_3]$.
In summary, we conclude that $\mathbf{Cl}(K) \cong \mathbb{Z}_2$.

11 Unit Groups

11.1 Dirichlet's Unit Theorem

Dirichlet's unit theorem gives us a way of (at least abstractly) getting a handle on the group of units of $\mathcal{O}_K$.

Theorem 11.1 (Dirichlet's Unit Theorem) *Let $K/\mathbb{Q}$ be an extension of degree n with r_1 real embeddings and r_2 (pairs of) complex embeddings. Let $\mathcal{O}_K^\times$ be the group of units of $\mathcal{O}_K$. Then*

$$\mathcal{O}_K^\times \cong w_K \times \mathbb{Z}^{r_1+r_2-1}$$

where w_K is the group of roots of unity in $\mathcal{O}_K$.

It's useful to keep in mind what the isomorphism actually is. What we're saying is that there are $m := r_1 + r_2 - 1$ units in $\mathcal{O}_K$, which we label $u_1, \ldots, u_m$ such that every other unit is of the form

$$\omega u_1^{n_1} \cdots u_m^{n_m}$$

for some root of unity ω and integers $n_1, \ldots, n_m$. The u_i are called *fundamental units* of $\mathcal{O}_K$. Some examples might help make this more concrete.

Example 11.2. Consider the case of any real quadratic field K where we have $r_1 = 2$ and $r_2 = 0$. In this case we have $r_1 + r_2 - 1 = 1$ and the only roots of unit in a real field are ± 1. Therefore there exists some unit $u \in \mathcal{O}_K$ such that every unit in $\mathcal{O}_K$ is of the form $\pm u^n$ for some integer n.
Even more concretely we can consider the case where $K = \mathbb{Q}(\sqrt{2})$. In this case we see that $1 + \sqrt{2}$ is a unit (since $(1 + \sqrt{2})(-1 + \sqrt{2}) = 1$). We will show later than that $1 + \sqrt{2}$ is in fact a fundamental unit so every unit is of the form $\pm(1 + \sqrt{2})^n$.

Lemma 11.3 *If $\alpha \in \mathcal{O}_K^\times$ then $\mathbf{Nm}(\alpha) = \pm 1$.*

Proof. We have that α and α^{-1} are in $\mathcal{O}_K$. Therefore $\mathbf{Nm}(\alpha)$ and $\mathbf{Nm}(\alpha^{-1})$ are in $\mathbb{Z}$ and hence by multiplicativity of norms we conclude $\mathbf{Nm}(\alpha)$ is a unit of $\mathbb{Z}$ which are exactly ± 1. □

By Dirichlet's unit theorem, we see that the group of units of a quadratic imaginary field is exactly the group of roots of unity.

Lemma 11.4 *Let $K = \mathbb{Q}(\sqrt{-D})$. If $D \geq 5$ then $\mathcal{O}_K^\times = \{\pm 1\}$.*

Proof. This follows readily from the the previous lemma since the only elements of norm 1 are exactly ± 1. □

11.2 Example: Finding group of units

Here we find the group of units of $K = \mathbb{Q}(\sqrt{3})$. In this case we know that $\mathcal{O}_K = \mathbb{Z}[\sqrt{3}]$. We begin by finding a unit which amounts to finding an element of norm 1 or integer solutions to $m^2 - 3n^2 = 1$. Checking some numbers we find an example solution with $m = 2, n = 1$.

In fact we claim that $u := 2 + \sqrt{3}$ is a fundamental unit. In order to see this, suppose $2 + \sqrt{3} = (m + n\sqrt{3})^p$ for some integer p. Since p is at least 2 and $2 + \sqrt{3} > 1$ we have

$$\left| m + n\sqrt{3} \right| < \sqrt{2 + \sqrt{3}}$$

By taking conjugates we know $2 - \sqrt{3} = (m - n\sqrt{3})^p$ and since the left hand side is less than 1 (in absolute value) we conclude

$$\left| m - n\sqrt{3} \right| < 1$$

Then by the triangle inequality we conclude

$$|m| \leq \frac{\sqrt{2 + \sqrt{3}} + 1}{2} \approx 1.46 \cdots < 2$$

Thus the only possibilities for m are ± 1. But it is easy to see that the only solution to $m^2 - 3n^2 = 1$ with these m is $n = 0$ and clearly $-1, 1$ are not fundamental units.

One reason to explictly find unit groups is that it gives us tools for determining whether or not a given ideal is principal. For example notice $\mathbb{Q}(\sqrt{3})$ we have

$$(11) = (11, 5 - \sqrt{3})(11, 5 + \sqrt{3})$$

The question becomes is $(11, 5 - \sqrt{3})$ (or its conjugate) principal? If it were principal we would have some $\alpha := m + n\sqrt{3} \in \mathcal{O}_K = \mathbb{Z}[\sqrt{3}]$ such that

$$\pm 11 = \mathsf{nm}_{K/\mathbb{Q}}(\alpha) = m^2 - 3n^2$$

In fact by reducing mod 3, we see that there are no solutions to $11 = m^2 - 3n^2$ (since squares are always either 0 or 1 mod 3 while $11 = 2 \bmod 3$). Thus we are looking for integer solutions to

$$-11 = m^2 - 3n^2$$

Pick a unit u in $\mathcal{O}_K$. Above we found that $2 - \sqrt{3}$ is a fundamental unit in $\mathcal{O}_K$ which makes this a particularly convenient choice for u. Notice that because u is a unit we have $-11 = \alpha\overline{\alpha} = (\alpha u)\overline{\alpha u}$. [TODO: Finish]

11.3 Relative Units

Definition 11.5. Let K be a number field. Let S be a finite set of non-zero prime ideals of $\mathcal{O}_K$. Then we define

$$\mathcal{O}_{K,S} := \{x \in K : x = 0 \text{ or } (x) \text{ has denominators in } S\}$$

12 Ramification

We want to study how primes (and indeed ideals) behave when lifted to field extensions. We begin with the following theorem which gives us a relationship between the degree of the extension and the 'amount of splitting'.

Theorem 12.1 *Let K be a number field and $[K : \mathbb{Q}] = n$. Let p be a prime integer. Then $p\mathcal{O}_K$ is an ideal in $\mathcal{O}_K$ so we consider its factorisation*

$$p\mathcal{O}_K = \prod_{i=1}^{m} P_i^{e_i}$$

where the P_i are distinct prime ideals. Define $f_i := [\mathbb{F}_{P_i} : \mathbb{F}_p]$ where $\mathbb{F}_{P_i} := \mathcal{O}_K/P_i$ (this makes sense because $\mathbb{Z} \subset \mathcal{O}_K$ and $p\mathbb{Z} \subset P_i$ so we have containment of quotients as well $\mathbb{Z}/p\mathbb{Z} \subset \mathcal{O}_K/P_i$). Then

$$n = \sum_{i=1}^{m} e_i f_i$$

Proof. This is easy to prove by taking norms of both sides and using multiplicativity of norms

$$\begin{aligned} p^n = \mathbf{Nm}(p\mathcal{O}_K) &= \prod_{i=1}^{m} \mathbf{Nm}(P_i)^{e_i} \\ &= \prod_{i=1}^{m} |\mathbb{F}_{P_i}|^{e_i} \\ &= p^{\sum e_i f_i} \end{aligned}$$

□

Definition 12.2 (Residual and ramification degrees)**.** The f_i are called the *residual/inertial degrees* and the e_i are the *ramification degrees*.

We want to kind of general these (and some previous constructions) to arbitrary extensions L/K as opposed to just extensions of $\mathbb{Q}$. We begin by discussing lifts of ideals

Definition 12.3 (Lifting ideals)**.** Let L/K be a field extension and $I \subset \mathcal{O}_K$ an ideal. Then we define

$$I_L := I\mathcal{O}_L$$

where the right hand side is the ideal generated by I in $\mathcal{O}_L$.

Remark 12.4. Typically one thinks of these in terms of generators. Then the generators of I and I_L are the same. For example if we take $(2) \subset \mathbb{Z}$ and lift it to $\mathbb{Z}[i] \subset \mathbb{Q}(i)$ we get the ideal (2). However in the former case we have $(2) = \{2n : n \in \mathbb{Z}\}$ while in the latter case we have $(2) = \{2a + 2bi : a, b \in \mathbb{Z}\}$.

Remark 12.5. We have

$$(IJ)_L = I_L J_L$$

This can be argued by considering generators since on either side we are simply considering products of the same generators.

The map defined above from ideal in K to ideals in L is injective.

