ALGEBRAIC NUMBER THEORY

ASHWIN IYENGAR

Contents

1. Motivation

1.1. **Fermat.** A large part of the motivation for algebraic number theory comes from trying to solve Diophantine equations. In other words, if we take a polynomial $p(\underline{x}) \in \mathbb{Z}[x_1, \ldots, x_n]$, we can ask which values $\underline{a} = (a_1, \ldots, a_n) \in \mathbb{Z}^n$ satisfy $p(\underline{a}) = 0$. This is an extremely difficult question in general, as illustrated by the following theorem.

Theorem 1.1.1 (Matyasevich–Robinson–Davis–Putnam)**.** *There exists no algorithm which takes an arbitrary polynomial in a finite number of variables with $\mathbb{Z}$ coefficients and determines whether or not it has a solution.*

Moreover, in any given axiomatization of number theory, one can prove that there exists such a polynomial which has no solutions, but one cannot prove this from the axioms.

This means that if we want to solve Diophantine equations, we have to find some deeper structure in a particular equation in order to approach it.

Let's pick a particularly famous example with a long and tumultuous history: fix a positive integer n and consider

$$p(x) = x^n + y^n - z^n$$

In other words, we want to look for triples $(x, y, z) \in \mathbb{Z}^3$ such that $x^n + y^n = z^n$.

- For $n = 1$, the solutions are easy to classify.
- For $n = 2$ the solutions are called *Pythagorean triples*, and it is known completely how to classify them. There are a few different (essentially similar) proofs, but the basic idea is to factor the equation as
$$(x + iy)(x - iy) = z^2$$
(where $i^2 = -1$) and use properties of "prime numbers" in the ring
$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\},$$
which is the ring of *Gaussian integers*. We will come back to this ring later, but you can already get a hint at how solving equations in $\mathbb{Z}$ might involve working with numbers slightly more general than ordinary integers.
- For $n > 2$:

  Theorem 1.1.2 ("Fermat's Last Theorem", due to work of many many people)**.** *There exist no solutions to $x^n + y^n = z^n$ for $n > 2$ and $xyz \neq 0$.*

  While this course will *not* cover the general proof, which uses the so-called "modularity of elliptic curves", we will now talk about some special cases.

Let's focus more on the $n > 2$ case. First let's perform a reduction step. If $n = pm$ for p an odd prime, then $x^n + y^n = z^n$ implies $(x^m)^p + (y^m)^p = (z^m)^p$. If not, then $n = 2^r$, and then $x^n + y^n = z^n$ implies $(x^{2^{r-2}})^4 + (y^{2^{r-2}})^4 = (z^{2^{r-2}})^4$. So we are reduced to proving Fermat's Last Theorem for $n = 4$ and $n = p$ an odd prime.

Fermat famously claimed to have proven his "Last Theorem", but unfortunately his proof didn't fit into the margins. It is widely suspected that he had a proof which worked in certain cases, but which fails in general for reasons that will become the general theme of the course. The case $n = 4$, for which Fermat gave a complete proof, can be done by the method of *infinite descent*, and is left as an exercise.

Exercise 1.1.3. Complete Problem 2 in https://services.math.duke.edu/~jdr/mathcamp/hw1.pdf.

The odd prime case is *much* harder, and the eventual proof was only completed in the 1990s by Andrew Wiles and his student Richard Taylor, although it built on important work of many many other people. On the other hand, specific cases are accessible by elementary methods.

Example 1.1.4. Let's think about the case $p = 3$. As before, we want to *factorize* $x^3 + y^3$, and we do so as follows. Let $\zeta_3 = e^{2\pi i/3}$ so that $\zeta_3^3 = 1$ (we say that ζ_3 is a *primitive third root of unity*). Then

$$z^3 = x^3 + y^3 = (x + y)(x + \zeta_3 y)(x + \zeta_3^2 y), \tag{1}$$

and as before, we now want to use properties of "prime numbers" in the ring

$$\mathbb{Z}[\zeta_3] = \{a + b\zeta_3 : a, b \in \mathbb{Z}\},$$

In the end, one ends up showing that the three factors on the right side of Equation 1 are either coprime or share one factor in common depending on whether $3 \mid xyz$. In both cases there is an argument using congruences that leads to a contradiction which we will see later in the course once we understand class groups better.

The thing that I haven't yet said is that so far in the examples I've given the rings $\mathbb{Z}[i]$ and $\mathbb{Z}[\zeta_3]$ are *unique factorization domains*, which is why the arguments work. This basically means that any number in $\mathbb{Z}[i]$ can be uniquely factored into "prime numbers". Thus far it's not even clear what we mean by "prime numbers", but we will talk about this in a bit. Note that to make the argument above work we already need this notion, because we used the word "coprime" in the above paragraph. However in general we will not have unique factorization: already $\mathbb{Z}[\zeta_{23}]$ is not a UFD.

1.2. **Pell.**

So far we have reduced the study of a family of Diophantine equations to understanding rings obtained by taking $\mathbb{Z}$ and adjoining roots of 1. Here is another equation, known as *Pell's equation*, which we can use to motivate our study of another class of algebraic number rings:

$$x^2 - ny^2 = 1.$$

Remark 1.2.1. Historically these equations were studied because a solution implies a rational approximation to $\sqrt{n}$: indeed the equation rewrites as $(x/y)^2 - n = 1/y^2$, so if y is large enough then we get a decent approximation.

So we want to classify solutions to this equation. How do we do it? Surprise, we factor the sum:

$$1 = x^2 - ny^2 = (x + \sqrt{n}y)(x - \sqrt{n}y)$$

and now we can try to study the ring $\mathbb{Z}[\sqrt{n}]$. But this time instead of thinking about "prime numbers" in this ring, we note that a solution to the above equation is a *unit* in $\mathbb{Z}[\sqrt{n}]$ (a unit is a number x such that there exists y so that $xy = 1$). So this gives us a reason to try to understand the units in number rings. One of our goals will be to prove the following:

Theorem 1.2.2 (Dirichlet's Unit Theorem)**.** *Let K be a number field with r_1 real embeddings and r_2 complex conjugate pairs of complex embeddings. If $\mathcal{O}_K$ denotes the ring of integers in K, then*

$$\mathcal{O}_K^\times \cong \mu(K) \times \mathbb{Z}^{r_1+r_2-1}$$

where $\mu(K) = \{x \in K : x^n = 1 \text{ for some } n > 0\}$.

If any of this terminology is unfamiliar then don't worry, we will cover it in later lectures. For now, we'll content ourselves by noting that the field $K = \mathbb{Q}(\sqrt{n})$, which has ring of integers $\mathcal{O}_K = \mathbb{Z}[\sqrt{n}]$ (for simplicity, restrict to the case where n is squarefree and $n \not\equiv 1 \mod 4$), has $r_1 = 2$ and $r_2 = 0$. So by Dirichlet's unit theorem,

$$\mathbb{Z}(\sqrt{n})^\times \cong \{\pm 1\} \times \mathbb{Z}.$$

Therefore if we find a generator of the copy of $\mathbb{Z}$ in the product, we have an algorithm which generates all possible candidate solutions to Pell's equation.

1.3. $\mathbb{Z}$**.** Let's recall some basic properties of $\mathbb{Z}$, which we will later generalize.

Exercise 1.3.1.

- **Well-ordering principle**: every non-empty subset of $\mathbb{Z}_{\geq 0}$ contains a smallest element. Equivalently, there is no infinitely descending sequence $a_1 > a_2 > \cdots > a_k > \cdots$ in $\mathbb{Z}_{\geq 0}$. We will take this as an axiom: depending on which logical framework you work in, it's either an axiom or a theorem.
- **Prime factorization**: every positive integer a can be written as
$$a = p_1^{n_1} \cdots p_k^{n_k}$$
where $p_1, \ldots, p_k$ are distinct prime numbers.

  Proof. Exercise. Hint: use the well-ordering principle. □
- **Division algorithm**: Let $a, b \in \mathbb{Z}$ with $b \neq 0$. There exist unique $q, r \in \mathbb{Z}$ such that $a = qb + r$ and
$$0 \leq r < |b|.$$

  Proof. Exercise. Hint: apply the well-ordering principle to the set $\{n \in \mathbb{Z}_{\geq 0} : a - sb, s \in \mathbb{Z}\}$. □
- **Bézout's identity**: For $a, b \in \mathbb{Z}$ (not both 0) there exist $x, y \in \mathbb{Z}$ such that
$$\gcd(a, b) = ax + by.$$

  Proof. Exercise. Hint: apply the well-ordering principle to $\{ax + by : x, y \in \mathbb{Z}\} \cap \mathbb{Z}_{>0}$. Alternatively, perform the *Euclidean algorithm.* □
- **Euclid's lemma**: If $a, b \in \mathbb{Z}$ and p is prime and $p \mid a, b$, then either $p \mid a$ or $p \mid b$.

  Proof. Exercise. Hint: use Bézout's identity. □
- **Uniqueness of prime factorization**: If $a > 0$ and
$$p_1^{n_1} \cdots p_k^{n_k} = a = q_1^{m_1} \cdots q_\ell^{m_\ell}$$
are distinct prime factorizations, then $k = \ell$ and up to reordering we have $p_i = q_i$ and $n_i = m_i$.

  Proof. Exercise. Hint: repeatedly apply Euclid's lemma. □
- **Separating powers**: If $a, b, c \in \mathbb{Z} \setminus \{0\}$ and $n > 0$ such that $a^n = bc$, then if $\gcd(b, c) = 1$ there exist $b_0, c_0 \in \mathbb{Z}$ such that
$$b = \pm b_0^n \text{ and } c = \pm c_0^n.$$

  Proof. Exercise. Hint: use uniqueness of factorization. □

1.4. $\mathbb{Z}[i]$**.** Recall before that we wanted to classify solutions to $x^2 + y^2 = z^2$ by reformulating it as $(x + iy)(x - iy) = z^2$ and then using properties of primes in $\mathbb{Z}[i]$, the ring of *Gaussian integers*. What are those properties? Let's try to mimic the properties of $\mathbb{Z}$ above. There is no well-ordering principle in this setting, but we can instead push ourselves down into a situation where we can use the well-ordering principle for $\mathbb{Z}$.

Definition 1.4.1. The norm map $N : \mathbb{Z}[i] \to \mathbb{Z}$ is given by
$$N(a + bi) := (a + bi)(a - bi) = a^2 + b^2.$$

Of course if we embed $\mathbb{Z}[i] \hookrightarrow \mathbb{C}$, then N is just the square of the usual Euclidean norm.

Exercise 1.4.2. Show that $N(\alpha) = 1$ if and only if $\alpha \in \mathbb{Z}[i]^\times$. In particular, determine $\mathbb{Z}[i]^\times$ explicitly and verify Theorem 1.2.2 in this case. You may assume that the roots of unity in $\mathbb{Q}(i)^\times$ are contained in $\mathbb{Z}[i]^\times$, and that $r_1 = 0$ and $r_2 = 1$.

Proposition 1.4.3. *For any $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0$, there exists κ, λ such that $\alpha = \kappa\beta + \lambda$ and $N(\lambda) < N(\beta)$.*

Proof. By the well-ordering principle, the set $\{n \in \mathbb{Z} : n = N(\alpha - \sigma\beta) \text{ for } \sigma \in \mathbb{Z}[i]\}$ has a smallest element, so call it ℓ. Then $\ell = N(\alpha - \kappa\beta)$ for some specific $\kappa \in \mathbb{Z}[i]$, so let $\lambda = \alpha - \kappa\beta$. It remains to show that $N(\lambda) < N(\beta)$. Now note that $\mathbb{Z}[i]$, when plotted in the complex plane, is exactly the integer gridpoints, and geometrically one sees that κ is the closest gridpoint to the complex number α/β. In particular this implies that $N(\alpha/\beta - \kappa) < (1/2)^2 + (1/2)^2 < 1$, and therefore

$$N(\lambda) = N(\alpha - \kappa\beta) < N(\beta).$$

□

Remark 1.4.4. If $D(x, 1)$ denotes a disk of radius 1 in the complex plane around a point $x \in \mathbb{C}$, then this proof can be reinterpreted as saying

$$\mathbb{C} = \bigcup_{x \in \mathbb{Z}[i]} D(x, 1)$$

Remarkably,

$$\mathbb{C} \neq \bigcup_{x \in \mathbb{Z}[\zeta_{23}]} D(x, 1)$$

but I see no clear and intuitive geometric reason why you should expect this to be true. In fact if you start plotting points near the origin, it looks like $\mathbb{Z}[\zeta_{23}]$ has *more* of a chance of satisfying this property!

Exercise 1.4.5. Using Proposition 1.4.3, prove that for any $\alpha, \beta \in \mathbb{Z}[i]$ not both zero, there exists a greatest common divisor. In other words, show that there exists $\delta \in \mathbb{Z}[i]$ which divides both α and β, and such that every common divisor of α and β divides δ (hint: try to adapt the Euclidean algorithm for $\mathbb{Z}$ to $\mathbb{Z}[i]$). In fact, show further that there exist exactly 4 greatest common divisors (hint: think about $\mathbb{Z}[i]^\times$). Can you think of a way to canonically distinguish one of them?

Ultimately we want unique factorization, so let's talk about primes. The definition of a prime number in $\mathbb{Z}$ is usually stated as "a positive integer whose positive divisors are 1 and itself". On the other hand:

Lemma 1.4.6. *$p > 0$ is a prime number if and only if it is not equal to 1 and*

$$p \mid nm \implies p \mid n \text{ or } p \mid m$$

for all $n, m \in \mathbb{Z}_{>0}$.

Something that will be a key point in what follows is that Lemma 1.4.6 is not always true in general. What does this mean? If we allow ourselves to enlarge what we consider a prime number in $\mathbb{Z}$, we can make a more uniform definition.

Definition 1.4.7. Fix a commutative ring R. If $r, s \in R$ then we say $r \mid s$ if $s = rt$ for some $t \in R$. An element $r \in R \setminus (R^\times \cup \{0\})$ is

- *prime* if $r \mid st \implies r \mid s$ or $r \mid t$ for all $s, t \in R$.
- *irreducible* if $r = st$ implies that either s or t is in $R^\times$.

Lemma 1.4.8. *In an integral domain, all primes are irreducible.*

Proof. If r is prime and $r = st$, then without loss of generality $st \mid s$, so $s = stu$ for some $u \in R$. Since R is an integral domain $1 = tu$, so $t \in R^\times$. □

We will see an example later of an integral domain which contains an irreducible element that is not prime.

Remark 1.4.9. So Lemma 1.4.6 *almost* says that in $\mathbb{Z}$, prime = irreducible; the issue is that with this new definition, prime elements of $\mathbb{Z}$ are now allowed to be negative. So for instance both 3 and -3 are prime elements in $\mathbb{Z}$. The choice of positive vs negative in the usual definition of a prime number is similar to the canonical choice of gcd that you found in Exercise 1.4.5.

Exercise 1.4.10.

(1) Show that in $\mathbb{Z}[i]$, irreducibles are prime.

(2) Show that if $N(\alpha)$ is prime then α is prime in $\mathbb{Z}[i]$. Prove or disprove the converse.

(3) Finally, conclude that $\mathbb{Z}[i]$ has unique factorization. In other words, show that every nonzero $\alpha \in \mathbb{Z}[i]$ can be written uniquely in the form
$$\pi_1^{n_1} \cdots \pi_k^{n_k}$$
up to reordering and multiplication by a unit in $\mathbb{Z}[i]^\times$, for π_i distinct primes in $\mathbb{Z}[i]$ (hint: induct on $N(\alpha)$).

(4) Bonus exercise (tricky): classify all of the primes in $\mathbb{Z}[i]$ in terms of the primes in $\mathbb{Z}$ (hint: use the norm).

Using unique factorization we have the separating powers property:

Proposition 1.4.11. *In $\mathbb{Z}[i]$, if $\alpha, \beta, \gamma \in \mathbb{Z}[i] \setminus \{0\}$ and $n > 0$ such that $\alpha^n = \beta\gamma$ then if β, γ share no common prime factors there exists β_0, γ_0 such that $\beta = \mu\beta_0^n$ and $\gamma = \mu'\gamma_0^n$ with μ, μ' units.*

Proof. The proof is basically the same as for $\mathbb{Z}$: use unique factorization and coprimality. □

Now let's go back to the Fermat problem. We had $(x+iy)(x-iy) = z^2$. By eliminating common factors we may assume x, y, z are pairwise coprime (i.e. the triple is *primitive*). We also note that z must be odd in this case: if z were even then either x and y are both even and they're no longer pairwise coprime, or x and y are both odd, and working mod 4 one reaches a contradiction.