Proposition 12.6 *Given an extension L/K and $I \subset \mathcal{O}_K$ an ideal we have*

$$I_L \cap \mathcal{O}_K = I$$

Proof. By construction we have $I \subset I_L \cap \mathcal{O}_K$. It remains to show the reverse inclusion. Let's first show the case for principal ideals. In other words, we claim that for all $\alpha \in \mathcal{O}_K$ we have

$$\alpha\mathcal{O}_L \cap \mathcal{O}_K = \alpha\mathcal{O}_K$$

This is easy since

$$\begin{aligned}
\beta \in \alpha\mathcal{O}_L \cap \mathcal{O}_K &\Leftrightarrow \beta/\alpha \in \mathcal{O}_L \text{ and } \beta \in \mathcal{O}_K \\
&\Leftrightarrow \frac{\beta}{\alpha} \in \mathcal{O}_L \text{ and } \beta \in \mathcal{O}_K \\
&\Leftrightarrow \frac{\beta}{\alpha} \text{ is an algebraic integer and in } K \\
&\Leftrightarrow \beta \in \mathcal{O}_K
\end{aligned}$$

Now given an arbitrary ideal $I \subset \mathcal{O}_K$ we can use the finiteness of the class group to conclude that I^m is principal for some (positive) integer m. Then by above we have $(I^m)_L \cap \mathcal{O}_K = I^m = (I \cap \mathcal{O}_K)^m$. On the other hand

$$(I^m)_L \cap \mathcal{O}_K = I_L^m \cap \mathcal{O}_K \supset (I_L \cap \mathcal{O}_K)^m$$

Therefore $I^m = (I_L \cap \mathcal{O}_K)^m$ and since one contains the other we conclude $I = I_L \cap \mathcal{O}_K$. □

If $I \subset K$ is a fractional ideal we can consider

$$I_L = I\mathcal{O}_L \subset L$$

Definition 12.7 (Norms)**.** Let L/K be number fields and $I \subset \mathcal{O}_L$. Let M be a normal closure of L. Then we define

$$\mathbf{Nm}_{L/K}(I) := \prod_{\sigma \in \mathrm{Gal}(M/K)/\mathrm{Gal}(M/L)} \sigma(I_M)$$

(notice with the quotient we simply mean the cosets in the Galois group as opposed to an actual quotient since the subgroup may not be normal).

Remark 12.8. Notice that as defined this norm sends an ideal in $\mathcal{O}_L$ to an ideal of $\mathcal{O}_M$. This is rather unsatisfying and we will fix it soon.

The simplest examples to think of are naturally cases where L/K is Galois in which case we are simply multiplying by all the conjugates of I_L.

Example 12.9. Consider $K = \mathbb{Q}(\sqrt{5})$ and the (non-principal) ideal $I = (11, 5 - \sqrt{3})$. Then

$$\begin{aligned}\mathbf{Nm}_{K/\mathbb{Q}}(I) &= (11, 5 - \sqrt{3})(11, 5 + \sqrt{3}) \\ &= (121, 11(5 - \sqrt{3}), 11(5 + \sqrt{3}), 22)\end{aligned}$$

Notice that the gcd of 121 and 22 is 11 and every generator is a multiple of 11. Therefore we have

$$\mathbf{Nm}_{K/\mathbb{Q}}(I) = (11) = 11\mathbb{Z}$$

Proposition 12.10 *The norm defined above satisfies the following properties:*

1. $\mathbf{Nm}_{L/K}(IJ) = \mathbf{Nm}_{L/K}(I)\mathbf{Nm}_{L/K}(J)$
2. *Let $\alpha \in \mathcal{O}_L$. Then*

$$\mathbf{Nm}_{L/K}(\alpha\mathcal{O}_L) = \prod_{\sigma \in \mathrm{Gal}(M/K)/\mathrm{Gal}(M/L)} \sigma(\alpha) \cdot \mathcal{O}_M = nm_{L/K}(\alpha) \cdot \mathcal{O}_M$$

3. *Similar to above, it follows that if $\alpha \in I$ then $nm_{L/K}(\alpha) \in \mathbf{Nm}_{L/K}(I)$*

Proof. Immediate from the definition □

Another natural definition of the norm, without needing to go the normal closure is

Definition 12.11 (Norm)**.** Given field extensions L/K and $I \subset \mathcal{O}_L$ an ideal, we define

$$\widetilde{\mathbf{Nm}}_{L/K}(I) := (\mathsf{nm}_{L/K}(\alpha) : \alpha \in I) \in I_K$$

In other words, we look at the ideal of $\mathcal{O}_K$ generated by the norms of all $\alpha \in I$.

In fact these two definitions of norms coincide. In order to prove this statement we need the following lemma.

Lemma 12.12 *Let I, J be non-zero ideals of $\mathcal{O}_K$. Then there exists $\alpha \in I$ such that $\alpha\mathcal{O}_K = I \cdot I'$ where $\gcd(I', J) = \mathcal{O}_K$.*

Proof. We first decompose I and J to their prime factors

$$I = \prod_{i=1}^{k} P_i^{m_i}, \quad J = \prod_{i=1}^{k} P_i^{n_i}$$

(notice we are using the same primes for both ideals so some of the m_i and n_i may be 0). Now consider the map

$$\mathcal{O}_K \to \bigoplus_{i=1}^{k} \mathcal{O}_K/P_i^{m_i+1}$$

which we know by the Chinese Remainder Theorem is onto. In particular then there exists $\alpha \in \mathcal{O}_K$ such that $\alpha \in P_i^{m_i} \setminus P_i^{m_i+1}$ for all i. This means $\alpha \in I$ so $(\alpha) \subset I$ which is equivalent to saying $I \mid (\alpha)$. In particular then there exists an integral ideal I' such that $II' = (\alpha)$.

It is clear that I' must be coprime to J. We know the only prime factors J could have are the P_i so all we need is that none of the P_i are factors of I'. But if this was the case for some P_i then $II' = (\alpha)$ would imply that $P_i^{m_i+1} \mid (\alpha)$ which contradicts our choice of α. □

Theorem 12.13 *Given $I \subset \mathcal{O}_L$ an ideal, we have*

$$\mathbf{Nm}_{L/K}(I) = (\widetilde{\mathbf{Nm}}_{L/K}(I))_M$$

Proof. We know $\mathsf{nm}_{L/K}(\alpha) \in \mathbf{Nm}_{L/K}(I)$ for every $\alpha \in I$ so in particular we conclude

$$\mathbf{Nm}_{L/K}(I) \supset (\widetilde{\mathbf{Nm}}_{L/K}(I))_M$$

Thus there exists an ideal $J \subset \mathcal{O}_M$ such that

$$J \cdot \mathbf{Nm}_{L/K}(I) = (\widetilde{\mathbf{Nm}}_{L/K}(I))_M$$

We will show that $J = \mathcal{O}_M$.

Notice that since the other two ideals are Galois invariant, so is J. We will use this below. Using the above Lemma 12.12 choose $\alpha \in I$ such that $\alpha\mathcal{O}_L = II'$ and I' is coprime to $J \cap \mathcal{O}_L$. Then we have

$$\mathbf{Nm}_{L/K}(I) \cdot \mathbf{Nm}_{L/K}(I') = \mathbf{Nm}_{L/K}(\alpha\mathcal{O}_L) = \mathbf{Nm}_{L/K}(\alpha) \cdot \mathcal{O}_M$$

Since $\mathsf{nm}_{L/K}(\alpha) \in \widetilde{\mathbf{Nm}}_{L/K}(I)$ we have

$$J \cdot \mathbf{Nm}_{L/K}(I) = (\widetilde{\mathbf{Nm}}_{L/K}(I))_M \mid \mathsf{nm}_{L/K}(\alpha) \cdot \mathcal{O}_M = \mathbf{Nm}_{L/K}(I)\mathbf{Nm}_{L/K}(I')$$

Therefore $J \mid \mathbf{Nm}_{L/K}(I')$.

Now recall that I' is coprime to $J \cap \mathcal{O}_L$. Therefore their lifts to M are also coprime: i.e. I'_M is coprime to J. This is equivalent to saying

$$I'_M + J = \mathcal{O}_M$$

Applying a Galois automorphism to both sides and using the fact that J is Galois invariant, we get

$$\sigma(I'_M) + J = \sigma(\mathcal{O}_M) = \mathcal{O}_M$$

Thus J is coprime to all conjugates $\sigma(I'_M)$ of I'_M. Since $J|\mathbf{Nm}_{L/K}(I')$ but must also be coprime to it, we conclude that $J = \mathcal{O}_M$. □

From now on we will use $\mathbf{Nm}_{L/K}(I)$ to mean $\widetilde{\mathbf{Nm}}_{L/K}(I)$ (although we will often think of it using the original definition as the product of its conjugates). The main benefit is that $\mathbf{Nm}_{L/K}(I)$ is actually an ideal in K now. Let's explore some more of its properties.

Proposition 12.14 *Let $L \supset K \supset F$ be number fields. Let I be an ideal of $\mathcal{O}_L$, I_0 an ideal of $\mathcal{O}_F$ and α an element of L. Then*

(a) $\mathbf{Nm}_{L/F}(\alpha\mathcal{O}_L) = \mathbf{Nm}_{L/F}(\alpha) \cdot \mathcal{O}_F$

(b) $\mathbf{Nm}_{K/F}(\mathbf{Nm}_{L/K}(I)) = \mathbf{Nm}_{L/F}(I)$

(c) $\mathbf{Nm}_{L/F}((I_0)_L) = I_0^{[L:F]}$

(d) $\mathit{Norm}(I_0) \cdot \mathbb{Z} = \mathbf{Nm}_{F/\mathbb{Q}}(I_0)$

Proof. (a) This holds essentially by definition

$$\begin{aligned}\mathbf{Nm}_{L/F}(\alpha\mathcal{O}_L) &= (\mathbf{Nm}_{L/F}(\alpha\beta) : \beta \in \mathcal{O}_L) \\ &= (\mathbf{Nm}_{L/F}(\alpha) \cdot \mathbf{Nm}_{L/F}(\beta) : \beta \in \mathcal{O}_L) \\ &= \mathbf{Nm}_{L/F}(\alpha) \cdot \mathcal{O}_F\end{aligned}$$

(b) Let M be the normal closure of L. Then

$$(\mathbf{Nm}_{L/K}(I))_M = \prod_{\sigma \in \mathsf{Gal}(M/K)/\mathsf{Gal}(M/L)} \sigma(I_M)$$