Lemma 1.4.12. *$x + iy$ and $x - iy$ share no prime factors in $\mathbb{Z}[i]$.*

Proof. First note that x and y share no prime factors in $\mathbb{Z}[i]$. For this, suppose $x = gu$ and $y = gv$ for $g, u, v \in \mathbb{Z}[i]$. Then u, v are colinear, i.e. are $\mathbb{Z}$-multiples of some $h \in \mathbb{Z}[i]$. So $x = ngh$ and $y = mgh$. But then $gh \in \mathbb{Z}$ and divides both x and y so must be ± 1, and thus g is a unit.

Then if $x + iy$ and $x - iy$ had a common prime factor δ, we could conclude that δ divides both $2x$ and $2iy$, and thus divides 2 since i is a unit and x and y are coprime. But then z^2 would be even, which is a contradiction. □

So Proposition 1.4.11 implies that there exists some $\alpha \in \mathbb{Z}[i]$ such that $x + iy = \mu\alpha^2$ for μ a unit. Write $\alpha = m + in$. By swapping some signs and possibly swapping $n \leftrightarrow m$ or $x \leftrightarrow y$, we may assume $\mu = 1$.

Corollary 1.4.13. *Every primitive Pythagorean triple (x, y, z) can be written $x = m^2 - n^2$ and $y = 2mn$ for some $m, n \in \mathbb{Z}$, and conversely any $m, n \in \mathbb{Z}$ not both zero generates a Pythagorean triple.*

Proof. Square α. □

1.5. **Fermat for $p = 3$.**

Now back to Fermat's last theorem. Again, our general strategy is to factor the expression $x^p + y^p$ by adjoining p-power roots of unity. However, it turns out that these sorts of arguments are only tractable when we have unique factorization in $\mathbb{Z}[\zeta_p]$, or something slightly weaker.

Exercise 1.5.1. Prove that $\mathbb{Z}[\zeta_3]$ is a unique factorization domain (hint: try to mimic the case $\mathbb{Z}[i]$ as in Exercise 1.4.10 — the hardest part will be showing the division algorithm, so try to plot the points of $\mathbb{Z}[\zeta_3]$ in the complex plane and reason like in the Gaussian integer case).

Rather than finish the proof of Fermat's last theorem in this case, we will instead prove a more general result (Theorem 1.5.4) later on.

In general, $\mathbb{Z}[\zeta_p]$ will not have unique factorization. In fact, in general it is an open problem whether the ring of integers $\mathcal{O}_K$ in an arbitrary number field $K/\mathbb{Q}$ has unique factorization; for example, we don't even know whether there are infinitely many K with this property.

Remark 1.5.2. On the other hand, what we will show is that $\mathcal{O}_K$ is a *Dedekind domain*, which in particular implies that every nonzero *ideal* in $\mathcal{O}_K$ can be written uniquely as the product of nonzero prime ideals. We will study the behavior of prime ideals in Dedekind domains in detail, and see the relation to factorizations of numbers.

This leads to the notion of the *class number* h_K, which is an invariant associated with K which precisely measures the degree to which unique factorization fails; when $h_K = 1$, $\mathcal{O}_K$ is a unique factorization domain, and when $h_K > 1$ it is not (we will define this precisely later and study it in detail). But even though $h_{\mathbb{Q}(\zeta_p)} > 1$ in general (for example, when $p = 23$ this is already true), to prove Fermat's last theorem we just need something weaker:

Definition 1.5.3. A prime number p is *regular* if $p \nmid h_{\mathbb{Q}(\zeta_p)}$.

Later, we will prove the following theorem:

Theorem 1.5.4 (Kummer)**.** *If $p \geq 3$ is a regular prime, then $x^p + y^p = z^p$ has no solutions with $xyz \neq 0$.*

2. Number fields and algebra

Now we will talk about number fields in general. In doing so, we will review some basic notions in commutative algebra.

2.1. Galois theory.

Let's first recall a few facts from Galois theory.

Definition 2.1.1. If K/F is an algebraic extension of fields and $\alpha \in K$, then there exists a unique nonzero monic polynomial $p_\alpha(x) \in F[x]$ of minimal degree called the *minimal polynomial* characterized by the property that $p_\alpha(\alpha) = 0$ and $p_\alpha \mid q$ for any $q \in F[x]$ with $q(\alpha) = 0$.

For instance, the minimal polynomial of $\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ is $x^2 - 2$.

Definition 2.1.2. An algebraic extension K/F is *separable* if p_α has distinct roots for all $\alpha \in K$, and *inseparable* otherwise.

A standard example of an inseparable extension is the extension $\mathbb{F}_p((t^{1/p}))/\mathbb{F}_p((t))$. Note the minimal polynomial of $t^{1/p}$ is $x^p - t$, and if you view it as a polynomial in $\mathbb{F}_p((t^{1/p}))$, then it factors as

$$x^p - t = (x - t^{1/p})^p$$

and so has only one root with multiplicity p. In some sense this is the "only example", which is made precise by the following exercise:

Exercise 2.1.3 (Challenging)**.** Show that a field F admits an inseparable extension if and only if $\operatorname{char} F > 0$ and the *Frobenius* map $F \to F$ taking $x \mapsto x^p$ is not surjective (hint: think about the derivative of the minimal polynomial). In particular in characteristic 0 all algebraic extensions are separable.

The *primitive element theorem* says that a finite separable field extension K/F can always be written in the form $K = F(\alpha)$ for some $\alpha \in K$. If the field extension is not separable then one can always write $K = F(\alpha_1, \ldots, \alpha_m)$ for some α_i (but m can be arbitrarily large, see [BM40]).

Definition 2.1.4. An algebraic extension K/F is *normal* if whenever $p(x) \in F[x]$ has a root in K, K contains all of the roots. An algebraic extension is *Galois* if it is separable and normal. In this case we write $\operatorname{Gal}(K/F) := \operatorname{Aut}(K/F)$. If K/F is finite, one always has $|\operatorname{Aut}(K/F)| \leq [K : F]$ with equality if and only if K/F is Galois.

If K/F is a Galois extension and $K = F(\alpha)$ for some $\alpha \in K$, then an automorphism of K permutes the roots of p_α and in fact is determined by the permutation.

The typical example of a non-normal (and hence non-Galois) extension of $\mathbb{Q}$ is $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. In this case note that $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$, while the other two roots of $x^3 - 2$ are the complex numbers $\zeta_3 \sqrt[3]{2}$ and $\zeta_3^2 \sqrt[3]{2}$.

So a normal closure of $\mathbb{Q}(\sqrt[3]{2})$ is a splitting field of $x^3 - 2$, i.e. $\mathbb{Q}(\zeta_3, \sqrt[3]{2})$.

Exercise 2.1.5.

(1) Classify all finite extensions of the finite field $\mathbb{F}_p$ with p elements. Are there any non-normal or non-separable finite extensions?

(2) Determine the minimal polynomial of ζ_p for all primes p. Show that $\mathbb{Q}(\zeta_p)$ is a normal extension of $\mathbb{Q}$ and determine the Galois group of $\mathbb{Q}(\zeta_p)/\mathbb{Q}$. Here $\zeta_p = e^{2\pi i/p}$ is a primitive pth root of unity.

(3) Find $\alpha \in \mathbb{C}$ such that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\alpha)$.

Theorem 2.1.6 (Fundamental Theorem of Galois Theory)**.** *If K/F is a finite Galois extension with Galois group G, then there is an inclusion-reversing bijection*

$$\{\textit{subgroups of } G\} \xleftrightarrow{\sim} \{\textit{intermediate extensions } F \subseteq E \subseteq K\}$$
$$H \mapsto K^H$$
$$\operatorname{Aut}(K/E) \leftarrow\!\shortmid E$$

Furthermore $H \leq G$ is normal if and only if K^H/F is normal, in which case $\operatorname{Gal}(K^H/F) \cong G/H$.

Exercise 2.1.7. Using the fundamental theorem, list all of the intermediate fields between $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Exercise 2.1.8. Show that if K/F is a finite extension then there exists a unique (up to isomorphism) *normal closure* $\widetilde{K}$ of K over F: in other words, a normal extension $\widetilde{K}/F$ containing K and no smaller normal extension of F.

2.2. **Different kinds of rings.** Now let's study some classes of integral domains of interest, whose fraction fields will ultimately be the number fields we are interested in.

Definition 2.2.1. An integral domain A is a *Euclidean domain* if there exists a function $f : A \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ such that

- for all $a, b \in A$ with $b \neq 0$ there exist $q, r \in A$ such that $a = qb + r$ and either $r = 0$ or $f(r) < f(b)$.

As we saw earlier, $\mathbb{Z}$ is a Euclidean domain for the absolute value, as well as $\mathbb{Z}[i]$ with the norm N.

Exercise 2.2.2. If F is a field, show that $F[x]$ is a Euclidean domain.

As we mentioned before, prime ideals in number rings often behave better than prime numbers in the ring. For Euclidean domains, things are particularly nice.

Lemma 2.2.3. *If A is a Euclidean domain with Euclidean function f and $I \subset A$ is a nonzero ideal, then there exists a nonzero $d \in A$ such that $I = (d)$.*

Proof. The set $f(I \setminus \{0\})$ has a minimum element by the well-ordering principle, call it $f(d)$. Then if $a \in I$ is nonzero, Definition 2.2.1 implies that there exist $q, r \in A$ such that $a = qd + r$ with $f(r) < f(d)$. Since $a, d \in I$ we also have $r \in I$. But if $r \neq 0$ then we get $f(d) \leq f(r)$ by minimality, which is a contradiction, so $r = 0$. Thus $a = qd$, so in fact $I = (d)$. □

In view of this, we make the following definition.

Definition 2.2.4. An integral domain is a *principal ideal domain (or PID)* if every ideal I is of the form $I = (d)$ for some $d \in A$.

Thus Lemma 2.2.3 says that a Euclidean domain is a PID. As we will see later prime ideals will always have unique factorization, but for PIDs the situation is nicer.

Exercise 2.2.5. Show that a PID is Noetherian, i.e. satisfies the ascending chain condition.

Proposition 2.2.6. *If A is a PID, then every nonzero nonunit $a \in A$ can be written uniquely in the form*

$$a = p_1^{n_1} \cdots p_k^{n_k}$$

up to reordering and scaling by units, where the p_i are distinct irreducible elements of A.

Proof. If a is not irreducible, then it can be written $a = a_1 a_2$ where a_1 and a_2 are nonzero nonunits. If a_1 and a_2 are irreducible, then we are done. Otherwise, without loss of generality $a_1 = a_{11} a_{12}$ where a_{11} and a_{12} are nonzero nonunits. If a cannot be completely factorized, then this process will repeat infinitely, leading to a chain of proper inclusions

$$(a) \subset (a_1) \subset (a_{11}) \subset (a_{111}) \subset \cdots \subset R$$

But since A is Noetherian, this process terminates, which is a contradiction. □

Exercise 2.2.7. Finish the proof of Proposition 2.2.6 by showing uniqueness of the decomposition.

In view of this, we make the following definition.

Definition 2.2.8. An integral domain is a *unique factorization domain (UFD)* if every nonzero nonunit $a \in A$ can be written uniquely in the form

$$a = p_1^{n_1} \cdots p_k^{n_k}$$

up to reordering and scaling by units, where the p_i are distinct irreducible elements of A.

Exercise 2.2.9.

(1) Show that in a UFD the prime elements are exactly the irreducible elements.

(2) Show that if A is a UFD then $A[x]$ is a UFD. (hint: why is $\mathrm{Frac}(A)[x]$ a UFD? could this be useful?)

In order to fruitfully study algebraic number rings, we will need the notion of integral closure. Algebraic number theory is really about studying the properties of rings that you get when you solve equations, so it shouldn't be too surprising that this definition shows up.

Definition 2.2.10. If $A \subset B$ are rings and $b \in B$, then we say that b is *integral over A* if there exists a monic polynomial $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in A[x]$ such that $p(b) = 0$.

Exercise 2.2.11. Prove that $1/3$ is not integral over $\mathbb{Z}$. With proof, decide whether or not $(1 + \sqrt{17})/2$ is integral over $\mathbb{Z}$. Hint: think about the quadratic formula.

Lemma 2.2.12. *If $A \subset B$ then $b \in B$ is integral over A if and only if $A[b]$ is a finitely generated A-module.*

Proof. If b is integral over A then we may write $b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$. Therefore any polynomial expression in b over A can be written as an A-linear combination of $\left\{1, \ldots, b^{n-1}\right\}$, so $A[b]$ is finitely generated.

Conversely, suppose $A[b]$ is generated by $b_1, \ldots, b_m$ as an A-module. Since every element of $A[b]$ can be written as a polynomial in b, we may write $b_i = p_i(b)$ for some $p_i \in A[x]$. If $n = \max \deg p_i$, then

$$0 = b^{n+1} - a_1 p_1(b) + \cdots + a_n p_n(b)$$

for some $a_i \in A$ and therefore b solves a monic polynomial expression with A-coefficients. □

Exercise 2.2.13.

(1) Use Lemma 2.2.12 to show that the subset

$$\widetilde{A} = \{b \in B : b \text{ is integral over } A\} \subset B$$

is actually a subring of B containing A (hint: first use Lemma 2.2.12 to prove that $b \in B$ is integral over A if and only if $A[b] \subset A' \subset B$ for some finitely generated A-module A').

(2) Extend Lemma 2.2.12 to show that $b_1, \ldots, b_n$ are integral over A if and only if $A[b_1, \ldots, b_n]$ is a finitely generated A-module.

Remark 2.2.14. For those who are geometrically minded, taking integral closure is the algebraic analog of taking the *normalization* of a scheme.

Definition 2.2.15. Fix $A \subset B$.

- We call $\widetilde{A}$ the *integral closure of A in B*.
- If $\widetilde{A} = A$ then we say that A is *integrally closed in B*.
- If A is an integral domain, then we say that A is *integrally closed* if it is integrally closed in $\mathrm{Frac}(A)$, its field of fractions.
- If $\widetilde{A} = B$ then we say that B is *integral over A*.

Exercise 2.2.16.

(1) If $A \subset B \subset C$, B is integral over A and C is integral over B, then show that C is integral over A.

(2) For $A \subset B$ show that $\widetilde{A}$ is integrally closed in B.

(3) Show that $\mathbb{Z}$ is integrally closed.

(4) Now show that any UFD is integrally closed.

2.3. Number fields.

Finally, we come to the main definition of the course.

Definition 2.3.1. A finite extension $F/\mathbb{Q}$ is called a *number field*. Its *degree* is $[F : \mathbb{Q}] = \dim_{\mathbb{Q}} F$. The integral closure of $\mathbb{Z}$ in F, which we denote by $\mathcal{O}_F$, is called the *ring of integers of F*. Equivalently,

$$\mathcal{O}_F = \{c \in F : p(c) = 0 \text{ for some monic } p \in \mathbb{Z}[x]\}$$

An *algebraic number* is an element of a number field and an *algebraic integer* is an element of the ring of integers of a number field. Clearly an algebraic number is an algebraic integer if and only if it solves a monic polynomial in $\mathbb{Z}[x]$.

Example 2.3.2. You might imagine that algebraic numbers are algebraic integers if they "don't have denominators", but as the following example (generalizing Exercise 2.2.11) shows, it's not that straightforward. If d is an integer, then $\sqrt{-d}$ is an algebraic number. But what about

$$\alpha = \frac{-1 \pm \sqrt{-d}}{2}?$$

Check that

$$\alpha^2 = -\alpha - \frac{d+1}{4}.$$

So if $d \equiv 3 \mod 4$ then α solves a monic polynomial with coefficients in $\mathbb{Z}$. On the other hand, if $d \not\equiv 3 \mod 4$ then our usual intuition wins out, and as we will see, $\mathcal{O}_{\mathbb{Q}(\sqrt{-d})} = \left\{a + b\sqrt{-d} : a, b \in \mathbb{Z}\right\}$.

Remark 2.3.3. If F is a number field, one can always write $\mathbb{Q}(\alpha)$ and then $1, \alpha, \dots, \alpha^{[F:\mathbb{Q}]-1}$ is a basis for F over $\mathbb{Q}$. However as Example 2.3.2 above shows, it is not necessarily the case that $\mathcal{O}_F = \mathbb{Z}[\alpha]$. In fact, it is not even always true that $\mathcal{O}_F = \mathbb{Z}[\beta]$ for any *single* β! More on this in a bit.

Exercise 2.3.4. Write down (with proof) an element of $\mathbb{Q}(\sqrt{3}) \setminus \mathcal{O}_{\mathbb{Q}(\sqrt{3})}$.

Exercise 2.3.5. Show that if α is an algebraic *number*, then there exists $m \in \mathbb{Z}_{>0}$ such that $m\alpha$ is an algebraic *integer*.

Here is a way to go between different number fields. Let K/F be an extension of number fields.

Definition 2.3.6. For $\alpha \in K$ the map $m_\alpha : K \to K$ given by multiplication by α is an F-linear map. In view of this we define the *norm* and *trace* by taking

$$\begin{aligned} N_{K/F} : K &\to F \\ \alpha &\mapsto \det(m_\alpha : K \to K) \\ \operatorname{tr}_{K/F} : K &\to F \\ \alpha &\mapsto \operatorname{tr}(m_\alpha : K \to K) \end{aligned}$$

Exercise 2.3.7. Show that $\operatorname{tr}_{K/F} : K \to F$ is an F-linear map, and show that $N_{K/F} : K^\times \to F^\times$ is a group homomorphism.

Proposition 2.3.8. *Assume K/F is Galois. For $\alpha \in K$ the characteristic polynomial of m_α splits as*

$$f_\alpha(x) = \prod_{\sigma \in \operatorname{Gal}(K/F)} (x - \sigma(\alpha))$$

In particular,

$$\operatorname{tr}_{K/F}(\alpha) = \sum_{\sigma \in \operatorname{Gal}(K/F)} \sigma(\alpha) \text{ and } N_{K/F}(\alpha) = \prod_{\sigma \in \operatorname{Gal}(K/F)} \sigma(\alpha).$$

Proof. First we show that $f_\alpha(x) = p_\alpha(x)^d$ where p_α denotes the minimal polynomial and $d = [K : F(\alpha)]$.

For this, let $m = [F(\alpha) : F]$. Then we may write

$$p_\alpha(x) = x^m + c_{m-1}x^{m-1} + \cdots + c_0$$

for some $c_i \in F$. Note that $1, \alpha, \dots, \alpha^{m-1}$ is a basis for $F(\alpha)$ over F, so if we fix a basis $\beta_1, \dots, \beta_d$ of K over $F(\alpha)$ then

$$\beta_1, \beta_1\alpha, \dots, \beta_1\alpha^{m-1}; \dots; \beta_d\alpha, \dots, \beta_d\alpha^{m-1}$$

is a basis for K/F. the matrix for the map $m_\alpha : K \to K$ is, with respect to this basis is

$$\begin{pmatrix} M & & \\ & \ddots & \\ & & M \end{pmatrix}$$

(taken d times) where

$$M = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 \\ -c_0 & -c_1 & -c_2 & \cdots & c_{m-1} \end{pmatrix}$$

and one can check that the characteristic polynomial of M is exactly p_α. Therefore, $f_\alpha(x) = p_\alpha(x)^d$.

If $\sigma \in \mathrm{Gal}(K/F)$ and $\tau \in \mathrm{Gal}(K/F(\alpha))$ then $\sigma\tau(\alpha) = \sigma(\alpha)$. If $\sigma_1, \dots, \sigma_m$ denote left coset representatives of $\mathrm{Gal}(K/F(\alpha))$ in $\mathrm{Gal}(K/F)$, then

$$p_\alpha(x) = \prod_{i=1}^{m}(x - \sigma_i(\alpha))$$

and so

$$\prod_{\sigma \in \mathrm{Gal}(K/F)}(x - \sigma(\alpha)) = \prod_{i=1}^{m} \prod_{\tau \in \mathrm{Gal}(K/F(\alpha))}(x - \sigma_i\tau(\alpha)) = \prod_{i=1}^{m}(x - \sigma_i(\alpha))^d = p_\alpha(x)^d = f_\alpha(x).$$

The claims about the norm and trace follow. □

Exercise 2.3.9.

(1) Using the normal closure (c.f. Exercise 2.1.8) try to remove the assumption that K/F is Galois from Proposition 2.3.8 (hint: you need to replace $\mathrm{Gal}(K/F)$ with the set of field embeddings $F \hookrightarrow \mathbb{C}$. how do these embeddings relate to the normal closure?).

(2) Show that if $L/K/F$ is a tower of number fields, then $\mathrm{tr}_{K/F} \circ \mathrm{tr}_{L/K} = \mathrm{tr}_{F/L}$ and $N_{K/F} \circ N_{L/K} = N_{F/L}$). You can assume part (1) of the exercise.

Corollary 2.3.10. *If K/F is a finite Galois extension of number fields then $\mathrm{tr}_{K/F}(\mathcal{O}_K) \subset \mathcal{O}_F$ and $N_{K/F}(\mathcal{O}_K) \subset \mathcal{O}_F$.*

Proof. Note that $\mathcal{O}_K$ is the integral closure of $\mathcal{O}_F$ in K. So if $\alpha \in \mathcal{O}_K$ then α is integral over $\mathcal{O}_F$. But then for all $\sigma \in \mathrm{Gal}(K/F)$, the element $\sigma(\alpha)$ is again integral. To see this, note that if α is a root of the monic polynomial $p(x) \in F[x]$, then $\sigma(\alpha)$ is as well because σ is a ring homomorphism. So

$$\mathrm{tr}_{K/F}(\alpha) = \sum_{\sigma \in \mathrm{Gal}(K/F)} \sigma(\alpha) \text{ and } N_{K/F} = \prod_{\sigma \in \mathrm{Gal}(K/F)} \sigma(\alpha)$$

are also integral over $\mathcal{O}_F$. But they are elements of F and $\mathcal{O}_F$ is integrally closed (since it is defined as an integral closure), so they live in $\mathcal{O}_F$. □

2.4. Integral bases.

Let us return to the discussion of giving a description of $\mathcal{O}_F$.

Definition 2.4.1. If K is a number field of degree $n = [K : \mathbb{Q}]$, and M is a finitely generated $\mathcal{O}_K$-submodule of K, then an *integral basis* of M is a tuple $\alpha_1, \dots, \alpha_n \in M$ such that every $\alpha \in M$ can be written uniquely as

$$\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n$$

for $a_i \in \mathbb{Z}$.

In particular, such an M admits an integral basis if and only if it is a free abelian group of rank $n = [K : \mathbb{Q}]$.

On the road to proving existence of integral bases, we first encounter the discriminant.

Definition 2.4.2. If K/F is a Galois extension of number fields and $\alpha_1, \dots, \alpha_n$ is a basis of K over F, then the *discriminant* of the basis is

$$d_{K/F}(\alpha_1, \dots, \alpha_n) := \det((\sigma_i(\alpha_j))_{i,j})^2$$

where σ_i runs through the elements of $\mathrm{Gal}(K/F)$.

Remark 2.4.3. As you will show in Exercise 2.4.13, the discriminant of a basis is closely related to the discriminant of a polynomial.

Exercise 2.4.4. Show that

$$d(\alpha_1,\dots,\alpha_n) = \det((\operatorname{tr}_{K/F}(\alpha_i\alpha_j))_{i,j})$$

(hint: use Proposition 2.3.8). Conclude that if $\alpha_1,\dots,\alpha_n \in \mathcal{O}_K$ then $d(\alpha_1,\dots,\alpha_n) \in \mathcal{O}_F$.

In view of Exercise 2.4.4, we can extend the definition of the discriminant to any extension K/F of number fields, not necessarily Galois.

Fact 2.4.5. $d(\alpha_1,\dots,\alpha_n) \neq 0$.

Proof. Omitted: the idea is to show that the pairing $(x,y) \mapsto \operatorname{tr}_{K/F}(xy)$ is a nondegenerate bilinear pairing. □

Lemma 2.4.6. *If $\alpha_1,\dots,\alpha_n$ is a basis for K/F which is contained in $\mathcal{O}_K$, then*

$$d\mathcal{O}_K \subset \mathcal{O}_F\alpha_1 + \cdots + \mathcal{O}_F\alpha_n \subset \mathcal{O}_K$$

with $d = d(\alpha_1,\dots,\alpha_n)$.

Proof. If $\alpha \in \mathcal{O}_K$ then we may write $\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n$ for $a_i \in F$. We want to show that $da_i \in \mathcal{O}_F$ for all i. Note

$$(\operatorname{tr}_{K/F}(\alpha_i\alpha))_i^T = (\operatorname{tr}_{K/F}(\alpha_i\alpha_j))_{i,j} \times (a_j)_j^T$$

But now note that $\operatorname{tr}_{K/F}(\alpha_i\alpha) \in \mathcal{O}_F$ and $d \neq 0$, so each a_j is the quotient of an element of $\mathcal{O}_F$ by d, and thus $da_j \in \mathcal{O}_F$. □

Corollary 2.4.7. *$\mathcal{O}_K$ admits an integral basis, and furthermore every nonzero finitely generated $\mathcal{O}_K$-submodule of K admits an integral basis.*

Proof. Let $M \neq 0$ denote the submodule in the statement with generators $\beta_1,\dots,\beta_r \in M$. Using Exercise 2.3.5 pick $a \in \mathbb{Z}$ such that $a\beta_i \in \mathcal{O}_K$, so that $aM \subset \mathcal{O}_K$. Also using Exercise 2.3.5 we can also pick a basis $\alpha_1,\dots,\alpha_n \in \mathcal{O}_K$ of $K/\mathbb{Q}$ so by Lemma 2.4.6 we have (with $d = d_{K/F}(\alpha_i)$)

$$adM \subset d\mathcal{O}_K \subset \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n.$$

The right hand side is a finitely generated abelian group, so since $\mathbb{Z}$ is Noetherian we see that adM and $d\mathcal{O}_K$, and hence M and $\mathcal{O}_K$, are finitely generated abelian groups. But since they all are contained in the field K they are $\mathbb{Z}$-torsion-free, so the structure theorem for finitely generated abelian groups implies that they are free. Since $\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Q} = K$ we see that $\operatorname{rank}\mathcal{O}_K = n$. We know that

$$\operatorname{rank} M = \operatorname{rank} adM \leq \operatorname{rank}\mathcal{O}_K = n$$

so it remains to show that $\operatorname{rank} M \geq n$. But for this, note that M is a finitely generated free abelian group, so $M \otimes_{\mathbb{Z}} \mathbb{Q}$ is a nonzero $\mathbb{Q}$-vector space of dimension $\operatorname{rank} M$. But M is also an $\mathcal{O}_K$-module, so $M \otimes_{\mathbb{Z}} \mathbb{Q}$ is a nonzero K-vector space. Therefore,

$$\operatorname{rank} M = \dim_{\mathbb{Q}}(M \otimes_{\mathbb{Z}} \mathbb{Q}) \geq \dim_{\mathbb{Q}} K = n.$$

□

Exercise 2.4.8. For any number field K, use Exercise 2.3.5 and Corollary 2.4.7 to construct a ring isomorphism $\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Q} \xrightarrow{\sim} K$.

Remark 2.4.9. If we consider an extension K/F of number fields instead of $K/\mathbb{Q}$, then Corollary 2.4.7 is still true (with the same proof) if $\mathcal{O}_F$ is a PID; in this case, we can replace the use of the structure theorem for f.g. abelian groups with the structure theorem for f.g. modules over a PID.

Definition 2.4.10. The *discriminant of* $K/\mathbb{Q}$, denoted d_K, is the discriminant of an integral basis.

Exercise 2.4.11. Show that the discriminant is well-defined: in other words, show that it is independent of the choice of integral basis.

The proof of Corollary 2.4.7 doesn't give much of an idea of how to actually compute an integral basis, and in general this is not a straightforward problem. But it's easy to come up with bases of $K/\mathbb{Q}$, so one plausible approach is to pick such a basis $\alpha_1, \dots, \alpha_n$ and try to massage it into an integral basis of $\mathcal{O}_K$ over $\mathbb{Z}$.

The first step, as in the previous proof, is to scale things so that $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$. At that point, what can we say about the resulting basis? The only thing we know how to compute is the discriminant d. But how much information can the discriminant tell us about the basis? Note that the basis generates a finitely generated $\mathbb{Z}$-module $\mathfrak{a} = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n \subset \mathcal{O}_K$. Suppose further that $\mathfrak{a}$ is in fact an $\mathcal{O}_K$-module. Then since $\mathcal{O}_K/\mathfrak{a}$ is finite, we can speak about its index $[\mathcal{O}_K : \mathfrak{a}] := |\mathcal{O}_K/\mathfrak{a}|$.

Lemma 2.4.12. *If $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$ is a basis for $K/\mathbb{Q}$ and $\mathfrak{a} = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$ is an $\mathcal{O}_K$-module, then*

$$d(\alpha_1, \dots, \alpha_n) = [\mathcal{O}_K : \mathfrak{a}]^2 d_K$$

So for example, if one computes that $d(\alpha_1, \dots, \alpha_n)$ is squarefree, then it implies that $\alpha_1, \dots, \alpha_n$ is an integral basis. On the other hand, as the following guided exercise shows, this isn't necessarily a necessary condition, only sufficient.

Exercise 2.4.13. Fix D a squarefree integer (i.e. if p is prime and $p \mid D$ then $p^2 \nmid D$). Show that

$$d_{\mathbb{Q}(\sqrt{D})} = \begin{cases} D & \text{if } D \equiv 1 \mod 4 \\ 4D & \text{if } D \equiv 2, 3 \mod 4 \end{cases}.$$

and find an integral basis for $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ (hint: think about Example 2.3.2).

3. Dedekind domains

3.1. **Failure of unique factorization.** Now let's talk about unique factorization again.

Let's first record a specific instance of the general problem. Consider the field $K = \mathbb{Q}(\sqrt{-5})$. By Exercise 2.4.13 we know that $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\sqrt{-5}$. Now note that $21 = 3 \times 7$, but also

$$21 = 1 + 20 = 1^2 - (-20)^2 = 1^2 - (2(-5))^2 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}).$$

So we have two decompositions of 21. Are they distinct irreducible elements?

Lemma 3.1.1. *3 is irreducible in $\mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$.*

Proof. Suppose $3 = \alpha\beta$ with α and β non-units. Then

$$9 = N_{K/\mathbb{Q}}(3) = N_{K/\mathbb{Q}}(\alpha)N_{K/\mathbb{Q}}(\beta).$$

But since α, β are not units, neither are $N_{K/\mathbb{Q}}(\alpha)$ and $N_{K/\mathbb{Q}}(\beta)$, so $N_{K/\mathbb{Q}}(\alpha) = \pm 3$. Write $\alpha = x + y\sqrt{-5}$ with $x, y \in \mathbb{Z}$. Then we have

$$x^2 + 5y^2 = \pm 3$$

which is a contradiction. □

Exercise 3.1.2. Via the same method as in Lemma 3.1.1, show that 7 and $1 \pm 2\sqrt{-5}$ are irreducible in $\mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$ as well.

Finally, note that

$$\frac{1 \pm 2\sqrt{-5}}{3} \text{ and } \frac{1 \pm 2\sqrt{-5}}{7}$$

are both not in $\mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$, so these factorizations violate uniqueness.

3.2. **The definition.** Now back to commutative algebra, so that we can “fix” the problem.

Definition 3.2.1. If R is a ring, the *Krull dimension* $\dim R \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$ is the length of the longest chain of prime ideals $\mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_k$.

For instance, a field has Krull dimension 0, since the only prime ideal is (0). The ring $\mathbb{Z}$ has Krull dimension 1. To see this note (p) is maximal (since $\mathbb{Z}/p$ is a field) and if $I \subset (p)$ is nonzero and prime then $I = (q)$ for some prime number q, but then $p \mid q$ so $p = q$.

Exercise 3.2.2.

- If $R_1, \ldots, R_k$ is a finite collection of rings, then show that $\dim R_1 \times \cdots \times R_k = \max\{\dim R_1, \cdots, \dim R_k\}$ (hint: think about the structure of prime ideals in the product).
- A field has Krull dimension 0. Conversely show that an Noetherian integral domain of Krull dimension 0 is a field.
- Optional (harder): can you characterize Noetherian reduced rings of Krull dimension 0? (hint: take for granted that a Noetherian ring of Krull dimension 0 is Artinian)
- Show that a PID which is *not* a field has Krull dimension 1 (hint: this is equivalent to showing that every nonzero prime ideal is maximal).

So what are the basic properties of $\mathcal{O}_K$? The basic statement is as follows.