Thus

$$\begin{aligned}(\mathbf{Nm}_{K/F}(\mathbf{Nm}_{L/K}(I)))_M &= \prod_{\tau\in \mathsf{Gal}(M/F)/\mathsf{Gal}(M/K)} \tau((\mathbf{Nm}_{L/K}(I))_M) \\ &= \prod_{\tau\in \mathsf{Gal}(M/F)/\mathsf{Gal}(M/K)} \prod_{\sigma\in \mathsf{Gal}(M/K)/\mathsf{Gal}(M/L)} \tau(\sigma(I_M)) \\ &= \prod_{\sigma'\in \mathsf{Gal}(M/F)/\mathsf{Gal}(M/L)} \sigma'(I_M) \\ &= (\mathbf{Nm}_{L/F}(I))_M\end{aligned}$$

(c) Let $m > 0$ be an integer so that $I_0 = \alpha\mathcal{O}_F$. Thus

$$\begin{aligned}(\mathbf{Nm}_{L/F}(I_0)_L)^m = \mathbf{Nm}_{L/F}((I_0)_L^m) \\ &= \mathbf{Nm}_{L/F}((I_0^m)_L) \\ &= \mathbf{Nm}_{L/F}(\alpha\mathcal{O}_F) \\ &= \alpha^{[L:F]}\mathcal{O}_F \\ &= I_0^{m[L:F]}\end{aligned}$$

Thus by uniquness of prime factorisation, since their m-th powers are equal, we conclude

$$\mathbf{Nm}_{L/F}(I_0) = I_0^{[L:F]}$$

(d) Once again choose m so that $I_0^m = \alpha\mathcal{O}_F$ so we have

$$\mathsf{Norm}(I_0)^m = \mathsf{Norm}(I_0^m) = \mathsf{Norm}(\alpha\mathcal{O}_F) = \left|\mathsf{nm}_{F/\mathbb{Q}}(\alpha)\right|$$

Therefore we have

$$(\mathsf{Norm}(I_0)\cdot\mathbb{Z})^m = \mathsf{nm}_{F/\mathbb{Q}}(\alpha)\cdot\mathbb{Z} = \mathbf{Nm}_{F/\mathbb{Q}}(\alpha\mathcal{O}_F) = \mathbf{Nm}_{F/\mathbb{Q}}(I_0)^m$$

where the penultimate equality follows from the first property in the proposition. Thus we have

$$\mathsf{Norm}(I_0)\cdot\mathbb{Z} = \mathbf{Nm}_{F/\mathbb{Q}}(I_0)$$

□

A consequence of the above properties is the following useful proposition. This is a useful way of turning a given ideal into a principal ideal when raising it to a sufficiently high power (as we've done before) may not be useful.

Proposition 12.15 *Let K be a number field and $I \subset \mathcal{O}_K$ an ideal. Then there exists a finite extension L/K such that I_L is principal.*

Proof. As we have so often done, choose $m > 0$ so that $I^m = \alpha\mathcal{O}_K$. Let $L = K(\beta)$ where β is such that $\beta^m = \alpha$ (in other words β is an m-th root of α). Then we have

$$I_L^m = (\alpha\mathcal{O}_K)_L = \alpha\mathcal{O}_L = \beta^m\mathcal{O}_L = (\beta\mathcal{O}_L)^m$$

Thus

$$I_L = \beta\mathcal{O}_L$$

□

Let L/K be number fields. Let $Q \subset \mathcal{O}_L$ be a (non-zero) prime ideal. Then $P = Q \cap \mathcal{O}_K$ is a prime ideal of $\mathcal{O}_K$. Then $\mathbb{F}_Q := \mathcal{O}_L/Q$ and $\mathbb{F}_P := \mathcal{O}_K/P$ are fields with the former containing the latter. So we consider the degree of this extension which, as we will see, is a very important quantity.

$$f := [\mathbb{F}_Q : \mathbb{F}_P]$$

Theorem 12.16 *(a)* $\mathbf{Nm}_{L/K}(Q) = P^f$

(b) Given $P \subset \mathcal{O}_K$ prime, we can consider the prime factorisation of P_L

$$P_L = \prod_{i=1}^{g} Q_i^{e_i}$$

Define $f_i := [\mathbb{F}_{Q_i} : \mathbb{F}_P]$. Then

$$\sum_{i=1}^{g} e_i f_i = [L : K]$$

Remark 12.17. The statement should remind one of Theorem 12.1. This theorem is a generalisation of that one to the case of general (finite) field extensions instead of just field extensions over $\mathbb{Q}$.

Proof. (a) First let's show that $\mathbf{Nm}_{L/K}(Q)$ is a power of P. From Proposition 12.14 we know $\mathbf{Nm}_{L/K}(P_L) = P^{[L:K]}$. Now since $P \subset Q$ (by definition) we have $P_L \subset Q$. Thus $\mathbf{Nm}_{L/K}(P_L) \subset \mathbf{Nm}_{L/K}(Q)$ which is equivalent to saying

$$\mathbf{Nm}_{L/K}(Q) \mid \mathbf{Nm}_{L/K}(P_L) = P^{[L:K]}$$

Thus by unique prime factorisation of ideal, we conclude that $\mathbf{Nm}_{L/K}(Q) = P^m$ for some positive integer m.

Recall from Proposition 12.14 that

$$\mathbf{Nm}_{K/\mathbb{Q}}(\mathbf{Nm}_{L/K}(Q)) = \mathbf{Nm}_{L/\mathbb{Q}}(Q)$$

In particular this means $\text{Norm}(\mathbf{Nm}_{L/K}(Q)) = \text{Norm}(Q) = |\mathbb{F}_Q|$ (where by $|\cdot|$ we mean the cardinality of the set, this equality holds by definition of Norm and $\mathbb{F}_Q$). On the other hand we have

$$|\mathbb{F}_Q| = \text{Norm}(\mathbf{Nm}_{L/K}(Q)) = \text{Norm}(P^m) = |\mathbb{F}_P|^m$$

Therefore $m = [\mathbb{F}_Q : \mathbb{F}_P]$.

(b) The second statement follows by taking norms of both sides of the factorisation.

$$P^{[L:K]} = \mathbf{Nm}_{L/K}(P_L) = \prod_{i=1}^{g} \mathbf{Nm}_{L/K}(Q_i)^{e_i} = \prod_{i=1}^{g} (P^{f_i})^{e_i}$$

We get the statement be equating the exponents.

□

Example 12.18. Take $L = \mathbb{Q}(i), K = \mathbb{Q}$. Take $P = 2\mathbb{Z}$. Then $P_L = 2\mathbb{Z}[i]$. We begin by factorising this ideal. This amounts to factorsing 2 in $\mathcal{O}_L = \mathbb{Z}[i]$. Thus we have

$$P_L = ((1+i)\mathcal{O}_L)^2 = Q^2$$

where $Q := (1+i)\mathcal{O}_L$. In this case we have $g = 1$ and $e = 2$ which forces $f = 1$. Alternatively we can also compute f directly. Notice $\mathbb{F}_P = \mathbb{Z}/(2) = \mathbb{F}_2$. Similarly

$$\mathbb{F}_Q = \mathbb{Z}[x]/(x^2+1)/(1+x) = \mathbb{Z}[x]/(1+x)/(x^2+1) = \mathbb{Z}/(2) = \mathbb{F}_2$$

That is $\mathbb{F}_Q = \mathbb{F}_2$ so $f = [\mathbb{F}_Q : \mathbb{F}_P] = 1$.
On the other hand take $P = 3\mathbb{Z}$. Then $P_L = 3\mathcal{O}_L$ is prime. We can find this by considering the quotient

$$\mathcal{O}_L/3\mathcal{O}_L = \mathbb{Z}[x]/(x^2+1)/(3) = \mathbb{F}_3[x]/(x^2+1) = \mathbb{F}_9$$

Therefore $f = [\mathbb{F}_9 : \mathbb{F}_3] = 2$. In total we have $g = 1, e = 1, f = 2$.
The final behaviour we could have is when the prime (ideal) splits into distinct primes. For example take $P = 13\mathbb{Z}$. Then $P_L = 13\mathcal{O}_L = (2+3i)\mathcal{O}_L \cdot (2-3i)\mathcal{O}_L$. In this case we have $g = 2$ so we must have $e_1 = f_1 = 1$ and $e_2 = f_2 = 1$.