Theorem 3.2.3. *$\mathcal{O}_K$ is a Noetherian and integrally closed domain of Krull dimension 1.*

Proof. To show that $\mathcal{O}_K$ is Noetherian we need to show that every ideal $I \subset \mathcal{O}_K$ is a finitely generated $\mathcal{O}_K$-module. But I is a $\mathbb{Z}$-submodule of $\mathcal{O}_K$, and $\mathcal{O}_K$ is finitely generated over $\mathbb{Z}$ by Corollary 2.4.7, so I is finitely generated over $\mathbb{Z}$ since $\mathbb{Z}$ is Noetherian, so it's finitely generated over $\mathcal{O}_K$. It is integrally closed by Exercise 2.2.16(2), so it remains to show that every nonzero prime ideal is maximal.

First of all note that if $\mathfrak{q} \subset \mathcal{O}_K$ is a prime ideal, then $\mathfrak{p} = \mathfrak{q} \cap \mathbb{Z}$ is a prime ideal in $\mathbb{Z}$. If $\mathfrak{q} = 0$ then $\mathfrak{p} = 0$, but what about if $\mathfrak{p} \neq 0$? Then pick a nonzero $y \in \mathfrak{p}$. Since $y \in \mathcal{O}_K$ there exists $p \in \mathbb{Z}[x]$ such that

$$p(y) = y^n + a_{n-1}y^{n-1} + \cdots + a_0 = 0$$

with $a_0 \neq 0$. It follows that $a_0 \in \mathfrak{q} \cap \mathbb{Z} = \mathfrak{p}$, so $\mathfrak{p} \neq 0$ hence $\mathfrak{p} = (p)$ for some prime number p. Then the map $\mathbb{Z} \to \mathcal{O}_K$ induces a map

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \to \mathcal{O}_K/\mathfrak{q}$$

and since $\mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-module it follows that $\mathcal{O}_K/\mathfrak{q}$ is a finite-dimensional $\mathbb{F}_p$-vector space and is thus finite. But $\mathcal{O}_K/\mathfrak{q}$ is also an integral domain.

Exercise 3.2.4. Show that a finite integral domain is a field.

Applying the exercise, we see that $\mathcal{O}_K/\mathfrak{q}$ is actually a field, so $\mathfrak{q}$ must be maximal. □

Definition 3.2.5. An integral domain is a *Dedekind domain* if it is Noetherian, integrally closed, and has Krull dimension ≤ 1.

So as we saw above, even though $\mathbb{Z}[\sqrt{-5}]$ is not a PID, it is still a Dedekind domain.

Exercise 3.2.6. Show that every PID is a Dedekind domain (hint: put together earlier exercises).

3.3. **Unique factorization in Dedekind domains.** Let $\mathcal{O}$ be an arbitrary Dedekind domain, not necessarily the ring of integers of a number field. Let $K = \mathrm{Frac}(\mathcal{O})$. First, a technical lemma.

Lemma 3.3.1. *Every nonzero ideal $I \subset \mathcal{O}$ contains $\mathfrak{p}_1 \cdots \mathfrak{p}_n$ for some nonzero prime ideals $\mathfrak{p}_i$.*

Proof. Say X denotes the set of nonzero ideals which don't contain the product of primes. If X is nonempty, then since $\mathcal{O}$ is Noetherian we must have that X contains a maximal element I under inclusion. Note I itself can't be prime, so there exist $x, y \in \mathcal{O}$ such that $xy \in I$ but $x, y \notin I$. So then if we let $I_x = I + (x)$ and $I_y = I + (y)$, it follows that $I \subsetneq I_x, I_y$ so $I_x, I_y \notin X$ and hence both contain the product of prime ideals. But note $I_x I_y \subset I$ and thus I contains the product of prime ideals, a contradiction. □

We're going to develop some theory that will let us upgrade the inclusion to an equality. But first we will give a name to some objects we have seen before.

Definition 3.3.2. A *fractional ideal of $\mathcal{O}$* is a finitely generated $\mathcal{O}$-submodule of K.

In particular, any ideal is a fractional ideal, but in general there are more things appearing: the point is that generators of a fractional ideal might be elements of $K \setminus \mathcal{O}$. For instance, if you pick $1/x \in K \setminus \mathcal{O}$ then $\frac{1}{x}\mathcal{O}$ is a fractional ideal.

Exercise 3.3.3.

(1) Show that an $\mathcal{O}$-submodule $\mathfrak{a} \subset K$ is a fractional ideal if and only if there exists a nonzero $r \in \mathcal{O}$ such that $r\mathfrak{a} \subset \mathcal{O}$ (hint: pick a generating set first).

(2) Show that the sum and product of two fractional ideals is again a fractional ideal.

Definition 3.3.4. A *principal fractional ideal* is a fractional ideal of the form $x\mathcal{O}$ for some $x \in K$.

In this way, fractional ideals encompass the notion of "an element of K", or "a fraction of elements in $\mathcal{O}$". But since there are examples of Dedekind domains which are not UFDs (and in particular, not PIDs either), there are non-principal fractional ideals, which means that this is a strict generalization of the notion of an element. Still, it would be nice if they behave like elements, so we'll show now that this is in fact the case.

For instance, you can always divide by a nonzero number in K, so we'd like to be able to "divide" fractional ideals by each other.

Definition 3.3.5. If $\mathfrak{a}, \mathfrak{b} \subset K$ are two fractional ideals with $\mathfrak{b} \neq 0$, their *generalized ideal quotient* is

$$(\mathfrak{a} : \mathfrak{b}) = \{x \in K : x\mathfrak{b} \subset \mathfrak{a}\}.$$

Note that $(\mathfrak{a} : \mathcal{O}) = \{x \in K : x\mathcal{O} \subset \mathfrak{a}\} = \mathfrak{a}$.

Lemma 3.3.6. *$(\mathfrak{a} : \mathfrak{b})$ is a fractional ideal.*

Proof. Note first that if $x, y \in (\mathfrak{a} : \mathfrak{b})$ then $(x+y)\mathfrak{b} = x\mathfrak{b} + y\mathfrak{b} \subset \mathfrak{a} + \mathfrak{a} = \mathfrak{a}$ and if $r \in \mathcal{O}$ then $rx\mathfrak{b} \subset r\mathfrak{a} \subset \mathfrak{a}$, so $x + y, rx \in \mathfrak{a}$ This shows that $(\mathfrak{a} : \mathfrak{b}) \subset K$ is an $\mathcal{O}$-submodule.

It remains to show that $(\mathfrak{a} : \mathfrak{b})$ is finitely generated. For this, first suppose $\mathfrak{a}, \mathfrak{b}$ are actually ideals in $\mathcal{O}$. If $b \in \mathfrak{b}$ is nonzero, then $b(\mathfrak{a} : \mathfrak{b}) \subset \mathfrak{a} \subset \mathcal{O}$ and we apply Exercise 3.3.3(1). By the same exercise there exist nonzero $a, b \in \mathcal{O}$ such that $a\mathfrak{a}, b\mathfrak{b} \subset \mathcal{O}$, so we may apply the previous case noting that

$$(\mathfrak{a} : \mathfrak{b}) = (ab\mathfrak{a} : ab\mathfrak{b}).$$

□

The next exercise is a sanity check of this definition.

Exercise 3.3.7. Show that if $x, y \in K$ with $y \neq 0$ then $(x\mathcal{O} : y\mathcal{O}) = \frac{x}{y}\mathcal{O}$. This shows that the map $K \to \{\text{fractional ideals of } \mathcal{O}\}$ sending $x \mapsto x\mathcal{O}$ preserves division. Does it preserve multiplication? What about addition?

Definition 3.3.8. If $\mathfrak{a}$ is a nonzero fractional ideal we let

$$\mathfrak{a}^{-1} := (\mathcal{O} : \mathfrak{a}) = \{x \in K : x\mathfrak{a} \subset \mathcal{O}\}.$$

Lemma 3.3.9. *If $\mathfrak{p} \subset \mathcal{O}$ is a nonzero prime ideal, then there exists $z \in K \setminus \mathcal{O}$ such that*

$$z\mathfrak{p} \subset \mathcal{O}.$$

In particular, $\mathfrak{p}^{-1} \neq \mathcal{O}$.

Proof. Fix $x \in \mathfrak{p}$ nonzero. By Lemma 3.3.1 we may pick the smallest r such that $(x) \supset \mathfrak{p}_1 \cdots \mathfrak{p}_r$ (for $\mathfrak{p}_i$ nonzero). Since $\mathfrak{p} \supset \mathfrak{p}_1 \cdots \mathfrak{p}_r$ we conclude that $\mathfrak{p} \supset \mathfrak{p}_1$ (up to reordering), but $\mathfrak{p}_1$ is maximal so $\mathfrak{p} = \mathfrak{p}_1$.

By assumption $\mathfrak{p}_2 \cdots \mathfrak{p}_r \not\subset (x)$, so there exists some $y \in \mathfrak{p}_2 \cdots \mathfrak{p}_r$ such that $y \notin (x)$, so $z := y/x \notin \mathcal{O}$. But $y\mathfrak{p} = y\mathfrak{p}_1 \subset \mathfrak{p}_1 \cdots \mathfrak{p}_r \subset (x)$ so $y/x\mathfrak{p} \subset \mathcal{O}$. So $z = y/x \in \mathfrak{p}^{-1}$. □

Corollary 3.3.10. *We have $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$.*

Proof. Note that $1 \in \mathfrak{p}^{-1}$, so

$$\mathfrak{p} \subset \mathfrak{p}\mathfrak{p}^{-1} \subset \mathcal{O}$$

Therefore $\mathfrak{p}\mathfrak{p}^{-1}$ is an ideal in $\mathcal{O}$ but since $\mathfrak{p}$ is maximal we must either have $\mathfrak{p} = \mathfrak{p}\mathfrak{p}^{-1}$ or $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$.

So suppose $\mathfrak{p} = \mathfrak{p}\mathfrak{p}^{-1}$ and by Lemma 3.3.9 we can pick $z \in \mathfrak{p}^{-1} \setminus \mathcal{O}$. But $z\mathfrak{p} \subset \mathfrak{p}$ and since $\mathfrak{p}$ is finitely generated over $\mathcal{O}$ by, say, $a_1, \dots, a_m$, we may write

$$za_i = \sum_j c_{ij} a_j$$

for some $c_{ij} \in \mathcal{O}$. Rearranging, we may write

$$\sum_j (z\delta_{ij} - c_{ij}) a_j = 0$$

But this means that the matrix $A = z\,\mathrm{id}_m - (c_{ij})_{ij}$ kills the nonzero vector $(a_1, \cdots, a_m)^T$ and thus $\det(A) = 0$. But that means that z is a root of the monic polynomial

$$f(X) := \det(X\,\mathrm{id}_m - c_{ij}) \in \mathcal{O}[X]$$

and thus $z \in \mathcal{O}$ since $\mathcal{O}$ is integrally closed, a contradiction. □

Theorem 3.3.11. *If $I \subset \mathcal{O}$ is a nonzero proper ideal then I admits a factorization*

$$I = \mathfrak{p}_1 \cdots \mathfrak{p}_r$$

into nonzero prime ideals $\mathfrak{p}_i$ which is unique up to reordering.

Proof. We proceed as in the proof of Lemma 3.3.1. Let X denote the set of ideals in $\mathcal{O}$ which cannot be written as a product of primes (i.e. do not satisfy the statement of the Theorem). If X is non-empty, then X has a maximal element I since $\mathcal{O}$ is Noetherian. By Zorn's lemma $I \subset \mathfrak{p}$ for some maximal ideal $\mathfrak{p} \subset \mathcal{O}$. Note $\mathfrak{p}$ is prime so $I \neq \mathfrak{p}$. This in fact implies that $\mathfrak{p}^{-1}I \subsetneq \mathfrak{p}^{-1}\mathfrak{p} = \mathcal{O}$. Therefore, $\mathfrak{p}^{-1}I$ is a proper ideal of $\mathcal{O}$ containing I, which means that $\mathfrak{p}^{-1}I \notin X$ by maximality. But that implies that

$$\mathfrak{p}^{-1}I = \mathfrak{p}_1 \cdots \mathfrak{p}_r$$

for some maximal ideals $\mathfrak{p}_i$, and thus

$$I = \mathfrak{p}(\mathfrak{p}^{-1}I) = \mathfrak{p}\mathfrak{p}_1 \cdots \mathfrak{p}_r,$$

a contradiction. Thus we get existence.

Now suppose $\mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s$. Then

$$\mathfrak{p}_1 \supset \mathfrak{q}_1 \cdot \mathfrak{q}_r$$

so up to reordering, $\mathfrak{p}_1 \supset \mathfrak{q}_1$. But since $\mathfrak{q}_1$ is maximal, $\mathfrak{p}_1 = \mathfrak{q}_1$. By multiplying both sides by $\mathfrak{p}_1^{-1}$ we get

$$\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_2 \cdots \mathfrak{q}_r$$

so if we repeat this we will eventually see that $r = s$ and $\mathfrak{p}_i = \mathfrak{q}_i$ (after reordering). □

Remark 3.3.12. The omission of (0) and (1) is a bit artificial; if we remove the assumption that the prime ideals $\mathfrak{p}_i$ be nonzero, then (0) satisfies the existence part of the theorem, but *not* the uniqueness part for dumb reasons. Similarly, $\prod_{i \in \varnothing} \mathfrak{p}_i = (1)$ by convention.

Exercise 3.3.13. Theorem 3.3.11 in particular applies when $\mathcal{O} = \mathbb{Z}$ to give unique factorization of integers into prime numbers (up to a ± 1 ambiguity). Rewrite this proof for $\mathcal{O} = \mathbb{Z}$ without using the word "ideal" and without referencing any ideals. Does this work for any PID?

Remember the properties satisfied by the integers given in Exercise 1.3.1? Noetherianity replaced the well-ordering principle. We have uniqueness of factorization. In fact, we also have a gcd! In particular if we write

$$I = \prod_{i=1}^{r} \mathfrak{p}_i^{v_i} \text{ and } J = \prod_{i=1}^{s} \mathfrak{p}_i^{w_i}$$

with $v_\mathfrak{p} \geq 0$, then $\gcd(I, J) := \prod_{i=1}^{r} \mathfrak{p}_i^{\min(v_i, w_i)}$ is the gcd of I and J, where we say that $\mathfrak{a} \mid \mathfrak{b}$ if $\mathfrak{a} \supset \mathfrak{b}$.

Exercise 3.3.14.

(1) Show that $\gcd(I, J) = I + J$. Find a similar description of the least common multiple and show that $\operatorname{lcm}(I, J) = I \cap J$.

(2) Formulate and prove a "separating powers" principle for ideals in a Dedekind domain.

Exercise 3.3.15. Show that any fractional ideal can be written uniquely in the form

$$\mathfrak{a} = \frac{\mathfrak{p}_1 \cdots \mathfrak{p}_r}{\mathfrak{q}_1 \cdots \mathfrak{q}_s} := \mathfrak{p}_1 \cdots \mathfrak{p}_r (\mathfrak{q}_1)^{-1} \cdots (\mathfrak{q}_s)^{-1}$$

up to reordering, where $\mathfrak{p}_i \neq \mathfrak{q}_j$ for all i and j.

Lemma 3.3.16. *The set of fractional ideals J_K is an abelian group under multiplication.*

Proof. Associativity is clear from the definition. The ideal $\mathcal{O}_K$ is a multiplicative unit. We showed the existence of inverses of nonzero prime ideals in Corollary 3.3.10, and for general fractional ideals use Exercise 3.3.15 to reduce to this case. □

In view of Exercise 3.3.15, we see that any fractional ideal $\mathfrak{a}$ can be written uniquely as

$$\prod_{\mathfrak{p} \text{ maximal}} \mathfrak{p}^{v_\mathfrak{p}}$$

where $v_\mathfrak{p} = 0$ for all but finitely many $\mathfrak{p}$. In summary, what we have shown is that J_K is the free abelian group on the set of maximal ideals of $\mathcal{O}$. This gives rise to an exact sequence

$$1 \to \mathcal{O}^\times \hookrightarrow K^\times \xrightarrow{x \mapsto x\mathcal{O}_K} J_K \twoheadrightarrow \mathrm{Cl}_K \to 0.$$

Note the image of $K^\times \to J_K$ is exactly the subgroup of principal fractional ideals $P_K \leq J_K$, and $\mathrm{Cl}_K := J_K / P_K$ by definition.

Definition 3.3.17. The *class group of K* is Cl_K.

Note at this point that we only assumed that $\mathcal{O}$ was an arbitrary Dedekind domain with fraction field K. But:

Theorem 3.3.18. *If K is a number field and $\mathcal{O}_K$ is its ring of integers, then Cl_K is finite.*

Definition 3.3.19. The *class number of K* is $h_K := |\operatorname{Cl}_K|$.