Example 12.19. Things were fairly simple in the previous example because of the small degree. For a slightly more complicated example let's take $K = \mathbb{Q}$ (again) and $L = \mathbb{Q}(\zeta)$ where ζ is a fifth root of unity. In other words ζ satisfies

$$1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 = 0$$

We will prove later that the ring of integers $\mathcal{O}_L$ is $\mathbb{Z}[\zeta] = \mathbb{Z}[x]/(x^4+x^3+x^2+x+1)$.
Consider $P = (19)$. We compute

$$\begin{aligned}
\mathcal{O}_L/19\mathcal{O}_L &= \mathbb{Z}[x]/(x^4+x^3+x^2+x+1)/(19) \\
&= \mathbb{F}_{19}[x]/(x^4+x^3+x^2+x+1) \\
&= \mathbb{F}_{19}[x]/(x^2+5x+1)(x^2-4x+1) \\
&= \mathbb{F}_{19^2} \oplus \mathbb{F}_{19^2}
\end{aligned}$$

Therefore we have $g = 2$, $e_1 = e_2 = 1$ and $f_1 = f_2 = 2$.
The factorisation of the polynomial over $\mathbb{F}_{19}$ may be difficult to do. There is another way of seeing why the quartic would split into a product of quadratics. Factorising $f(x) = x^4 + x^3 + x^2 + x + 1$ over $\mathbb{F}_{19}$ is essentially asking what extension of $\mathbb{F}_{19}$ has a fifth room of unity. We deduce this using the very useful fact that $F^\times$, for any finite field, is a cyclic group. This immediately tells us that $\mathbb{F}_{19}$ has no fifth roots of unity since such an element would have order 5 in the multiplicative group but $\left|\mathbb{F}_{19}^\times\right| = 19 - 1 = 18$ so $\mathbb{F}_{19}^\times$ cannot have an element of order 5 (in other words the polynomial $f(x)$ has no solution in $\mathbb{F}_{19}$). On the other hand $\left|\mathbb{F}_{19^2}^\times\right| = 19^2 - 1 = 360$ certainly does have an element of order 5 and this element is of course a fifth root of unity. Thus we conclude that although $f(x)$ has no linear factors, it does have a quadratic factor from which it is immediate that it must be the product of two quadratics. Since the polynomial is separable, it must be the product of distinct quadratic polynomials.

Example 12.20. Finally, let's look at a non-Galois example. As the classic example of such cases, let's take $L = \mathbb{Q}(\sqrt[3]{2})$ and $K = \mathbb{Q}$. We have proven previously that $\mathcal{O}_L = \mathbb{Z}[\sqrt[3]{2}]$. Take $P = (41)$. Then

$$\mathcal{O}_L/P\mathcal{O}_L = \mathbb{F}_{41}[x]/(x^3 - 2) = \mathbb{F}_{41}[x]/(x - 5)(x^2 + 5x + 25)$$

Thus the prime factors of P_L are $Q_1 = (41, \sqrt[3]{2} - 5)$ and $Q_2 = (41, \sqrt[3]{4} + 5\sqrt[3]{2} + 25)$. In other words we have $g = 2, e_1 = 1, f_1 = 1, e_2 = 1$ and $f_2 = 2$.
Once again, even without explicit factorisation, we can deduce that $f(x) = x^3 - 2$ splits as a product of a linear and a quadratic term. First we can simply try all the elements of $\mathbb{F}_{41}$ to check whether any are cube roots of 2. Alternatively, notice that $\left|\mathbb{F}_{41}^\times\right| = 40$ is not a multiple of 3. Thus cubing is an isomorphism of $\mathbb{F}_{41}^\times$ so in particular there is an element (in fact it is unique) whose cube is 2. This also shows that there are no other linear factors since we only found the unique cube root of 2 in $\mathbb{F}_{41}$ while the polynomial is separable (notice $f(x)$ and $f'(x)$ are coprime in $\mathbb{F}_{41}$). Therefore $f(x)$ must be a product of a linear and quadratic factor.
Alternatively, notice we have a cube root of 2 in $\mathbb{F}_{41}$ and the remaining cube roots differ by cube roots of unity. Using the same argument as in the previous example, one can check that although $\mathbb{F}_{41}$ does not have any cube roots of unity, $\mathbb{F}_{41^2}$ does. This is another way to conclude we must have a quadratic term in the factorisation.

12.1 Decomposition and ramification groups

In this section, unless otherwise specified, then L/K is a Galois extension and G will often be used to denote the Galois group $\mathbf{Gal}(L/K)$.

Theorem 12.21 *Let $P \subset \mathcal{O}_K$ be a non-zero prime ideal. Let $Q, Q' \subset \mathcal{O}_L$ be prime ideals dividing P_L. Then there is some $\sigma \in \mathbf{Gal}(L/K)$ such that $\sigma \cdot Q = Q'$. In other words, the Galois group $\mathbf{Gal}(L/K)$ acts transitively on the prime factors of P_L.*

Proof. Suppose

$$P_L = \prod_{i=1}^{g} Q_i^{e_i}$$

One of the Q_i is Q and one of them is Q'. Without loss of generality we can assume $Q = Q_1$ and $Q' = Q_2$. From Theorem 12.16 we know that $P \mid \mathbf{Nm}_{L/K}(Q)$. For any ideals $I, J \subset \mathcal{O}_K$ we have

$$I \mid J \Leftrightarrow I_L \mid J_L$$

(one way to see this is by recalling that divisibility of ideals is equivalent to containment). Therefore, we have

$$\prod_{i=1}^{g} Q_i^{e_i} = P_L \mid (\mathbf{Nm}_{L/K}(Q))_L = \prod_{\sigma \in \mathbf{Gal}(L/K)} \sigma \cdot Q$$

Thus by primality we know there exists some σ in the Galois group such that $Q' \mid \sigma \cdot Q_1$. But since σ is an isomorphism and Q_1 is prime, $\sigma \cdot Q_1$ must also be prime (hence maximal) so we have $Q' = \sigma \cdot Q_1$. □

Corollary 12.22 *Suppose L/K is Galois. Let P be a prime ideal in K and $P_L = \prod_{i=1}^{g} Q_i^{e_i}$ its prime factorisation in L. Then*

$$e_1 = e_2 = \cdots = e_g \text{ and } f_1 = f_2 = \cdots = f_g$$

where, as usual, $f_i = [\mathbb{F}_{Q_i} : \mathbb{F}_P]$. In particular we have

$$[L : K] = efg$$

Definition 12.23 (Decomposition Group)**.** Let L/K be an extension which, as usual in this section, we assume to be Galois. Let $P \subset \mathcal{O}_K$ and let Q be one of the prime factors of P_L. Then we define the *decomposition group* (of Q) by

$$D_Q := \{\sigma \in \mathbf{Gal}(L/K) : \sigma \cdot Q = Q\}$$

Notice that if Q and Q' are both primes dividing P_L then by the above theorem, we know there is some σ in the Galois group taking Q to Q' and so

$$D_{Q'} = \sigma D_Q \sigma^{-1}$$

Thus all these decomposition groups are isomorphic (and indeed are conjugate subgroups of the Galois group).

Example 12.24. Consider $L = \mathbb{Q}(i)$ and $K = \mathbb{Q}$. Take $P = 5\mathbb{Z}$. Then its lift $5\mathcal{O}_L$ is not prime and splits into the product $(1+2i)\mathcal{O}_L \cdot (1-2i)\mathcal{O}_L$. Let's take the first term to be Q and compute D_Q. The Galois group $\mathbf{Gal}(L/K)$ is the group of 2 elements $\{1, \sigma\}$ where σ is the conjugation map. Obviously $1 \in D_Q$ so it only remains to check whether σ fixes Q or not. We compute

$$\sigma \cdot (1+2i)\mathcal{O}_L = (1-2i)\mathcal{O}_L \neq (1+2i)\mathcal{O}_L$$

Thus the decomposition group D_Q in this case is trivial, simply $\{1\}$.

Example 12.25. For another example, consider the same setup as above with $L = \mathbb{Q}(i)$ and $K = \mathbb{Q}$ but with $P = 7\mathbb{Z}$. In this case $7\mathcal{O}_L$ is prime so D_Q must be everything. This is because the Galois

group acts transitiviely on the primes over P but since there is only one prime, all elements of the Galois group must send it to itself.

Every element σ of the Galois group gives an automorphism of the ring of integers $\sigma : \mathcal{O}_L \to \mathcal{O}_L$. If $\sigma \in D_Q$ then σ descends to a quotient $\overline{\sigma} : \mathcal{O}_L/Q \to \mathcal{O}_L/Q$. Notice also that we have $\mathcal{O}_K \subset \mathcal{O}_L$ and $P \subset Q$ so $\mathcal{O}_K/P \subset \mathcal{O}_L/Q$. Moreover since σ is in the Galois group, we know it fixes K and hence it fixes $\mathcal{O}_K$. Putting this altogether we see that $\overline{\sigma} : \mathcal{O}_L/Q \to \mathcal{O}_L/Q$ is a field automorphism fixing $\mathcal{O}_K/P$, which is to say $\overline{\sigma} \in \mathbf{Gal}(\mathbb{F}_Q/\mathbb{F}_P)$. In fact, somewhat surprisingly, every element of $\mathbf{Gal}(\mathbb{F}_Q/\mathbb{F}_P)$ arises in this manner.

Theorem 12.26 *The map $D_Q \to \mathbf{Gal}(\mathbb{F}_Q/\mathbb{F}_P)$ is onto.*

Proof. Choose $\widetilde{\alpha} \in \mathbb{F}_Q$ such that $\mathbb{F}_P(\widetilde{\alpha}) = \mathbb{F}_Q$. Such an $\widetilde{\alpha}$ exists because a finite field extension of any finite field is simple.