We will prove this later, after discussing Minkowski's theorem.

Here we note an important point: if $\mathrm{Cl}_K = 0$ then $J_K = P_K$, and therefore every fractional ideal is a principal fractional ideal. In particular, $\mathcal{O}$ is a PID. Conversely if $\mathcal{O}$ is a PID, then in fact every fractional ideal is principal, so $\mathrm{Cl}_K = 0$. Note finally that a Dedekind domain is a PID if and only if it is a UFD (this is an exercise), so the class group can be thought of as a group measuring the "failure of unique factorization".

Exercise 3.3.20. Show that if p is a prime number then $p \nmid h_K$ if and only if every fractional ideal $\mathfrak{a}$ satisfying $\mathfrak{a}^p \in P_K$ is principal.

The previous exercise can be used to show Fermat's Last Theorem for regular primes, as defined earlier in Definition 1.5.3.

Remark 3.3.21. It is not in general true that class groups are finite. A famous theorem of Claborn in [Cla66] states that *every* abelian group can be realized as the class group of some Dedekind domain. For example, one can show that $\mathbb{C}[X, \sqrt{X^3 - X}]$ is a Dedekind domain with class group isomorphic to the 2-torus $\mathbb{C}/(\mathbb{Z} + \mathbb{Z}i)$.

For the more geometrically inclined, this is related to the fact that the ideal class group of a Dedekind domain A is the *Picard group* of $\operatorname{Spec} A$. In the above example, $\operatorname{Spec} A$ is the elliptic curve $y^2 = x^3 - x$ over $\mathbb{C}$ minus the point ∞, and the Picard group of an elliptic curve is $\mathbb{Z}$ times its $\mathbb{C}$-points.

On the other hand, it is not known whether every finite abelian group arises as the class group of a finite extension of $\mathbb{Q}$.

4. Finiteness of the class group

In this section let K be a number field with ring of integers $\mathcal{O}_K$. We wish to prove Theorem 3.3.18, which says that Cl_K is finite. For this, we will use *Minkowski theory*, which concerns the study of lattices and volumes in Euclidean space. In addition, Minkowski theory will give us actual computational tools that we can then use to compute h_K in certain cases.

To begin, we first extend the analogy between numbers and fractional ideals further.

4.1. **Norms of ideals.**

Definition 4.1.1. If $I \subset \mathcal{O}_K$ is a nonzero ideal, then we let

$$N(I) = [\mathcal{O}_K : I] := |\mathcal{O}_K/I| \in \mathbb{Z}$$

which we call the *absolute norm of I*.

Exercise 4.1.2. Show that this is well-defined; in other words, show that $\mathcal{O}_K/I$ is finite (hint: we already showed this when I is a prime ideal).

To justify this generalization of norm to the ideal setting, we note:

Lemma 4.1.3. *If $\alpha \in \mathcal{O}_K$ then $N((\alpha)) = N_{K/\mathbb{Q}}(\alpha)$.*

Proof. Pick an integral basis $\omega_1, \dots, \omega_n$ for $\mathcal{O}_K$. Then if we act by α on this integral basis we get a basis $\alpha\omega_1, \dots, \alpha\omega_n$ of (α). By definition $N_{K/\mathbb{Q}}(\alpha)$ is the determinant of the change of basis matrix between these two bases (viewed as $\mathbb{Q}$-bases of K). But the determinant of a change of basis matrix exactly measures the ratio of the volumes of the fundamental domains of the $\mathbb{Z}$-lattices spanned by the bases — this is a standard fact about determinants which we will not prove. But the ratio of volumes of the fundamental domain is exactly the number of points of $\mathcal{O}_K$ in a fundamental domain of (α): in other words $|\mathcal{O}_K/(\alpha)|$. □

Moreover, this norm plays well with multiplication.

Lemma 4.1.4. *If* $I = \mathfrak{p}_1^{m_1} \cdots \mathfrak{p}_r^{m_r}$, *then*

$$N(I) = N(\mathfrak{p}_1)^{m_1} \cdots N(\mathfrak{p}_r)^{m_r}$$

Proof. The Chinese remainder theorem gives

$$\mathcal{O}_K/I = \mathcal{O}_K/\mathfrak{p}_1^{m_1} \oplus \cdots \oplus \mathcal{O}_K/\mathfrak{p}_r^{m_r}$$

from which it follows that

$$N(I) = N(\mathfrak{p}_1^{m_1}) \cdots N(\mathfrak{p}_r^{m_r})$$

so now we need to show that if $\mathfrak{p} \subset \mathcal{O}_K$ is prime then $N(\mathfrak{p}^m) = N(\mathfrak{p})^m$. But note

$$|\mathcal{O}_K/\mathfrak{p}^m| = |\mathcal{O}_K/\mathfrak{p}| \times |\mathfrak{p}/\mathfrak{p}^2| \times \cdots \times |\mathfrak{p}^{m-1}/\mathfrak{p}^m|$$

Here $\mathfrak{p}/\mathfrak{p}^2$ is the quotient of the two $\mathcal{O}_K$-modules.

Exercise 4.1.5. Note $k_\mathfrak{p} := \mathcal{O}_K/\mathfrak{p}$ is a field (we're in a Dedekind domain so $\mathfrak{p}$ is maximal). For $a > 0$ find a canonical $k_\mathfrak{p}$-vector space structure on $\mathfrak{p}^a/\mathfrak{p}^{a+1}$ and show that it has dimension 1.

Therefore $|\mathfrak{p}^a/\mathfrak{p}^{a+1}| = |\mathcal{O}_K/\mathfrak{p}|$ and so we're done. □

Corollary 4.1.6. *The absolute norm extends to a group homomorphism*

$$N : J_K \to \mathbb{Q}_{>0}^\times.$$

Proof. For $\mathfrak{p} \subset \mathcal{O}_K$ a nonzero ideal define $N(\mathfrak{p}^{-1}) = N(\mathfrak{p})^{-1}$ and extend multiplicatively. □

Exercise 4.1.7. Why did we call N the *absolute norm*? Absoluteness refers to the fact that we are going down from K to $\mathbb{Q}$, in the sense of Lemma 4.1.3. On the other hand, suppose you have an extension of number fields K/F. Then can you think of a way to define an analogous "relative norm"

$$N_{K/F} : J_K \to J_F \ ?$$

Since $\mathbb{Z}$ is a PID we have an isomorphism $\varphi : J_\mathbb{Q} \cong \mathbb{Q}^\times/\{\pm 1\} \cong \mathbb{Q}_{>0}^\times$. This follows from the exact sequence

$$1 \to \mathbb{Z}^\times = \{\pm 1\} \to \mathbb{Q}^\times \to J_\mathbb{Q} \to \mathrm{Cl}_\mathbb{Q} = 1 \to 1$$

so check that your definition satisfies $\varphi \circ N_{K/\mathbb{Q}} = N$.

4.2. **General strategy.** How can we use the norm to prove the finiteness of the class group? Let's try the simplest case. How do we show that the class group of $\mathbb{Q}$ is finite? Of course we know that $h_\mathbb{Q} = 1$ since $\mathbb{Z}$ is a PID, but let's reason via a different method.

The class group $\mathrm{Cl}_\mathbb{Q} \xrightarrow{\sim} \mathbb{Q}_{>0}^\times/\sim$ consists of equivalence classes of fractions (in fact there's only one equivalence class but ignore this for now). For any $C > 0$ we know that the set

$$\{a \in \mathbb{Z}_{>0} : N(a) = |a| < C\}$$

is finite. In other words, if you put a bound on the norm then you only get finitely many numbers. Therefore, if you pick C such that every equivalence class in $\mathrm{Cl}_\mathbb{Q}$ contains an $a \in \mathbb{Z}_{>0}$ with $N(a) < C$, then you're done because there are only finitely many such a. Furthermore, if C is very small then you get a bound on the number of possible equivalence classes: in this case if $1 < C < 2$ then the set above is a singleton.

Of course this is all a bit contrived because we know there's only one equivalence class in $\mathrm{Cl}_\mathbb{Q}$, but the point is that this strategy works in general.

Proposition 4.2.1. *If* $C > 0$ *then*

$$\{I \subset \mathcal{O}_K : N(I) < C\}$$

is finite.

Proof. First note that if $\mathfrak{p}$ is a nonzero prime such that $\mathfrak{p} \cap \mathbb{Z} = (p)$ then $N(\mathfrak{p}) = |\mathcal{O}/\mathfrak{p}| = p^f$ for some $f \geq 1$, because $\mathcal{O}/\mathfrak{p}$ is a finite dimensional $\mathbb{F}_p$-vector space. But note that the condition $\mathfrak{p} \cap \mathbb{Z} = (p)$ is equivalent to $\mathfrak{p} \mid (p)$, i.e. $\mathfrak{p}$ appears in the factorization of (p) into prime ideals. Since this factorization is finite, there are only finitely many $\mathfrak{p}$ such that $\mathfrak{p} \cap \mathbb{Z} = (p)$, and so

$$\{\mathfrak{p} \subset \mathcal{O}_K \text{ prime } : N(\mathfrak{p}) < C\}$$

is bounded for any $C > 0$.

Now if we write $I = \mathfrak{p}_1 \cdots \mathfrak{p}_n$ then

$$N(I) = N(\mathfrak{p}_1) \cdots N(\mathfrak{p}_n)$$

so if we require $N(I) < C$ then clearly there are only finitely many ways to do this. □

So now it remains to find a constant C such that every equivalence class in Cl_K contains an ideal $I \subset \mathcal{O}_K$ such that $N(I) < C$. Minkowski theory will show us that we can take

$$C = \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}$$

where d_K is the discriminant, as before, and s denotes the number of conjugate pairs of mappings $K \hookrightarrow \mathbb{C}$.

4.3. **Minkowski theory.**

Lemma 4.3.1. *If $K/\mathbb{Q}$ is a number field of degree $n = [K : \mathbb{Q}]$, then there are exactly n distinct embeddings $K \hookrightarrow \mathbb{C}$.*

Proof. By the primitive element theorem, there exists α such that $K = \mathbb{Q}(\alpha)$, where α is the root of the minimal polynomial p_α of degree n. Since any homomorphism of characteristic zero fields preserves the prime field $\mathbb{Q}$, an embedding $\tau : K \hookrightarrow \mathbb{C}$ is determined by where it sends α. But $\mathbb{C}$ contains all of the (distinct) roots of p_α (each of which is algebraically indistinguishable), so there are precisely n choices of where α can go, all valid. □

Furthermore, note that if $\tau : K \hookrightarrow \mathbb{C}$ is an embedding, then $K \xrightarrow{\tau} \mathbb{C} \xrightarrow{c} \mathbb{C}$ is also an embedding; here c denotes the complex conjugation automorphism of $\mathbb{C}$.

Definition 4.3.2. If $\tau : K \hookrightarrow \mathbb{C}$ is an embedding of K into $\mathbb{C}$ then we say that τ is *real* if its image is contained in $\mathbb{R}$, and *complex* otherwise. In other words, τ is real if and only if $\tau = c \circ \tau$. We denote by r or r_1 the number of real embeddings of K, and by s or r_2 the number of complex conjugate pairs of embeddings.

So $n = r_1 + 2r_2 = r + 2s$.

Exercise 4.3.3. Show that there exists a canonical isomorphism

$$K \otimes_{\mathbb{Q}} \mathbb{C} \xrightarrow{\sim} \prod_{\tau : K \hookrightarrow \mathbb{C}} \mathbb{C}$$

such that the map $K \to K \otimes_{\mathbb{Q}} \mathbb{C} \to \prod_{\tau : K \hookrightarrow \mathbb{C}} \mathbb{C}$ sends α to $(\tau(\alpha))_{\tau : K \hookrightarrow \mathbb{C}}$ (hint: you know that $K = \mathbb{Q}(\alpha)$ for some $\alpha \in K$, how does this help?).

From now on we write $K_{\mathbb{C}} := K \otimes_{\mathbb{Q}} \mathbb{C}$, which is an n-dimensional $\mathbb{C}$-vector space. As such, it admits a natural inner product. Writing $x = (x_\tau)_{\tau : K \hookrightarrow \mathbb{C}}$, we have

$$\langle x, y \rangle = \sum_\tau x_\tau \overline{y_\tau},$$

which is $\mathbb{C}$-linear in x and y and satisfies $\langle x, y \rangle = \overline{\langle y, x \rangle}$ and $\langle x, x \rangle > 0$ for $x \neq 0$.

So right now we have a complex vector space which is defined naturally via K. But ultimately we want to do Euclidean geometry, so we first descend to the real numbers. There is a natural map

$$\begin{aligned} F : K_{\mathbb{C}} &\xrightarrow{\sim} K_{\mathbb{C}} \\ (x_\tau) &\mapsto (\overline{x_{\overline{\tau}}})_{\tau : K \hookrightarrow \mathbb{C}} \end{aligned}$$

given by complex conjugation.

Example 4.3.4. So for example, if $K = \mathbb{Q}(i)$ then $K_{\mathbb{C}} = \mathbb{C} \times \mathbb{C}$ and $F(x, y) = (\overline{y}, \overline{x})$. On the other hand if $K = \mathbb{Q}(\sqrt{2})$ then $K_{\mathbb{C}} = \mathbb{C} \times \mathbb{C}$ again but $F(x, y) = (\overline{x}, \overline{y})$.

Exercise 4.3.5.

- Check that $\langle Fx, Fy \rangle = \overline{\langle x, y \rangle}$.
- Note that F can alternatively be described as the map $K \otimes_{\mathbb{Q}} \mathbb{C} \xrightarrow{\mathrm{id} \otimes \overline{(\cdot)}} K \otimes_{\mathbb{Q}} \mathbb{C}$ taking $\alpha \otimes c \mapsto \alpha \otimes \overline{c}$. In other words, it is induced by the unique nontrivial element of $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$.

In view of Exercise 4.3.5 we define

$$K_{\mathbb{R}} := K_{\mathbb{C}}^{+} = K_{\mathbb{C}}^{F=1} = \{x \in K_{\mathbb{C}} : Fx = x\}.$$

Lemma 4.3.6. *$K_{\mathbb{R}}$ is an n-dimensional $\mathbb{R}$-vector space.*

Proof. If $\rho_1, \ldots, \rho_r$ are the real embeddings and $\sigma_1, \overline{\sigma_1}, \ldots, \sigma_s, \overline{\sigma_s}$ are the complex conjugate pairs of embeddings, then we can label the $\mathbb{C}$ appearing in $K_{\mathbb{C}}$ as

$$K_{\mathbb{C}} = \prod_{i=1}^{r} \mathbb{C}_{\rho_i} \times \prod_{i=1}^{s} (\mathbb{C}_{\sigma_i} \times \mathbb{C}_{\overline{\sigma_i}})$$

and F acts by complex conjugation on each $\mathbb{C}_{\rho_i}$ separately, and acts on each $(\mathbb{C}_{\sigma_i} \times \mathbb{C}_{\overline{\sigma_i}})$ by complex conjugation and swapping. Now if $x \in K_{\mathbb{C}}$ satisfies $F(x) = x$ then $x_{\rho_i} = \overline{x_{\rho_i}}$ for all i and $x_{\sigma_i} = x_{\overline{\sigma_i}}$ for all i. This means that $x_{\rho_i} \in \mathbb{R}$ and $x_{\overline{\sigma_i}}$ is completely determined by x_{σ_i}, which is a free choice in $\mathbb{C}$, which has real dimension 2. □

Remark 4.3.7. $K_{\mathbb{R}}$ can alternatively be described as $K \otimes_{\mathbb{Q}} \mathbb{R}$.

Thus we get an isomorphism

$$\begin{aligned} K_{\mathbb{R}} &\xrightarrow{\sim} \prod_{\tau : K \hookrightarrow \mathbb{C}} \mathbb{R} \\ (x_\tau)_{\tau : K \hookrightarrow \mathbb{C}} &\mapsto (z_\tau)_{\tau : K \hookrightarrow \mathbb{C}} \end{aligned}$$

where $z_\tau = x_\tau$ for τ real and $z_\tau = \mathrm{Re}(x_\tau)$ and $z_{\overline{\tau}} = \mathrm{Im}(x_\tau)$ for τ complex.

Exercise 4.3.8. Show that if $x, y \in K_{\mathbb{R}}$ then

$$\overline{\langle x, y \rangle} = \langle x, y \rangle$$

and so we get a map $\langle -, - \rangle : K_{\mathbb{R}} \times K_{\mathbb{R}} \to \mathbb{R}$.

Lemma 4.3.9. *The scalar product $\langle -, - \rangle : K_{\mathbb{R}} \times K_{\mathbb{R}} \to \mathbb{R}$ induces a scalar product on $\mathbb{R}^n$ under the above isomorphism, and is computed as*

$$\prod_{\tau} \mathbb{R} \times \prod_{\tau} \mathbb{R} \to \mathbb{R}$$

$$(x, y) \mapsto \sum_{i=1}^{r} \gamma_\tau x_\tau y_\tau$$

where

$$\gamma_\tau = \begin{cases} 1 & \tau \textit{ is real} \\ 2 & \tau \textit{ is complex} \end{cases}.$$

Proof. If τ is real then $x_\tau, y_\tau \in \mathbb{R}$, so $x_\tau \overline{y_\tau} = x_\tau z_\tau$. If τ is complex then write $x_\tau = a_\tau + b_\tau i$ and $y_\tau = c_\tau + d_\tau i$. Then

$$x_\tau \overline{y_\tau} + x_{\overline{\tau}} \overline{y_{\overline{\tau}}} = x_\tau \overline{y_\tau} + \overline{x_\tau} y_\tau = 2\operatorname{Re}(x_\tau \overline{y_\tau}) = 2(a_\tau c_\tau + b_\tau d_\tau).$$

□

This scalar product on $\mathbb{R}^n$ gives rise to a metric and makes $K_\mathbb{R}$ into a metric space, which then gives rise to a *measure* on $\mathbb{R}^n$, which differs from the usual Lebesgue measure (induced by the standard inner product) as follows: if X is a measurable subset of $\mathbb{R}^n$ then

$$\operatorname{vol}(X) = 2^s \operatorname{vol}_{\text{Lebesgue}}(X).$$

Exercise 4.3.10. Show that if $\alpha \in K$ then the map $K \to K_\mathbb{C}$ taking $\alpha \mapsto (\tau(\alpha))_\tau$ actually lands in $K_\mathbb{R}$ (hint: this is basically an exercise in unraveling the definitions. alternatively you can solve the exercises about tensor products first, and then this is immediate).

So we denote $j : K \to K_\mathbb{R}$.

Proposition 4.3.11. *Suppose $I \subset \mathcal{O}_K$ is a nonzero ideal. Then its image in $K_\mathbb{R}$ (which is a complete lattice) has fundamental domain D_I with volume $\sqrt{|d_K|}N(I)$.*

Proof. Fix a $\mathbb{Z}$-basis $\alpha_1, \dots, \alpha_n$ of I and let $\Gamma = \mathbb{Z}j(\alpha_1) + \dots + \mathbb{Z}j(\alpha_n) \subset K_\mathbb{R}$. This forms a complete lattice. Fix an ordering $\tau_1, \dots, \tau_n$ of the embeddings $K \hookrightarrow \mathbb{C}$ and let $A = (\tau_\ell(\alpha_i))_{i,\ell}$. By Lemma 2.4.12,

$$\det(A)^2 = d(\alpha_1, \dots, \alpha_n) = [\mathcal{O}_K : I]^2 d_K.$$

We are interested in computing

$$\operatorname{vol}(D_I) = \sqrt{|\det(\langle j(\alpha_i), j(\alpha_k)\rangle)_{i,k}|}$$

But

$$(\langle j(\alpha_i), j(\alpha_k)\rangle)_{i,k} = (\sum_{\ell=1}^n \tau_\ell(\alpha_i)\overline{\tau}_\ell(\alpha_k))_{i,k} = A\overline{A}^t$$

where $A = (\tau_\ell(\alpha_i))_{i,\ell}$. Therefore

$$\operatorname{vol}(D_I) = |\det(A)| = \sqrt{|d_K|}[\mathcal{O}_K : I] = \sqrt{|d_K|}N(I).$$

□

Recall that wanted to show that for any ideal class in Cl_K there exists a representative $I \subset \mathcal{O}_K$ such that $N(I) \le (2/\pi)^s \sqrt{|d_K|}$.

First pick an arbitrary fractional ideal $\mathfrak{a}$ in the class. Then there exists $\gamma \in \mathcal{O}_K$ such that $I := \gamma\mathfrak{a}^{-1} \subset \mathcal{O}_K$. Now if we can show that there exists a nonzero element $x \in I$ such that

$$N(xI^{-1}) \le (2/\pi)^s \sqrt{|d_K|}$$

then we would be done because then $xI^{-1} = x\gamma^{-1}\mathfrak{a} \subset \mathcal{O}_K$ is in the same fractional ideal class as $\mathfrak{a}$, and is bounded by $(2/\pi)^s \sqrt{|d_K|}$. So we prove this:

Proposition 4.3.12. *In every nonzero ideal $I \subset \mathcal{O}_K$, there exists some $x \in I$ such that*

$$|N_{K/\mathbb{Q}}(x)| \le \left(\frac{2}{\pi}\right)^s \sqrt{|d_K|}N(I)$$

First we sketch a proof of an auxiliary lemma:

Lemma 4.3.13. *If $c_\tau > 0$ are real numbers such that $c_\tau = c_{\overline{\tau}}$ such that*

$$\prod_\tau c_\tau > (2/\pi)^s \sqrt{|d_K|} N(I)$$

then there exists some nonzero $x \in I$ such that $|\tau(x)| < c_\tau$ for all $\tau : K \hookrightarrow \mathbb{C}$.

Proof sketch. Define $X = \{(z_\tau) \in K_\mathbb{R} : |z_\tau| < c_\tau\}$. This is convex and centrally symmetric (i.e. if $x \in X$ then $-x \in X$). One can compute that

$$\operatorname{vol}(X) > 2^n \operatorname{vol}(D_I)$$

and thus *Minkowski's lattice point theorem* (stated below in Theorem 4.3.15) says that X contains a nonzero lattice point. □

Exercise 4.3.14. Fill in the "one can compute that" in the above exercise: in other words, show that

$$\operatorname{vol}(\{(z_\tau) \in K_\mathbb{R} : |z_\tau| < c_\tau\}) > 2^n \operatorname{vol}(D_I)$$

(hint: use Proposition 4.3.11, and remember that volume is computed with respect to the scalar product on $K_\mathbb{R}$, so compute the image in $\prod_\tau \mathbb{R}$).

Proof of Proposition 4.3.12. Choose c_τ so that $\prod_\tau c_\tau = (2/\pi)^s \sqrt{|d_K|} N(I) + \epsilon$ for some $\epsilon > 0$. Then by the Lemma we can find $x \in I$ such that

$$|N_{K/\mathbb{Q}}(x)| = \prod_\tau |\tau(x)| < (2/\pi)^s \sqrt{|d_K|} N(I) + \epsilon$$

but since $\epsilon > 0$ is arbitrary and $|N_{K/\mathbb{Q}}(x)| \in \mathbb{Z}_{>0}$, we must have some nonzero $x \in I$ such that

$$|N_{K/\mathbb{Q}}(x)| \leq (2/\pi)^s \sqrt{|d_K|} N(I).$$

□

So finally we conclude that Cl_K is finite!

For the sake of completeness, we state Minkowski's lattice point theorem.

Theorem 4.3.15 (Minkowski). *Fix $L \subset \mathbb{R}^n$ is a lattice and D_L is a fundamental domain, and suppose $X \subset \mathbb{R}^n$ is a convex subset satisfying the property that $x \in X \iff -x \in X$ (we say X is centrally symmetric). Then if $\operatorname{vol}(X) > 2^n \operatorname{vol}(D_L)$, it follows that X contains a nonzero point in L.*

4.4. **Examples.** We have used Minkowski's Lattice Point Theorem to show that for any K, there exists a constant $C_K = (2/\pi)^s \sqrt{|d_K|}$ such that any ideal class contains an ideal with norm bounded by C_K.

Let's use this to compute a class number!

Example 4.4.1. Let's do what is possibly the simplest case. Consider the field $K = \mathbb{Q}(i)$. There is one conjugate pair of complex embeddings so $s = 1$. Recall from Exercise 2.4.13 that since $-1 \equiv 3 \bmod 4$ we have $d_K = -4$. So in this case

$$C_K = \frac{4}{\pi} < 2.$$

So every class in Cl_K contains a representative with norm $N(I) < 2$. But $N(I) \in \mathbb{Z}$ so $N(I) = 1$. But then $1 = N(I) = [\mathcal{O}_K : I]$ so $I = \mathcal{O}_K$. Thus $\mathcal{O}_K$ is the only ideal of norm one, and therefore $h_K = 1$.

Of course you might object that we already knew that $\mathbb{Z}[i]$ is a PID, but this gives another proof.

Exercise 4.4.2. Find every quadratic field $K/\mathbb{Q}$ (i.e. a field of the form $K = \mathbb{Q}(\sqrt{D})$ with $D \in \mathbb{Z}$ squarefree) satisfying $C_K < 2$. Conclude that $h_K = 1$ in these cases.

Before doing some other examples, let's pause here to note that our bound C_K is not actually optimal, so to do any more simple examples, we need something better. We won't actually prove the better bound, but we give a rough idea of how one can obtain it.

Definition 4.4.3. If $C \in \mathbb{R}$ is a number such that every class in Cl_K contains an ideal $I \subset \mathcal{O}_K$ such that $N(I) < C$, then we say that C is an *norm bound for K*.

In particular C_K is a norm bound for K.

Fact 4.4.4. *If $n = [K : \mathbb{Q}]$, the constant*

$$C'_K := \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|d_K|}$$

is a norm bound for K. We won't prove this, but the idea is to repeat the proof of Lemma 4.3.13 with the (centrally symmetric and convex) set

$$X' = \left\{(z_\tau) \in K_{\mathbb{R}} : \sum_\tau |z_\tau| < n\right\}$$

instead of X.

So now equipped with our much improved bound, let's see what we can do.

Example 4.4.5. Let $K = \mathbb{Q}(\sqrt{2})$, then $n = 2$ and there are no complex embeddings so $s = 0$. Note $d_K = 8$. We compute that

$$C_K = \sqrt{8} = 2\sqrt{2}.$$

But this is larger than 2. On the other hand,

$$C'_K = \frac{1}{2}\sqrt{8} = \sqrt{2} < 1$$

so as in Exercise 4.4.2, we see that $h_K = 1$.

Exercise 4.4.6. Find all quadratic fields K satisfying $C'_K < 2$.

Note that so far we've only been able to show that certain number fields have class number 1. To find fields with class number > 1 it's not enough to just have an upper bound, we need a lower bound as well.

We showed in Proposition 4.2.1 that the number of ideals I such that $N(I) < C$ for some given constant $C > 0$ is finite.

But we can be more precise about this: let's note one convenient fact that will help us do some calculations.

Lemma 4.4.7. *If C is a norm bound for K and*

$$\mathcal{P}_C := \{p \text{ prime } : p < C\},$$

Then Cl_K is generated by the classes of the primes appearing in the decomposition

$$p\mathcal{O}_K = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}$$

for all $p \in \mathcal{P}_C$.

Proof. We know that Cl_K is generated by the classes of the ideals with norm $N(I) < C$. By existence of prime factorization, this implies that Cl_K is generated by the classes of prime ideals with norm $N(\mathfrak{p}) < C$. But note that if $(p) = \mathfrak{p} \cap \mathbb{Z}$, then $\mathfrak{p} \mid (p)$, so $\mathfrak{p}$ appears in the prime factorization of p. Note further that $N(\mathfrak{p})$ is a power of p since $\mathcal{O}_K/\mathfrak{p}$ is a finite dimensional $\mathbb{F}_p$-vector space so $p < N(\mathfrak{p}) < C$ and thus $p \in \mathcal{P}_C$. □

Example 4.4.8. Let's consider $K = \mathbb{Q}(\sqrt{-5})$. We considered this example in Section 3.1 where we saw that $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ cannot be a unique factorization domain. Let's try to compute its class number. First note that $-5 \equiv 3 \mod 4$, there is one pair of complex embeddings and thus

$$C'_K = \frac{1}{2}\left(\frac{2}{\pi}\right)\sqrt{20} = \frac{4}{\pi}\sqrt{5} \cong 2.85 < 3.$$

So now we just need to count the number of ideals with norm 1 and 2. There's obviously only one ideal with norm 1. But we already know that $\mathcal{O}_K$ is not a UFD, so there must be a non-identity ideal class containing an ideal of norm 2. But by Lemma 4.4.7 we just need to figure out the prime factorization of $2\mathcal{O}_K$.

So what does a maximal ideal look like in $\mathbb{Z}[\sqrt{-5}]$? To find one, you can try quotienting by things until you get a field. For instance, first we may "force $\sqrt{-5}$ to be equal to an integer", i.e. quotient by $a - \sqrt{-5}$ for $a \in \mathbb{Z}$. This yields

$$\mathbb{Z}[\sqrt{-5}]/(a - \sqrt{-5}) = \mathbb{Z}[x]/(x^2 + 5, a - x) = \mathbb{Z}/(a^2 + 5)$$

In general this won't be a field unless $a^2 + 5$ is prime. But regardless, if you just pick $p \mid a^2 + 5$ then

$$\mathbb{Z}[\sqrt{-5}]/(p, a - \sqrt{-5}) = \mathbb{Z}/(a^2 + 5, p) = \mathbb{F}_p$$

which is a field, so $(p, a - \sqrt{-5})$ is a maximal ideal and obviously

$$(p, a - \sqrt{5}) \mid p\mathcal{O}_K.$$

Recall we are looking for prime ideals $\mathfrak{p}$ of norm 2, and so we must have $\mathfrak{p} \cap \mathbb{Z} = 2\mathbb{Z}$. Then a must be odd in order for $2 \mid a^2 + 5$. But then $a = 1 + 2b$ for some $b \in \mathbb{Z}$ so

$$(2, a - \sqrt{-5}) = (2, 1 + 2b - \sqrt{-5}) = (2, 1 - \sqrt{-5}) \mid 2\mathcal{O}_K$$

Note further that

$$(2, 1 - \sqrt{-5})^2 = (4, 2 - 2\sqrt{-5}, 4 - 2\sqrt{-5}) = (4, 2 - 2\sqrt{-5}, 2) = 2\mathcal{O}_K.$$

Finally note

$$4 = N(2\mathcal{O}_K) = N((2, 1 - \sqrt{-5}))^2$$

and therefore $(2, 1 - \sqrt{-5})$ is the only ideal of norm 2. So $h_K = 2$.

5. Prime Splitting

In view of Lemma 4.4.7, it becomes important to consider the process of taking a prime ideal $p\mathbb{Z} \leq \mathbb{Z}$ and considering the ideal generated by its image in $\mathcal{O}_K$. In general, the image, equal to $p\mathcal{O}_K$, won't be prime, but will still be nonzero and thus will have a decomposition into a product of nonzero primes in $\mathcal{O}_K$.

In fact, there's no reason we need to start with the ideal $p\mathbb{Z}$. In particular if L/K is a finite extension of number fields, we can start with a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ and consider the ideal generated by its image in $\mathcal{O}_L$. Again, this may not be prime, but will be nonzero and thus will split uniquely into prime factors.

One could in fact work in an even more general setting of an arbitrary extension of two Dedekind domains, but since we won't need this level of generality we will stick to the case of interest of number fields.

5.1. Inertia and ramification degrees.

Fix L/K an extension of number fields. Then $\mathcal{O}_K \subset \mathcal{O}_L$.

Exercise 5.1.1. Show that if $\mathfrak{p} \subset \mathcal{O}_K$ is a nonzero prime ideal, then $\mathfrak{p}\mathcal{O}_L \subset \mathcal{O}_L$ is a nonzero proper ideal (hint: this amounts to showing that it's not equal to $\mathcal{O}_L$).

Having done this, take $\mathfrak{p} \subset \mathcal{O}_K$ and decompose

$$\mathfrak{p}\mathcal{O}_L = \prod_{\mathfrak{q}} \mathfrak{q}_1^{e_{\mathfrak{q}/\mathfrak{p}}}$$

(this is a finite product).

Definition 5.1.2. The integer $e_{\mathfrak{q}/\mathfrak{p}}$ is called the *ramification index* of $\mathfrak{q}$ over $\mathfrak{p}$.