Let

$$P_L = \prod_{i=1}^{g} Q_i^{e_i}$$

be its prime decomposition as usual with $Q = Q_1$. Using the Chinese Remainder Theorem, we choose $\alpha \in \mathcal{O}_L$ a lift of $\widetilde{\alpha}$ such that

$$\alpha \equiv \begin{cases} \widetilde{\alpha} \bmod Q_1 \\ 0 \bmod Q_i \text{ for } i > 1 \end{cases}$$

Notice for $\sigma \in \mathbf{Gal}(L/K) \setminus D_Q$ we have $\alpha \in \sigma^{-1} \cdot Q$. This is because we know elements of the Galois group also act as maps on the set of prime factors of P_L. Since σ^{-1} does not fix Q (since σ does not fix Q), we conclude that $\sigma^{-1} \cdot Q = Q_i$ for some $i > 1$. But by choice of α we know $\alpha \in Q_i$ for all $i > 1$. Thus we have $\alpha \in \sigma^{-1} \cdot Q$ or, equivalently, $\sigma\alpha \in Q$. Now consider

$$h(x) := \prod_{\sigma \in G} (x - \sigma\alpha)$$

where G is the Galois group $\mathbf{Gal}(L/K)$. As this polynomial is fixed by the Galois group we conclude that $h(x)$ actually has coefficients in K. To be precise, it must be in $\mathcal{O}_K[x]$. Let $\widetilde{h}(x)$ be its reduction mod Q. Then we have

$$\widetilde{h}(x) = \prod_{\sigma \in G} (x - \overline{\sigma\alpha}) = \prod_{\sigma \in D_Q} (x - \overline{\sigma\alpha}) \cdot \prod_{\sigma \in G \setminus D_Q} (x - \overline{\sigma\alpha}) = \prod_{\sigma \in D_Q} (x - \overline{\sigma\alpha}) \cdot x^{|G \setminus D_Q|}$$

Notice that $h(\widetilde{\alpha}) = 0$ (this is because the identity is always in D_Q). Since $\widetilde{h}(x)$ is (also) a polynomial in $\mathbb{F}_P(x)$, all the conjugates of $\widetilde{\alpha}$ are also roots of $\widetilde{h}(x)$. To be precise, $\widetilde{h}(\tau\widetilde{\alpha}) = 0$ for all $\tau \in \mathbf{Gal}(\mathbb{F}_Q/\mathbb{F}_P)$. But we can see all the roots of $\widetilde{h}(x)$ in the decomposition above. Therefore we conclude that for all $\tau \in \mathbf{Gal}(\mathbb{F}_Q/\mathbb{F}_P)$ we can find $\sigma \in D_Q$ such that $\overline{\sigma\alpha} = \tau\widetilde{\alpha}$. This is exactly saying $\overline{\sigma}(\widetilde{\alpha}) = \tau(\widetilde{\alpha})$ and therefore $\overline{\sigma} = \tau$ since $\widetilde{\alpha}$ is generating. □

As one might expect the kernel of the above map is important and interesting.

Definition 12.27 (Inertia Group)**.** Given L/K Galois and a prime $P \subset \mathcal{O}_K$ with $Q \subset \mathcal{O}_L$ a prime over P, we define the *inertia group* I_Q to be the kernel of the homomorphism $D_Q \to \mathbf{Gal}(\mathbb{F}_Q/\mathbb{F}_P)$.

There are some immediate properties we can conclude about the inertia group.

Corollary 12.28 *Let L/K Galois and a prime $P \subset \mathcal{O}_K$ with $Q \subset \mathcal{O}_L$ a prime over P. Then I_Q is a normal subgroup of D_Q. Moreover $|D_Q/I_Q| = f$ and hence $|I_Q| = |D_Q|/f = e$.*

Proof. The first statement is immediate from the fact that I_Q is the kernel of a homomorphism. The second statement follows from the second isomorphism theorem and the fact that $|\mathbf{Gal}(\mathbb{F}_Q/\mathbb{F}_P)| = [\mathbb{F}_Q : \mathbb{F}_P] = f$. For the last part we need to show that $|D_Q| = ef$. In order to prove this, recall from Corollary 12.22 that $|G| = [L : K] = efg$. Since the Galois group acts transtively on the prime factors of P_L (see Theorem 12.21) we get

$$|D_Q| = \frac{|G|}{g} = ef$$

□

Corollary 12.29 *D_Q/I_Q is cyclic of order f.*

Proof. This is simply because $D_Q/I_Q \cong \mathbf{Gal}(\mathbb{F}_Q/\mathbb{F}_P)$ and the Galois group for any finite field is cyclic. □

There is another way to think of the inertia group.

Proposition 12.30

$$I_Q = \{\sigma \in G : \forall \alpha \in \mathcal{O}_L, \sigma\alpha - \alpha \in Q\}$$

Proof. This is really just a proof of unravelling definitions.

For the first inclusion let $\sigma \in I_Q$ and $\alpha \in \mathcal{O}_L$. Since σ is in I_Q it acts as the identity element in the Galois group $\mathbf{Gal}(\mathbb{F}_Q/\mathbb{F}_P)$. Therefore $\sigma(\overline{\alpha}) = \overline{\sigma(\alpha)} = \overline{\alpha}$ where $\overline{\alpha}$ is the image of α in $\mathbb{F}_Q$. But $\overline{\sigma(\alpha)} = \overline{\alpha}$ in $\mathbb{F}_Q$ is exactly saying $\sigma(\alpha) - \alpha \in Q$.

For the reverse inclusion, suppose σ is an element of the Galois group $\mathbf{Gal}(L/K)$ such that $\sigma\alpha - \alpha \in Q$ for every $\alpha \in \mathcal{O}_L$. First we show that $\sigma \in D_Q$. This is easy to see since $\sigma\alpha = \alpha + (\sigma\alpha - \alpha)$ so if $\alpha \in Q$ then the left hand side is also in Q since we can express it as a sum of things in Q. Now we need to check how $\overline{\sigma}$ acts on $\mathbb{F}_Q$.

Let $\overline{\alpha} \in \mathbb{F}_Q$ be arbitrary and α some lift of it. Then by assumption $\sigma\alpha - \alpha \in Q$. Thus $\overline{\sigma\alpha} = \overline{\alpha}$ in $\mathbb{F}_Q$. Thus $\overline{\sigma}$ acts as the identity map so lies in the kernel of the map $D_Q \to \mathbf{Gal}(\mathbb{F}_Q/\mathbb{F}_P)$. □

We can then also define the ramification group.

Definition 12.31. As with our usual setup let L/K Galois with P a prime in $\mathcal{O}_K$ with Q a prime in $\mathcal{O}_L$ over P. Then we define the *ramification group* by

$$V_Q := \{\sigma \in \mathbf{Gal}(L/K) : \text{for every } \alpha \in \mathcal{O}_L, \sigma\alpha - \alpha \in Q^2\}$$

Remark 12.32. Although we don't do so here, one can also investigate higher ramification groups by asking $\sigma\alpha - \alpha \in Q^n$ for bigger and bigger n. This produces a chain of subgroups that can contain important information about the extension.

Theorem 12.33 *We have the following properties for ramification groups:*

(a) V_Q *is a normal subgroup of* I_Q

(b) $I_Q/V_Q \hookrightarrow \mathbb{F}_Q^\times$

(c) V_Q *is a* p*-group and in fact is the unique* p*-Sylow subgroup of* I_Q

Proof. (a) Since D_Q fixes Q it also fixes Q^2. Thus D_Q acts on $\mathcal{O}_L/Q^2$ and the kernel of this action is exactly V_Q by construction. Therefore V_Q is normal in D_Q so must also be normal I_Q.

(b) Consider the $\mathcal{O}_L$-module Q/Q^2. On this module Q acts as 0 and thus scaling by $\mathcal{O}_L/Q$ is well-defined on Q/Q^2. In particular then, Q/Q^2 is an $\mathbb{F}_Q$-vector space. Let's determine its dimensions

$$\left|Q/Q^2\right| = [Q : Q^2] = \frac{[\mathcal{O}_L : Q]}{[\mathcal{O}_L : Q^2]} = \frac{\mathsf{Norm}(Q)}{\mathsf{Norm}(Q^2)} = \mathsf{Norm}(Q) = |\mathbb{F}_Q|$$

Therefore Q/Q^2 is a 1-dimensional vector space over $\mathbb{F}_Q$. In fact we claim $\sigma \in I_Q$ defines a vector space isomorphism of this vector space. The first thing we need to check is that σ is well-defined with respect to the quotient. We only need to check that σ sends Q^2 to Q^2. But every element of Q^2 is (possibly some linear combination of) elements of the form $\alpha\beta$ where $\alpha, beta$ are both elements of Q. We know σ sends Q to Q so $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$ lies in Q^2.

We already know σ respects addition so it only remains to check that σ respects scaling in $\mathbb{F}_Q$. Therefore let $\alpha \in \mathbb{F}_Q$ and $\bar{t} \in Q/Q^2$. Then we have

$$\sigma(\alpha\bar{t}) = \sigma(\alpha)\sigma(\bar{t}) = \alpha\sigma(\bar{t})$$

where we use the fact that $\sigma(\alpha) \equiv \alpha \bmod Q$. Thus we have the map

$$\phi : I_Q \to \mathbf{Aut}(Q/Q^2) = \mathbb{F}_Q^\times$$

We claim the kernel of this map is exactly I_Q (this gives the statement of theorem by the first isomorphism theorem). One of the inclusions is easy. Suppose $\sigma \in V_Q$. Then $\sigma(t) \equiv t \bmod Q^2$ which is to say σ acts trivially on Q/Q^2. The converse takes a little more work.

Now suppose $\sigma \in \ker(\phi)$. This means for all $\alpha \in Q$, we have $\sigma(\alpha) \equiv \alpha \bmod Q^2$. Since $\sigma \in I_Q$, it also acts trivially on $\mathbb{F}_Q$. In order to show that $\sigma \in V_Q$ we will argue that σ acts trivially on $\mathcal{O}_L/Q^2$. We claim we have

$$\mathcal{O}_L/Q^2 = (\mathcal{O}_L/Q^2)^\times \cup (1 + (\mathcal{O}_L/Q^2)^\times)$$

In order to see this let $\overline{\alpha} \in \mathcal{O}_L/Q^2$. Notice that the only ideals in $\mathcal{O}_L/Q^2$ are $\{0\}, \mathcal{O}_L/Q$ and $\mathcal{O}_L/Q^2$ (if there were any other ideals then there would be a (non-trivial) ideal dividing Q^2 different from Q). Then $(\overline{\alpha})$ is either $\mathcal{O}_L/Q$ or $\mathcal{O}_L/Q^2$ (of course it is non-zero). If $(\overline{\alpha}) = \mathcal{O}_L/Q^2$ then $\overline{\alpha}$ is a unit since it generates the entire ring. Now suppose $\overline{\alpha}$ and $1 - \overline{\alpha}$ are both non-units. Then $(\overline{\alpha}) = (1 - \overline{\alpha}) = \mathcal{O}_L/Q$. Since they generate the same ideal we conclude $\overline{\alpha} = u(1 - \overline{\alpha})$ where u is a unit in $\mathcal{O}_L/Q^2$. But this gives

$$1 = \overline{\alpha} + (1 - \overline{\alpha}) = u(1 - \overline{\alpha}) + (1 - \overline{\alpha}) = (1 - \overline{\alpha})(u + 1)$$

So that $1 - \overline{\alpha}$ is a unit contradicting our assumption. Thus at least one of $\overline{\alpha}$ and $1 - \overline{\alpha}$ must be a unit.

The next lemma shows that $(\mathcal{O}_L/Q^2)^\times = \mathbb{F}_Q^\times \oplus Q/Q^2$. Therefore σ fixes $(\mathcal{O}_L/Q^2)^\times$ and by the above decomposition it must fix all of $\mathcal{O}_L/Q^2$. Therefore $\sigma \in V_Q$.

(c)

□

Lemma 12.34 *Let $\pi : \mathcal{O}_L/Q^2 \to \mathcal{O}_L/Q = \mathbb{F}_Q$ be the projection map. Then $(\mathcal{O}_L/Q^2)^\times = \pi^{-1}(\mathbb{F}_Q^\times)$ and in fact*

$$(\mathcal{O}_L/Q^2)^\times \cong Q/Q^2 \oplus \phi(\mathbb{F}_Q^\times)$$

where $\phi : \mathbb{F}_Q^\times \to (\mathcal{O}_L/Q^2)^\times$ is given by $\phi(\alpha) = \widetilde{\alpha}^{Norm(Q)}$ where $\widetilde{\alpha}$ is a representative of α.

Proof. For notational convenience, define $R := \mathcal{O}_L/Q^2$ and $N := \mathrm{Norm}(Q)$. If $\alpha \in R^\times$ then certainly $\pi(\alpha) \in \mathbb{F}_Q^\times$ since homomorphisms carry units to units. Thus we immediately get $R^\times \subset \pi^{-1}(\mathbb{F}_Q^\times)$. In order to get the reverse inclusion let $\alpha \in \pi^{-1}(\mathbb{F}_Q^\times)$ and consider the ideal $I = (\alpha)$. The only possibilities for I are $I = R$ or $I = Q/Q^2$ as these are in the only non-zero ideals in R. We cannot have $I = Q/Q^2$ since that would imply that $\alpha \in Q$ so $\pi(\alpha) = 0$ would not be invertible. Thus we must have $I = R$. Since α generates the entire ring it must be a unit of R. This gives the exact sequence

$$0 \to Q/Q^2 \to \mathbb{R}^\times \to \mathbb{F}_Q^\times \to 0$$

where the map $Q/Q^2 \to R^\times$ is given by $t \mapsto 1 + t$. Notice this is indeed a homomorphism where the operation on the domain is addition and on the codomain is multiplication. So for example the inverse of $1 + t$ is $1 - t$ since $(1 + t)(1 - t) = 1 - t^2 = 1 \in R$ since $t^2 \in Q^2$.

We define a map $\phi : \mathbb{F}_Q^\times \to R^\times$ given by $\phi(\alpha) = \widetilde{\alpha}^N$ where $\widetilde{\alpha}$ is any representative of α. This is well-defined. If $\widetilde{\alpha}_1$ and $\widetilde{\alpha}_2$ are two representatives of α then

$$\widetilde{\alpha}_2^N = (wt\alpha_1 + (\widetilde{\alpha}_2 - \widetilde{\alpha}_1))^N = \widetilde{\alpha}_1^N + N(\widetilde{\alpha}_2 - \widetilde{\alpha}_1) + \binom{N}{2}\widetilde{\alpha}_1^{N-1}(\widetilde{\alpha}_2 - \widetilde{\alpha}_1)^2 + \cdots$$

Notice that every thing after the first term lies in Q^2 (in particular $\widetilde{\alpha}_2 - \widetilde{\alpha}_1 \in Q$ since they represent the same element of $\mathbb{F}_Q$ and N lies in Q since the norm of any ideal lies in the ideal). Thus the exact sequence splits and we conclude

$$R^\times \cong Q/Q^2 \oplus \phi(\mathbb{F}_Q^\times)$$

□

Example 12.35. The lemma above and its proof may solidify if we consider an example. Consider the case where $L = \mathbb{Q}(\sqrt{7})$. Then $\mathcal{O}_L = \mathbb{Z}[\sqrt{7}]$. Let's take $Q = \sqrt{7} \cdot \mathcal{O}_L$. Then $R = \mathbb{Z}[\sqrt{7}]/(\sqrt{7})^2 \cong \mathbb{F}_7[t]/(t^2)$. Then the exact sequnce is given by

$$0 \to t\mathbb{F}_7[t]/(t^2) \to (\mathbb{F}_7[t]/(t^2))^\times \to \mathbb{F}_7 \to 0$$

Let's describe all the units in $\mathbb{F}_7[t]/(t^2)$. By the above lemma this group of units is isomorphic to $(t)/(t^2) \oplus \mathbb{F}_7^\times$. We can describe this isomorphism explicitly. Given $\alpha \in \mathbb{F}_7$, we define $\widetilde{\alpha} = \alpha + \beta t$ for any $\beta \in \mathbb{F}_7$. Then

Proposition 12.36 *Let L/K be a Galois extension and $Q \subset \mathcal{O}_L$ a prime lying over some prime in $\mathcal{O}_K$. Then the ramification group V_Q is a p-group and $p\mathbb{Z} = Q \cap \mathbb{Z}$.*

Proof. Let $\sigma \in V_Q$ □

The next thing to consider is how the decomposition groups, inertial groups and ramification groups behave with one another when we have a chain of Galois extensions. In fact the relationships are exactly what one would expect. So let $L/K/F$ be Galois extensions and $R \subset \mathcal{O}_L$ prime. Define $Q := R \cap \mathcal{O}_K$ and $P := R \cap \mathcal{O}_F$. Let $G := \mathbf{Gal}(L/F)$ and $H := \mathbf{Gal}(L/K)$. We use $D_{L/K}, I_{L/K}, V_{L/K}$ to denote the decomposition, inertial and ramification groups for R over K and similarly define $D_{L/F}, I_{L/F}, V_{L/F}$ for the corresponding groups for R over F.

Theorem 12.37 *(a)* $D_{L/K} = D_{L/F} \cap H$

(b) $I_{L/K} = I_{L/F} \cap H$

(c) $V_{L/K} = V_{L/F} \cap H$

Proof. (a) $D_{L/K} = \{\sigma \in H : \sigma \cdot R = R\} = \{\sigma \in G : \sigma \cdot R = R\} \cap H = D_{L/F} \cap H$

(b) $I_{L/K} = \{\sigma \in D_{L/K} : \sigma|_{\mathbb{F}_R} \text{ is trivial}\} = \{\sigma \in D_{L/F} : \sigma|_{\mathbb{F}_R} \text{ is trivial}\} \cap D_{L/K} = I_{L/F} \cap D_{L/K} = I_{L/F} \cap H$

(c) $V_{L/K} = \{\sigma \in I_{L/K} : \sigma|_{\mathcal{O}_L/R^2} \text{ is trivial}\} = \{\sigma \in I_{L/F} : \sigma|_{\mathcal{O}_L/R^2} \text{ is trivial}\} \cap I_{L/K} = V_{L/F} \cap I_{L/K} = V_{L/F} \cap H$

□

Since K/F is Galois we can also consider the groups $D_{K/F}, I_{K/F}, V_{K/F}$ relative to Q over F. These groups are exactly the projections of the groups for R over F.

Theorem 12.38 *Let $\pi : G \to G/H$ be the projection map (since K/F is Galois we know H is normal in G). Then*

(a) $D_{L/K} = \pi(D_{L/F})$

(b) $I_{L/K} = \pi(I_{L/F})$

(c) $V_{L/K} = \pi(V_{L/F})$

Proof. (a) Let $\sigma \in D_{L/F}$. We want to show that $\pi(\sigma)$ fixes Q. Since $\sigma \in D_{L/F}$ by definition we have $\sigma \cdot R = R$. Therefore

$$\sigma(Q) = \sigma(R \cap \mathcal{O}_K) = \sigma(R) \cap \sigma(O_K) = R \cap \mathcal{O}_K = Q$$

For the reverse inclusion, let $\tau \in D_{K/F} \subset \mathbf{Gal}(K/F) \cong G/H$. By definition, we have $\tau \cdot Q = Q$. Let $\sigma \in \pi^{-1}(\tau)$. We would like to say σ fixes R which would give us $\sigma \in D_{L/F}$. Of course this need not be the case but we can modify σ so that this happens. Notice that because $\pi(\sigma)$ fixes Q we have $\sigma(R) \supset \sigma(Q_L) = Q_L$. Therefore $\sigma(R) \mid Q_L$. In particular then R and $\sigma(R)$ are both prime factors of Q_L so by Theorem 12.21 we conclude there exists $\sigma_0 \in H$ such that $\sigma_0(\sigma(R)) = R$. Therefore $\sigma_0\sigma \in D_{L/F}$ and $\pi(\sigma_0\sigma) = \pi(\sigma_0)\pi(\sigma) = \tau$ (notice $\pi(\sigma_0) = 1$ since $\sigma_0 \in H$).