We implicitly used in the previous section, this implies that $\mathfrak{q} \cap \mathcal{O}_K = \mathfrak{p}$. To see this, note that $\mathfrak{q} \cap \mathcal{O}_K$ is a prime ideal containing $\mathfrak{p}$, so just use maximality. There exists a factorization

$$\begin{tikzcd}
\mathcal{O}_K \arrow[r, hook] \arrow[d] & \mathcal{O}_L \arrow[d] \\
\mathcal{O}_K/\mathfrak{p} \arrow[r, dotted, "\exists"] & \mathcal{O}_L/\mathfrak{q}
\end{tikzcd}$$

Exercise 5.1.3. Show that $\mathcal{O}_L/\mathfrak{q}$ is a finite dimensional $\mathcal{O}_K/\mathfrak{p}$-vector space.

Definition 5.1.4. For $\mathfrak{q} \mid \mathfrak{p}\mathcal{O}_L$, the integer

$$f_{\mathfrak{q}/\mathfrak{p}} := [\mathcal{O}_L/\mathfrak{q} : \mathcal{O}_K/\mathfrak{p}] = \dim_{\mathcal{O}_K/\mathfrak{p}} \mathcal{O}_L/\mathfrak{q}$$

is called the *inertia degree* of $\mathfrak{q}$ over $\mathfrak{p}$.

Example 5.1.5. Let's do a simple example. Say $K = \mathbb{Q}(i)$. Consider the prime number 2. How does $2\mathcal{O}_K$ decompose? Note $\mathcal{O}_K = \mathbb{Z}[i]$ is a PID, so we just need to factor the number 2. But note that

$$(1+i)(1-i) = 2.$$

Note $-i \in \mathbb{Z}[i]^\times$ and $-i(1+i) = 1-i$, so $(1+i) = (1-i)$ (as ideals). This means that $2 = (1+i)^2$. Furthermore,

$$\mathbb{Z}[i]/(1+i) = \mathbb{Z}[x]/(x^2+1, 1+x) = \mathbb{Z}/2$$

So $(1+i)$ is a maximal ideal. Thus in this case $e_{(1+i)} = 2$ and $f_{(1+i)} = 1$. On the other hand, if p is any odd prime, then

$$\mathbb{Z}[i]/p = \mathbb{Z}[x]/(x^2+1, p) = \mathbb{F}_p[x]/x^2+1.$$

- If there exists some $a \in \mathbb{F}_p$ such that $a^2 = -1$ then $-a$ is a root as well and so $x^2+1 = (x-a)(x+a)$ for some $a \in \mathbb{F}_p$. Thus $p\mathbb{Z}[i]$ is not prime, so as we will see later this means that $p\mathbb{Z}[i] = \mathfrak{q}_1\mathfrak{q}_2$ with $\mathfrak{q}_1 \neq \mathfrak{q}_2$, and thus $e_1 = e_2 = f_1 = f_2 = 1$.
- On the other hand if there is no $a \in \mathbb{F}_p$ such that $a^2 = -1$ then x^2+1 is irreducible in $\mathbb{F}_p[x]$ so $\mathbb{Z}[i]/p\mathbb{Z}[i]$ is a degree 2 field extension of $\mathbb{F}_p$, and thus $p\mathbb{Z}[i]$ is a maximal ideal. This means that $e_1 = 1$ and $f_1 = 2$.

If you are familiar with *Legendre symbols* (and *quadratic reciprocity*), you now see that they can be used to determine the splitting behavior of odd primes in quadratic extensions!

Exercise 5.1.6. Show that if $K \subset L \subset M$ is a tower of number fields, and $\mathfrak{m} \subset \mathcal{O}_M$ is a maximal ideal with $\mathfrak{q} = \mathfrak{m} \cap \mathcal{O}_L$ and $\mathfrak{p} = \mathfrak{m} \cap \mathcal{O}_K$, then

$$e_{\mathfrak{m}/\mathfrak{p}} = e_{\mathfrak{m}/\mathfrak{q}} e_{\mathfrak{q}/\mathfrak{p}} \text{ and } f_{\mathfrak{m}/\mathfrak{p}} = f_{\mathfrak{m}/\mathfrak{q}} f_{\mathfrak{q}/\mathfrak{p}}.$$

In other words, the ramification and inertia degrees behave transitively with respect to multiplication.

Recall that if $\mathfrak{q} \subset \mathcal{O}_L$ is a prime ideal and $\mathfrak{p} = \mathfrak{q} \cap \mathcal{O}_K$ (which is also prime), then we say that $\mathfrak{q}$ *divides* $\mathfrak{p}$ and write $\mathfrak{q} \mid \mathfrak{p}$. This is also equivalent to the statement that $\mathfrak{q}$ shows up in the prime ideal factorization of $\mathfrak{p}\mathcal{O}_L$.

Proposition 5.1.7. *We have*

$$\sum_{\mathfrak{q}\mid\mathfrak{p}} e_{\mathfrak{q}/\mathfrak{p}} f_{\mathfrak{q}/\mathfrak{p}} = [L : K] = n.$$

Proof. By the Chinese remainder theorem we have

$$\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L = \bigoplus_{\mathfrak{q}} \mathcal{O}_L/\mathfrak{q}^{e_{\mathfrak{q}/\mathfrak{p}}}.$$

We will show that the left side has dimension n as an $\mathcal{O}_K/\mathfrak{p}$-vector space, and the right side has dimension $\sum_{\mathfrak{q}} e_{\mathfrak{q}/\mathfrak{p}} f_{\mathfrak{q}/\mathfrak{p}}$.

- For the left side, pick a basis $\overline{\omega_1}, \dots \overline{\omega_m}$ of $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ over $\mathcal{O}_K/\mathfrak{p}$, and then pick elements $\omega_1, \dots, \omega_m \in \mathcal{O}_L$ lifting the $\overline{\omega_i}$. We want to show that this is actually a basis for L/K so that $m = n$.

  For linear independence, suppose

$$a_1\omega_1 + \cdots + a_m\omega_m = 0 \tag{2}$$

  for some $a_i \in \mathcal{O}_K$.

Exercise 5.1.8. Show that there exists an element $a \in K$ such that $aa_i \in \mathcal{O}_K$ for all i, but also such that there exists some i satisfying $aa_i \notin \mathfrak{p}$. (hint: consider the fractional ideal $(a_1, \dots, a_n) \subset \mathcal{O}_K$ and its inverse).

Then scaling Equation 2 by a and reducing mod $\mathfrak{p}$ gives a contradiction to linear independence of the $\overline{\omega_i}$. I will skip the proof that it generates L in general and just prove it in the special case where $\mathfrak{p}$ is principal. Write $\mathfrak{p} = (x)$ for $x \in \mathcal{O}_K$. Then

$$N(\mathfrak{p}\mathcal{O}_L) = N(x\mathcal{O}_L) = N_{L/\mathbb{Q}}(x) = N_{K/\mathbb{Q}}(x)^{[L:K]} = N(x\mathcal{O}_K)^{[L:K]} = |\mathcal{O}_K/\mathfrak{p}|^{[L:K]}$$

- For the right side, note that

$$|\bigoplus_{\mathfrak{q}|\mathfrak{p}} \mathcal{O}_L/\mathfrak{q}^{e_{\mathfrak{q}/\mathfrak{p}}}| = \prod_{\mathfrak{q}|\mathfrak{p}} |\mathcal{O}_L/\mathfrak{q}^{e_{\mathfrak{q}/\mathfrak{p}}}| = \prod_{\mathfrak{q}|\mathfrak{p}} N(\mathfrak{q}^{e_{\mathfrak{q}/\mathfrak{p}}}) = \prod_{\mathfrak{q}|\mathfrak{p}} N(\mathfrak{q})^{e_{\mathfrak{q}/\mathfrak{p}}} = \prod_{\mathfrak{q}|\mathfrak{p}} N(\mathfrak{p})^{f_{\mathfrak{q}/\mathfrak{p}}e_{\mathfrak{q}/\mathfrak{p}}} = |\mathcal{O}_K/\mathfrak{p}|^{\sum_{\mathfrak{q}|\mathfrak{p}} f_{\mathfrak{q}/f\mathfrak{p}}e_{\mathfrak{q}/\mathfrak{p}}}.$$

□

So here is a bunch of terminology that people use.

Definition 5.1.9. Write $\mathfrak{p}\mathcal{O}_L = \prod_{\mathfrak{q}} \mathfrak{q}^{e_{\mathfrak{q}/\mathfrak{p}}}$.

- If $e_{\mathfrak{q}/\mathfrak{p}} = f_{\mathfrak{q}/\mathfrak{p}} = 1$ for all $\mathfrak{q}$, then we say that $\mathfrak{p}$ *splits completely* in L.
- If $\mathfrak{p}\mathcal{O}_L$ is a prime ideal we say that $\mathfrak{p}$ is *inert* in $\mathcal{O}_L$. In this case $e_{\mathfrak{p}\mathcal{O}_L/\mathfrak{p}} = 1$ and $f_{\mathfrak{p}\mathcal{O}_L/\mathfrak{q}} = n$.
- If $e_{\mathfrak{q}/\mathfrak{p}} = 1$ we say that $\mathfrak{q}$ is *unramified* over $\mathfrak{p}$.
- If $e_{\mathfrak{q}/\mathfrak{p}} > 1$ we say that $\mathfrak{q}$ is *ramified over* $\mathfrak{p}$.
- If $e_{\mathfrak{q}/\mathfrak{p}} > 1$ and $f_{\mathfrak{q}/\mathfrak{p}} = 1$ then $\mathfrak{q}$ is said to be *totally ramified over* $\mathfrak{p}$.
- If all $\mathfrak{q}/\mathfrak{p}$ are unramified then we say $\mathfrak{p}$ is *unramified* in $\mathcal{O}_L$.

5.2. Dedekind-Kummer theorem.

Now that we know a little bit about how the theory of prime factorization in rings of integers of number fields should go, it is worth asking whether it is possible, in practice, to compute such factorizations. In fact, not only is this possible but it's actually fairly straightforward, assuming you know how to factor polynomials in finite fields.

Recall from Corollary 2.4.7 that if K is a number field then $\mathcal{O}_K$ is a finitely generated free $\mathbb{Z}$-module. In other words, $\mathcal{O}_K$ admits an integral basis.

But what happens if we take L/K an arbitrary finite extension of number fields of degree $n = [L : K]$? Note that $\mathbb{Z}$ is a PID, and it turns out that if $\mathcal{O}_K$ is a PID as well then the same proof basically holds.

Proposition 5.2.1 ([Neu99, Proposition 2.10])**.** *If $\mathcal{O}_K$ is a PID, then $\mathcal{O}_L$ is a finitely generated free $\mathcal{O}_K$-module. In other words there is an isomorphism of $\mathcal{O}_K$-modules*

$$\mathcal{O}_L \cong \mathcal{O}_K\alpha_1 \oplus \cdots \oplus \mathcal{O}_K\alpha_n$$

for some $\alpha_i \in \mathcal{O}_L$.

As we have seen, in general $\mathcal{O}_K$ will not be a PID if $\mathrm{Cl}_K \neq 0$. But on the other it is still always true that $\mathcal{O}_L$ is a finitely generated *projective* $\mathcal{O}_K$-module — this follows from Lemma 2.4.6. The failure of projective modules over Dedekind domains to be free is exactly measured by the class group. We won't say more about this.

Recall that the primitive element theorem says that we may write $L = K(\alpha) = K[x]/(p_\alpha(x))$ for some α. In fact we may assume $\alpha \in \mathcal{O}_L$ by killing the denominators of α. However, it is not necessarily true that $\mathcal{O}_L = \mathcal{O}_K[\alpha] = \mathcal{O}_K[x]/(p_\alpha(x))$ for *any* α generating L over K. In other words, there exist many L/K such that $\{1, \alpha, \dots, \alpha^{n-1}\}$ does not necessarily generate $\mathcal{O}_L$ over $\mathcal{O}_K$ for *any* $\alpha \in \mathcal{O}_L$.

Definition 5.2.2. The *conductor* of $\mathcal{O}_K[\alpha]$ is the largest ideal of $\mathcal{O}_L$ contained in $\mathcal{O}_K[\alpha]$ and is denoted by C_α.

Note that C_α is also naturally an ideal in the ring $\mathcal{O}_K[\alpha]$.

Exercise 5.2.3. Show that

$$C_\alpha = \{x \in \mathcal{O}_L : x\mathcal{O}_L \subset \mathcal{O}_K[\alpha]\}.$$

Lemma 5.2.4. *C_α is nonzero.*

Proof. Since $1, \alpha, \ldots, \alpha^{n-1}$ are linearly independent in K, it follows that $\mathcal{O}_K[\alpha]$ is a free rank $n[K : \mathbb{Q}]$ $\mathbb{Z}$-module. But so is $\mathcal{O}_L$, so by the structure theorem for finitely generated $\mathbb{Z}$-modules the quotient $\mathcal{O}_L/\mathcal{O}_K[\alpha]$ must be finite. In particular

$$|\mathcal{O}_L/\mathcal{O}_K[\alpha]| \in C_\alpha.$$

□

The following theorem says that the splitting behavior of a prime ideal $\mathfrak{p}$ *away from the conductor* can be detected in the mod $\mathfrak{p}$ reduction of the minimal polynomial $p_\alpha(x) \in \mathcal{O}_K[x]$.

Theorem 5.2.5. *Suppose $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ such that $\mathfrak{p}\mathcal{O}_L$ does not contain any prime factors in common with C_α. Write $\overline{p}_\alpha \in k_\mathfrak{p}[x] := \mathcal{O}_K/\mathfrak{p}[x]$, the mod $\mathfrak{p}$ reduction of p_α. Write*

$$\overline{p}_\alpha(x) = \overline{p}_1(x)^{e_1} \cdots \overline{p}_r(x)^{e_r}$$

as the factorization of the polynomial into irreducible polynomials. Then if $p_i(x) \in \mathcal{O}_K[x]$ is an arbitrary lift of $\overline{p}_i(x)$, we have

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}$$

where $\mathfrak{q}_i = \mathfrak{p}\mathcal{O}_L + p_i(\alpha)\mathcal{O}_L$ and

$$f_{\mathfrak{q}_i/\mathfrak{p}} = \deg \overline{p}_i(x).$$

Proof. Since $\mathfrak{p}\mathcal{O}_L$ has no common factors with C_α, we have that $\mathfrak{p}\mathcal{O}_L + C_\alpha = \mathcal{O}_L$. Therefore $\mathfrak{p}\mathcal{O}_L + \mathcal{O}_K[\alpha] = \mathcal{O}_L$ and thus the map

$$\mathcal{O}_K[\alpha] \to \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$$

is surjective. The kernel is $\mathfrak{p}\mathcal{O}_L \cap \mathcal{O}_K[\alpha]$. Note

$$\mathcal{O}_K[\alpha] = (\mathfrak{p}\mathcal{O}_L + C_\alpha) \cap \mathcal{O}_K[\alpha] \subset \mathfrak{p}\mathcal{O}_L \cap \mathcal{O}_K[\alpha] + C_\alpha \subset \mathcal{O}_K[\alpha],$$

so $\mathcal{O}_K[\alpha] = \mathfrak{p}\mathcal{O}_L \cap \mathcal{O}_K[\alpha] + C_\alpha = \mathfrak{p}\mathcal{O}_K[\alpha] + C_\alpha$ (viewed as ideals in $\mathcal{O}_K[\alpha]$). Therefore

$$\mathfrak{p}\mathcal{O}_K[\alpha] \subseteq \mathfrak{p}\mathcal{O}_L \cap \mathcal{O}_K[\alpha] = (\mathfrak{p}\mathcal{O}_K[\alpha] + C_\alpha)(\mathfrak{p}\mathcal{O}_L \cap \mathcal{O}_K[\alpha]) \subseteq \mathfrak{p}\mathcal{O}_K[\alpha]$$

so we conclude that

$$\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \cong \mathcal{O}_K[\alpha]/\mathfrak{p}\mathcal{O}_K[\alpha] = \mathcal{O}_K[x]/(\mathfrak{p}, p_\alpha(x)) = k_\mathfrak{p}[x]/\overline{p}_\alpha(x).$$

By the Chinese Remainder Theorem

$$k_\mathfrak{p}[x]/\overline{p}_\alpha(x) = \prod_{i=1}^{r} k_\mathfrak{p}[x]/(\overline{p}_i(x))^{e_i}.$$

So the prime ideals of $k_\mathfrak{p}[x]/(\overline{p}_\alpha(x))$ are in bijection with the principal ideals $(\overline{p}_i(x))$. The preimages under the map $\mathcal{O}_L \to \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$, which are prime ideals in $\mathcal{O}_L$, are exactly the ideals

$$\mathfrak{q}_i := \mathfrak{p}\mathcal{O}_L + p_i(\alpha)\mathcal{O}_L$$

and moreover $\mathcal{O}_L/\mathfrak{q}_i \xrightarrow{\sim} \mathbb{F}_p[x]/(\overline{p}_i(x))$. Since $\overline{p}_i(x)$ is irreducible,

$$f_i := f_{\mathfrak{q}_i/\mathfrak{p}} = [\mathcal{O}_L/\mathfrak{q}_i : k_\mathfrak{p}] = \deg \overline{p}_i(x).$$

It remains to show that

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}.$$

But

$$\prod_{i=1}^{r} \mathfrak{q}_i^{e_i} = \prod_{i=1}^{r} (\mathfrak{p}\mathcal{O}_L + p_i(\alpha)\mathcal{O}_L)^{e_i} = \mathfrak{p}\mathcal{O}_L(\cdots) + \prod_{i=1}^{r} p_i(\alpha)^{e_i}\mathcal{O}_L \subset \mathfrak{p}\mathcal{O}_L$$

since the latter ideal reduces to $(\overline{p}_\alpha(\alpha)) = 0 \mod \mathfrak{p}\mathcal{O}_L$. Thus

$$\mathfrak{p}\mathcal{O}_L \mid \prod_{i=1}^{r} \mathfrak{q}_i^{e_i}.$$

But in fact this is an equality because p_α is a polynomial of degree n and thus $\sum_{i=1}^{r} e_i f_i = n$. □

Remark 5.2.6. If $\mathcal{O}_L = \mathcal{O}_K[\alpha]$, then $C_\alpha = \mathcal{O}_L$ by definition, in which case you can determine the splitting behavior of all primes, without any restrictions. But you have to be a bit careful: for instance, as we saw earlier, for squarefree D the ring $\mathcal{O}_{\mathbb{Q}(\sqrt{D})} = \mathbb{Z}[\sqrt{D}]$ if and only if $D \equiv 2, 3 \mod 4$. But even though this doesn't hold for $D \equiv 1 \mod 4$ you can still write $\mathcal{O}_{\mathbb{Q}(\sqrt{D})} = \mathbb{Z}[(1+\sqrt{D})/2]$. So even if the obvious α doesn't work there may still be some other α that works.