(b) Suppose $\sigma \in I_{L/F}$. Then, by definition, we know σ acts trivially on $\mathbb{F}_R$. But since $\mathbb{F}_Q \subset \mathbb{F}_R$ this means that σ also acts trivially on $\mathbb{F}_Q$. Thus we get $\pi(\sigma) \in I_{K/F}$. For the converse inclusion, let $\tau \in I_{K/F} \subset D_{K/F} = \pi(D_{L/F})$. Thus we can choose some $\sigma \in \pi^{-1}(\tau) \cap D_{L/F}$. Although σ might not lie in $I_{L/F}$, we show we can modify it by something in H so that the composition lies in $I_{L/F}$. In order to be an element of $I_{L/F}$ we would need σ to fix $\mathbb{F}_R$ (this is the definition of the inertia group). Although σ does indeed act on $\mathbb{F}_R$ (since it lies in $D_{L/F}$), there is not reason it needs to fix it. On the other hand, it does fix $\mathbb{F}_Q \subset \mathbb{F}_R$ (since $\pi(\sigma) \in I_{K/F}$). Thus σ defines an element, say a_σ of $\mathbf{Gal}(\mathbb{F}_R/\mathbb{F}_Q)$

Notice by definition, σ acts on $\mathbb{F}_R$ (because it is an element of $D_{L/F}$) and fixes $\mathbb{F}_Q$ (because $\pi(\sigma) \in I_{K/F}$). Thus σ gives an element of $\mathbf{Gal}(\mathbb{F}_R/\mathbb{F}_Q)$ which we denote a_σ. Recall the map $D_{L/K} \to \mathbf{Gal}(\mathbb{F}_R/\mathbb{F}_Q)$ is onto (by Theorem 12.26) which we means there exists $\sigma_0 \in D_{L/K} \subset H$ such that it is sent to a_σ. Then $\sigma_0^{-1}\sigma$ fixes $\mathbb{F}_R$ so $\sigma_0\sigma \in I_{L/F}$ and $\pi(\sigma_0^{-1}\sigma) = \pi(\sigma) = \tau$.

(c) Consider the map $\pi_0 : I_{L/F} \to I_{K/F}$. We know $V_{L/F}$ is the unique p-Sylow subgroup of $I_{L/F}$ (by Theorem 12.33). Then since π_0 is onto we have $\pi_0(V_{L/F}) \subset I_{K/F}$ is the unique p-Sylow normal subgroup (this is a purely group theoretic fact). Therefore $\pi_0(V_{L/F}) = V_{L/K}$.

□

Lemma 12.39 *Let G, H be groups and $pi : G \to H$ a surjective group homomorphism. If $M \lhd G$ is a (unique) p-Sylow subgroup, then $\pi(M)$ is a (unique) p-Sylow subgroup.*

Proof. Since π is onto we certainly have that $\pi(M)$ is a normal p-group of H. Thus π induces a (surjective) map $G/M \to H/\pi(M)$. Since M was p-Sylow we know $p \not| |G/M|$ and thus $p \not| |H/\pi(M)|$. Therefore $\pi(M)$ is a p-Sylow subgroup of H. □

Definition 12.40. Let L/K be number fields and $Q \subset \mathcal{O}_K$ a prime ideal and $Q_L = \prod_{i=1}^{g} P_i^{e_i}$ its factorisation (in L). Then we say Q ramifies in L if there exists some $e_i > 1$. Equivalently, Q ramifies in L if it is *not* squarefree.

Theorem 12.41 *Let L/Q be an extension of number fields and p a prime integer. Then $p\mathbb{Z}$ ramifies in L if and only if p divides Disc(L).*

Proof. Define $R := \mathcal{O}_L/p\mathcal{O}_L$. Since R is an $\mathbb{F}_p$-vector space so we can consider $\text{Disc}(R, \text{tr}_{R/\mathbb{F}_p})$ defined analogously to the the discriminant of fields over $\mathbb{Q}$. In fact, we have that $\text{Disc}(L) \equiv \text{Disc}(R, \text{tr}_{R/\mathbb{F}_p}) \bmod p$. Thus by Lemma 6.10, we have

$$p \mid \text{Disc}(L) \Leftrightarrow \text{tr}_{R/\mathbb{F}_p} : R \times R \to \mathbb{F}_p \text{ is degenerate}$$

where recall degeneracy means there exists some non-zero x such that for every y we have $\text{tr}_{R/\mathbb{F}_p}(x, y) = 0$.

Now suppose we have the factorisation $p\mathcal{O}_L = \prod_{i=1}^{g} Q_i^{e_i}$ so that by Chinese Remainder Theorem we have

$$R = \mathcal{O}_L/p\mathcal{O}_L \cong \bigoplus_{i=1}^{g} \underbrace{\mathcal{O}_L/Q_i^{e_i}}_{R_i}$$

First suppose p does not ramify in L. Then we will show the trace is non-degenerate. Since all the e_i are 1 we know $R_i = \mathcal{O}_L/Q_i$ is a field $\mathbb{F}_{Q_i}$. Let $\alpha \in R$ be any non-zero element. By the above identification we can write $\alpha = (\alpha_1, \ldots, \alpha_g)$ where each $\alpha_i \in \mathbb{F}_{Q_i}$. Since α is non-zero, there is some j such that α_j is non-zero. Then set $\beta = (\beta_1, \ldots, \beta_g)$ where $\beta_i = 0$ for $i \neq j$ and $\beta_j = \alpha_j^{-1}$. Then $\alpha\beta$ is 1 in the j-th coordinate and 0 everywhere else. Thus in particular $R_j \subset \alpha R$. We claim that $\text{tr}_{R_j/\mathbb{F}_p} : R_j \to \mathbb{F}_p$ is onto so in particular we can find some $\beta \in R$ such that $\text{tr}_{R/\mathbb{F}_p}(\alpha\beta)$ is non-zero.

Lemma 12.42 *If $\mathbb{F}_{q^n}/\mathbb{F}_q$ is a finite field extension, then $\text{tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q} : \mathbb{F}_{q^n} \to \mathbb{F}_q$ is surjective.*

Remark 12.43. This is a non-trivial statement. The trace map for the extensions $\mathbb{F}_p(t)/\mathbb{F}_p(t^p)$ is 0.

Proof. Recall that the trace is sum of all the conjugates of an element. Further recall that the Galois group $\mathbf{Gal}(\mathbb{F}_{q^n}/\mathbb{F}^q)$ is the cyclic group of order n generated by the Frobenius map $x \mapsto x^q$. Thus if $x \in \mathbb{F}_{q^n}$, its conjugates are $x^q, x^{q^2}, \ldots$ so that the trace map is given by

$$\text{tr}(x) = x + x^q + x^{q^2} + \cdots + x^{q^{n-1}}$$

This is a polynomial with at most q^{n-1} distinct roots so there must be some α such that $\text{tr}(\alpha)$ is non-zero. Since the codomain is one-dimensional this means that the trace map is onto. □

Now suppose p ramifies in L. Then without loss of generality, we can assume that $e_1 > 1$. Then consider $\pi \in Q_1 \setminus Q_1^2$. Then we can consider $\overline{\pi} \in \mathcal{O}_L/Q_1^{e_1}$ which is non-zero. Notice we have $\alpha = (\overline{\pi}, 0, \ldots, 0)$ is nilpotent since $\alpha^{e_1} = 0$. Then $\alpha\beta$ is nilpotent for every $\beta \in R$. Since nilpotent elements have trace 0, we conclude that the trace map is degenerate in this case and thus $p \mid \text{Disc}(L)$. □

Although we don't prove it there is a slightly stronger version of the statement.

Theorem 12.44 *Let p be a (positive) prime integer. Let $L/\mathbb{Q}$ be a field extension and $p\mathcal{O}_L = \prod Q_i^{e_i}$ a factorisation. Then*

1. *$p^{\sum(e_i-1)f_i} \mid Disc(L)$*
2. *$\sum(e_i-1)f_i$ is the exact power of p dividing $Disc(L)$ if and only if $p \nmid e_i$ for all i (if p divides some e_i we say that p is wildly ramified)*

13 Cyclotomic fields

Let p be an odd prime. Let $\zeta_p \in \mathbb{C}$ be a p-th root of unity. Then we define $K_p := \mathbb{Q}(\zeta_p)$. Notice that K_p automatically contains all the other p-th roots of unity since they are simply the powers of ζ_p. Thus we get the following nice statement.

Corollary 13.1 *The extension $K_p/\mathbb{Q}$ is Galois and has degree $p-1$.*

Proof. K_p is the splitting field of $x^p - 1$ thus it is Galois. The calculation of the degree takes a bit more work. It is immediate that the degree of the extension is at most $x^p - 1$ has a factor of degree $p-1$. □

Proposition 13.2 *If p is a prime integer then $[K_p : \mathbb{Q}] = p-1$. The ideal $P := (1-\zeta_p)$ is prime and $\mathbb{F}_P \cong \mathbb{F}_p$.*

Proof. The fact that the degree of the extension is at most $p-1$ is clear, since $x^p - 1$ has a factor of degree $p-1$. In order to see that the degree is exactly $p-1$, consider

$$f_p(x) := \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1 = \prod_{a=1}^{g}(x - \zeta_p^a)$$

Thus we have the relation

$$p = f_p(1) = \prod_{a=1}^{p-1}(1 - \zeta_p^a) \tag{13.1}$$

Notice we have $1 - \zeta_p \mid 1 - \zeta_p^a$. But since ζ_p^a is also a generator for the p-th roots of unity so there exists b such that $(\zeta_p^a)^b = \zeta_p$. This means $1 - \zeta_p^a \mid 1 - (\zeta_p^a)^b = 1 - \zeta_p$ (another way of thinking about this is all the p-th roots of unity are algebraically indistinguishable from each other so any relation like

the above one should be symmetrical). Therefore we get $(1-\zeta_p) = (1-\zeta_p^a)$ as ideals in $\mathcal{O}_{K_p}$. Then define $P := (1-\zeta_p)$ so by taking ideals of both sides of Equation 13.1 we get

$$(p) = P^{p-1}$$

Recall the relation $efg = [K_p : \mathbb{Q}]$ (see Corollary 12.22). By the above relation, we have e must be at least $p-1$. Since $[K_p : \mathbb{Q}] \leq p-1$, we conclude the degree is exactly $p-1$ with $e = p-1$ and $f = 1, g = 1$. Therefore P must be prime since $g = 1$ and since $f = 1$, we have $\mathbb{F}_P \cong \mathbb{F}_p$. □

Let's begin by computing the ring of integers. In this case, it is exactly what one would expect.

Proposition 13.3 $\mathcal{O}_{K_p} = \mathbb{Z}[\zeta_p]$

Proof. We will prove this by first computing the discriminant of $\mathbb{Z}[\zeta_p]$ and show no (proper) sublattice of it can be the ring of integers.

Consider the basis $\langle \zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1} \rangle$ for $\mathbb{Z}[\zeta_p]$. Then we have $\mathrm{tr}_{K_p/\mathbb{Q}}(1) = [K_p : \mathbb{Q}] = p-1$ and $\mathrm{tr}_{K_p/\mathbb{Q}}(\zeta_p^j) = \sum_{k=1}^{p-1} \zeta_p^k = -1$ for every j. Thus we have

$$\begin{aligned}
\mathrm{Disc}(\mathbb{Z}[\zeta_p]) &= \det(\mathrm{tr}(\zeta_p^i \zeta_p^j)_{i,j=1}^{p-1}) \\
&= \det \begin{pmatrix} -1 & \cdots & -1 & p-1 \\ -1 & \cdots & p-1 & -1 \\ \vdots & \iddots & \vdots & \vdots \\ p-1 & \cdots & -1 & -1 \end{pmatrix} \\
&\xrightarrow{\text{permute rows}} (-1)^{(p-1)/2} \det \begin{pmatrix} p-1 & -1 & \cdots & -1 \\ -1 & p-1 & \cdots & -1 \\ \vdots & \vdots & \ddots & \vdots \\ -1 & -1 & -1 & p-1 \end{pmatrix} \\
&\xrightarrow{\text{replace row 1 with sum of all rows}} (-1)^{(p-1)/2} \det \begin{pmatrix} 1 & 1 & \cdots & 1 \\ -1 & p-1 & \cdots & -1 \\ \vdots & \vdots & \ddots & \vdots \\ -1 & -1 & -1 & p-1 \end{pmatrix} \\
&\xrightarrow{\text{Add row 1 to all rows}} (-1)^{(p-1)/2} \det \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 0 & p & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & p \end{pmatrix} \\
&= (-1)^{(p-1)/2} p^{p-2}
\end{aligned}$$

There are a couple different ways to finish from here. The easiest way to finish is to appeal to Theorem 12.44. By the proof of Proposition 13.2, we know $p\mathcal{O}_L = P^{p-1}$ thus by Theorem 12.44 we conclude that p^{p-2} must divide the discriminant and hence $\mathbb{Z}[\zeta_p]$ must be the ring of integers itself (any sublattice would necessarily only be divisible by a smaller power of p).

Alternatively, we can argue as follows so we don't have to resort to an unproven theorem. Suppose $\mathbb{Z}[\zeta_p]$ is not the entire ring of integers $\mathcal{O}_{K_p}$ but rather a strict sublattice of it. Then we can find an element that lies in $1/p\mathbb{Z}[\zeta_p] \setminus \mathbb{Z}[\zeta_p]$ (in other words some y which lies outside of $\mathbb{Z}[\zeta_p]$ but py lies in $\mathbb{Z}[\zeta_p]$). In order to see why, notice the discriminant of $\mathbb{Z}[\zeta_p]$ is a power of p, we know $[\mathcal{O}_{K_p} : \mathbb{Z}[\zeta_p]]$ is also a power of p. So in particular, there is some b such that $p^b\mathcal{O}_{K_p} \subset \mathbb{Z}[\zeta_p]$. Thus if we take any $y \in \mathcal{O}_{K_p} \setminus \mathbb{Z}[\zeta_p]$, we can find minimal $c > 0$ such that $p^c y \in \mathbb{Z}[\zeta_p]$. Replacing y with $p^{c-1}y$ we get the desired element.

But now recall $(1-\zeta_p)^{p-1} = p\mathcal{O}_K$. Thus we have $(1-\zeta_p)^{p-1}y \in \mathbb{Z}[\zeta_p]$. Let $c > 0$ be minimal such that $(1-\zeta_p)^c y \in \mathbb{Z}[\zeta_p]$. As before, we can take $z = (1-\zeta_p)^{c-1}y$. This gives an element that lies in $1/(\zeta_p - 1)\mathbb{Z}[\zeta_p] \setminus \mathbb{Z}[\zeta_p]$. But this means $1/(\zeta_p - 1)$ is an algebraic integer but we know this cannot be the case since, for example, its norm is $1/p$ which is not an integer. □

Let's finish with some discussion of class groups in quadratic fields which are simple enough to be easy to calculate and play with but remain complex enough to have interesting patterns and relations.

Let D be a square free integer. Let $K = \mathbb{Q}(\sqrt{D})$ and D_K be the discriminant of this field. In other words

$$D_K = \begin{cases} 4D \text{ if } D & equiv 2, 3 \bmod 4 \\ D \text{ if } D & equiv 1 \bmod 4 \end{cases}$$

Let p be a prime dividing D_K. Then by Theorem 12.41, we know p ramifies in K. Since the degree of the extension is 2, we must have $p\mathcal{O}_K$ is a square (use Corollary 12.22). Let M_p be the 'square root' of the ideal. In other words $M_p^2 = p\mathcal{O}_K$. Thus we have

$$\left(\prod_{p|D_K} M_p\right)^2 = \prod_{p|D_K} p\mathcal{O}_K = \begin{cases} D_K/2 \cdot \mathcal{O}_K \text{ if } D \equiv 2, 3 \bmod 4 \\ D_K\mathcal{O}_K \text{ if } D \equiv 1 \bmod 4 \end{cases}$$

With the notation set up, we have the following theorem.

Theorem 13.4 *Let $D < 0$. Then $\{[M_p] : p$ is a prime dividing $D_K\}$ span an $\mathbb{F}_2$-vector space of dimension $\omega(D_K) - 1$, where $\omega(D_K)$ is the number of primes that ramify in K, or equivalently, the number of primes dividing D_K.*

Remark 13.5. It's perhaps worth discussing what exactly the statement of the theorem means. Label the prime factors of D_K by $p_1, \ldots, p_n$. Then if $e_1, \ldots, e_n$ are any integers then the product $[M_{p_1}]^{e_1} \cdots [M_{p_n}]^{e_n}$ is an element of $\mathbf{Cl}(K)$. Actually, by construction each $[M_{p_i}]$ has order 2 in $\mathbf{Cl}(K)$ so we only need to consider powers up to multiples of 2, i.e. $e_1, \cdots, e_n$ lying in $\mathbb{F}_2$. This is the sense in which the $[M_{p_i}]$ span an $\mathbb{F}_2$-vector space.

Proof. In order to show that the $[M_{p_i}]$ span an $\mathbb{F}_2$-vector space of dimension $\omega(D_K) - 1$ we need to show that the collection of all $[M_{p_i}]$ satisfies exactly one linear relation. It is easy to find such a relation

(because we are working over $\mathbb{F}_2$ this simply amounts to finding a product that is trivial in the class group).

Notice we have

$$\left(\prod_{p|D} M_p\right)^2 = D\mathcal{O}_K(\sqrt{D}\mathcal{O}_K)^2$$

By prime factorisation of ideals we conclude

$$\prod_{p|D} M_p = \sqrt{D}\mathcal{O}_K$$

and hence this product is trivial in the class group (as a side note, notice that the prime factors of D and are almost exactly the prime factors of D_K, with the possible exception of an extra 2 occurring if $D_K = 4D$. Other than that all prime factors appear exactly once as D is square free).

Now we show that there are no other relations among the S (i.e. any other collection of the $[M_p]$ is linearly independent). So suppose $S \subset \{p : p \mid D_K\}$ such that

$$\prod_{p\in S} M_p = \alpha\mathcal{O}_K$$

for some $\alpha \in \mathcal{O}_K$. We will show this leads to a contradiction.

We can write $\alpha = a + b\sqrt{D}$. Suppose $D \cong$ □