As a Corollary, we see that there are only finitely many ramified primes.

Corollary 5.2.7. *There are only finitely many prime ideals in $\mathcal{O}_K$ which ramify in $\mathcal{O}_L$.*

Proof. Note $1, \alpha, \ldots, \alpha^{n-1}$ is a basis for K over L. In fact (see [Neu99, Before Prop. I.2.8]),

$$d_{L/K,\alpha} = d_{L/K}(1, \alpha, \ldots, \alpha^{n-1}) = \prod_{i<j} (\alpha_i - \alpha_j)^2$$

which is the discriminant of the polynomial p_α. Now fix $\mathfrak{p}$ a prime ideal such that $\mathfrak{p} \nmid C_\alpha \cap \mathcal{O}_K$ and $\mathfrak{p} \nmid (d_{L/K,\alpha})$. Then $d_{L/K,\alpha} \not\equiv 0 \mod \mathfrak{p}$ and so $\overline{p}_\alpha(x)$ has no repeated roots, which means that when factored into irreducible polynomials there are no repeating factors, i.e.

$$\overline{p}_\alpha(x) = \overline{p}_1(x) \cdots \overline{p}_r(x)$$

for distinct $\overline{p}_i(x)$. But by Theorem 5.2.5 this means that

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1 \cdots \mathfrak{q}_r$$

for *distinct* $\mathfrak{q}_i$. Finally note that there are only finitely many primes dividing $(d_{L/K,\alpha})$ or $C_\alpha \cap \mathcal{O}_K$. □

Remark 5.2.8. In fact, the primes in $\mathcal{O}_K$ which are ramified are exactly the primes dividing

$$\sum_{\omega} d_{L/K}(\omega_1, \ldots, \omega_n)\mathcal{O}_K$$

where ω runs over all bases of L over K contained in $\mathcal{O}_L$. This involves the theory of the discriminant and the different, which we don't go into for now.

Exercise 5.2.9. If L/K is a finite extension, show that if $I, J \subset \mathcal{O}_K$ are ideals then $I = I\mathcal{O}_L \cap \mathcal{O}_K$ and show that $I \mid J \iff I\mathcal{O}_L \mid J\mathcal{O}_L$.

Exercise 5.2.10. Repeat Example 5.1.5 but now for any quadratic extension $\mathbb{Q}(\sqrt{D})$. In particular, for any prime number $p > 0$ compute the prime factorization p in $\mathbb{Q}(\sqrt{D})$ and compute $e_{\mathfrak{q}/p}$ and $f_{\mathfrak{q}/p}$ for all $\mathfrak{q}$ lying over p (hint: as in Example 5.1.5 you'll eventually reduce to the question of whether a number is a square mod p or not: you can stop there, that's a good enough criterion).

5.3. **Galois extensions.** One of our eventual goals is to understand *class field theory* which gives a tight relationship between Galois groups and class groups. So from now on, assume L/K is a Galois extension of number fields with Galois group $G := \mathrm{Gal}(L/K)$. Recall that J_K and J_L denote the groups of fractional ideals of K and L under multiplication respectively.

Lemma 5.3.1. *For any $\mathfrak{a} \in J_L$*

$$\sigma(\mathfrak{a}) = \{\sigma(x) : x \in \mathfrak{a}\} \in J_L$$

as well, and this defines a left action of G on J_L satisfying $\sigma(\mathfrak{a}\mathfrak{b}) = \sigma(\mathfrak{a})\sigma(\mathfrak{b})$ for all $\sigma \in G$ and $\mathfrak{a}, \mathfrak{b} \in J_L$.

Proof. First we show that $\sigma(\mathcal{O}_L) = \mathcal{O}_L$. For this, note that if $x \in \mathcal{O}_L$ then there exists some monic polynomial $f \in \mathcal{O}_K[x]$ such that $f(x) = 0$ and thus

$$0 = \sigma(f(x)) = f(\sigma(x))$$

so $\sigma(x) \in \mathcal{O}_L$ since $\mathcal{O}_L$ is the integral closure of $\mathcal{O}_K$ in L. This shows that $\mathcal{O}_L \subseteq \sigma^{-1}(\mathcal{O}_L)$, so $\sigma(\mathcal{O}_L) \subseteq \mathcal{O}_L$. The same argument with σ^{-1} shows that $\mathcal{O}_L \subseteq \sigma(\mathcal{O}_L)$.

Next, if $\mathfrak{a} \subset L$ is finitely generated over $\mathcal{O}_L$ then $\sigma(\mathfrak{a})$ is finitely generated over $\sigma(\mathcal{O}_L) = \mathcal{O}_L$, and thus belongs to J_L. Note further that $\sigma(\mathfrak{a}) = (0)$ if and only if $\mathfrak{a} = 0$ and

$$(\sigma\tau)(\mathfrak{a}) = \{\sigma(\tau(x)) : x \in \mathfrak{a}\} = \{\sigma(y) : y \in \tau(\mathfrak{a})\} = \sigma(\tau(\mathfrak{a}))$$

and thus G actually acts on J_L.

The rest of the proof is left as an exercise. □

Stated differently, Lemma 5.3.1 says that J_L is a *left G-module.*

Exercise 5.3.2.

(1) Finish the proof above: in particular show that if $\mathfrak{a}, \mathfrak{b} \in J_L$ then $\sigma(\mathfrak{a}\mathfrak{b}) = \sigma(\mathfrak{a})\sigma(\mathfrak{b})$.

(2) Using prime factorization in a Dedekind domain (you could also just do it directly), show that if $\mathfrak{q} \subset \mathcal{O}_L$ is a prime ideal then $\sigma(\mathfrak{q})$ is prime as well.

(3) Show that if $\mathfrak{q} \mid \mathfrak{p}$ then $\sigma(\mathfrak{q}) \mid \mathfrak{p}$ as well.

(4) Conclude that if $\mathfrak{p} \subset \mathcal{O}_K$ is prime then $\sigma(\mathfrak{p}\mathcal{O}_L) = \mathfrak{p}\mathcal{O}_L$.

(5) If $D \neq 0, 1$ is squarefree and p is a prime number which splits completely in $\mathbb{Q}(\sqrt{D})$ as $p = \mathfrak{p}_1\mathfrak{p}_2$ then determine how $\mathrm{Gal}(\mathbb{Q}(\sqrt{D})/\mathbb{Q})$ acts on $\mathfrak{p}_1$ and $\mathfrak{p}_2$ (hint: the Galois group only has one nontrivial element; also Example 5.1.5 and Exercise 5.2.10 let you compute $\mathfrak{p}_1$ and $\mathfrak{p}_2$).

By part (3) of the above exercise, the action of G restricts to an action on the set $\{\mathfrak{q} \mid \mathfrak{p}\} := \{\mathfrak{q} \subset \mathcal{O}_L : \mathfrak{q} \mid \mathfrak{p}\}$.

Lemma 5.3.3. *The G-action on $\{\mathfrak{q} \mid \mathfrak{p}\}$ is transitive. In other words for any $\mathfrak{q}_1, \mathfrak{q}_2 \mid \mathfrak{p}$ there exists σ such that $\sigma(\mathfrak{q}_1) = \mathfrak{q}_2$.*

Proof. Write $\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}$ and assume (without loss of generality) that $\mathfrak{q}_1, \mathfrak{q}_2$ lie in distinct G-orbits. By this assumption and the Chinese remainder theorem, we can choose $x \in \mathcal{O}_L$ such that

$$x \equiv 0 \mod \mathfrak{q}_1 \text{ and } x \equiv 1 \mod \mathfrak{q}_i \text{ for all } i > 1.$$

Note $x \in \mathfrak{q}_1$ so $N_{L/K}(x) \in \mathfrak{q}_1 \cap \mathcal{O}_L^G = \mathfrak{q}_1 \cap \mathcal{O}_K = \mathfrak{p}$. But $x \notin \mathfrak{q}_2$ and by assumption $\sigma(x) \notin \mathfrak{q}_i$ either for any σ. So $N_{L/K}(x) \notin \mathfrak{q}_2 \cap \mathcal{O}_K = \mathfrak{p}$. Contradiction. □

Transitivity implies:

Theorem 5.3.4. *The residue field degrees $f_\mathfrak{q} = [k_\mathfrak{q} : k_\mathfrak{p}]$ are the same for any $\mathfrak{q}$ as are the ramification indices $e_\mathfrak{q}$.*

Proof. The automorphism σ induces an isomorphism $k_{\mathfrak{q}} \to \mathcal{O}_L/\sigma(\mathfrak{q})$ which fixes $k_{\mathfrak{p}}$. For the equality of $e_{\mathfrak{q}}$ write

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}.$$

Then note

$$\mathfrak{p}\mathcal{O}_L = \sigma(\mathfrak{p}\mathcal{O}_L) = \sigma(\mathfrak{q}_1)^{e_1} \cdots \sigma(\mathfrak{q}_r)^{e_r}.$$

But then by transitivity and uniqueness of prime factorization we must have $e_1 = \cdots = e_r$. □

So in the Galois case we may write $e_{\mathfrak{p}}$ and $f_{\mathfrak{p}}$ instead of $e_{\mathfrak{q}}$ and $f_{\mathfrak{q}}$.

Definition 5.3.5. Let $g_{\mathfrak{p}} := \# \{\mathfrak{q} \mid \mathfrak{p}\}$. We may also abusively write $g_{\mathfrak{q}/\mathfrak{p}}$ as a way to specify which field extension we're considering.

Corollary 5.3.6. $n = [L : K] = e_{\mathfrak{p}} f_{\mathfrak{p}} g_{\mathfrak{p}}$.

Definition 5.3.7. If $\mathfrak{q} \subset \mathcal{O}_L$ is prime the *decomposition group at* $\mathfrak{q}$ is

$$D_{\mathfrak{q}} = \{\sigma \in G : \sigma(\mathfrak{q}) = \mathfrak{q}\}.$$

This is, in other words, the stabilizer of $\mathfrak{q}$ under the G-action on J_L.

Exercise 5.3.8. If $\mathfrak{p} \subseteq \mathcal{O}_K$ is prime then show that the decomposition groups $D_{\mathfrak{q}}$ for $\mathfrak{q} \mid \mathfrak{p}$ are all conjugate and compute $\# D_{\mathfrak{q}}$ and $[G : D_{\mathfrak{q}}]$ (hint: this is group theory).

As we noted before, any $\sigma \in G$ induces an $k_{\mathfrak{p}}$-linear isomorphism $\overline{\sigma} : k_{\mathfrak{q}} \to \mathcal{O}_L/\sigma(\mathfrak{q})$ for any $\mathfrak{q}$. Note $k_{\mathfrak{q}}/k_{\mathfrak{p}}$ is a finite extension of finite fields and is thus Galois, so if $\sigma \in D_{\mathfrak{q}}$ then we may write $\overline{\sigma} \in \mathrm{Gal}(k_{\mathfrak{q}}/k_{\mathfrak{p}})$ and so we get a group homomorphism

$$\begin{aligned} D_{\mathfrak{q}} &\to \mathrm{Gal}(k_{\mathfrak{q}}/k_{\mathfrak{p}}) \\ \sigma &\mapsto \overline{\sigma}. \end{aligned}$$

Since $D_{\mathfrak{q}}$ is a subgroup of $\mathrm{Gal}(L/K)$ it acts on L, so we can consider its fixed field $L^{D_{\mathfrak{q}}}$. Let $\mathfrak{q}' := \mathfrak{q} \cap \mathcal{O}_{L^{D_{\mathfrak{q}}}}$.

Proposition 5.3.9. *The prime $\mathfrak{q}'$ does not split in L; in other words $\mathfrak{q}$ is the only prime dividing $\mathfrak{q}'$ in $\mathcal{O}_L$. Furthermore $e_{\mathfrak{q}/\mathfrak{q}'} = e_{\mathfrak{q}/\mathfrak{p}}$ and $f_{\mathfrak{q}/\mathfrak{q}'} = f_{\mathfrak{q}/\mathfrak{p}}$, so $e_{\mathfrak{q}'/\mathfrak{p}} = f_{\mathfrak{q}'/\mathfrak{p}} = 1$.*

Proof. By Galois theory, $\mathrm{Gal}(L/L^{D_{\mathfrak{q}}}) = D_{\mathfrak{q}}$, so by Lemma 5.3.3 $D_{\mathfrak{q}}$ acts transitively on the primes lying over $\mathfrak{q}'$. But $\mathfrak{q}$ *itself* lies over this prime, and $D_{\mathfrak{q}}$ fixes it by definition. So it must be the only prime lying over it.

Galois theory tells us that $[L^{D_{\mathfrak{q}}} : K] = [G : D_{\mathfrak{q}}]$. Since G acts transitively on $\{\mathfrak{q} \mid \mathfrak{p}\}$, the orbit-stabilizer theorem tells us that $[G : D_{\mathfrak{q}}] = g_{\mathfrak{q}/\mathfrak{p}}$. But then

$$e_{\mathfrak{q}/\mathfrak{q}'} f_{\mathfrak{q}/\mathfrak{q}'} = [L : L^{D_{\mathfrak{q}}}] = [L : K]/[L^{D_{\mathfrak{q}}} : K] = \frac{e_{\mathfrak{q}/\mathfrak{p}} f_{\mathfrak{q}/\mathfrak{p}} g_{\mathfrak{q}/\mathfrak{p}}}{[L^{D_{\mathfrak{q}}} : K]} = e_{\mathfrak{q}/\mathfrak{p}} f_{\mathfrak{q}/\mathfrak{p}}$$

and by Exercise 5.1.6 we know that

$$\begin{aligned} e_{\mathfrak{q}/\mathfrak{p}} &= e_{\mathfrak{q}/\mathfrak{q}'} e_{\mathfrak{q}'/\mathfrak{p}} \\ f_{\mathfrak{q}/\mathfrak{p}} &= f_{\mathfrak{q}/\mathfrak{q}'} f_{\mathfrak{q}'/\mathfrak{p}} \end{aligned}$$

so the rest of the conclusions follow from the fact that all of these indices are positive integers. □

What we have just proven is that in a Galois extension even though one may have ramification (powers of a prime), inertia (extending the residue field), and splitting, by taking an intermediate field extension one can separate the ramification and inertia. In fact, we will show that there is another intermediate subfield $L^{D_{\mathfrak{q}}} \subset L^{I_{\mathfrak{q}}} \subset L$ such that every prime over $\mathfrak{p}$ in $L^{D_{\mathfrak{q}}}$ is inert in $L^{I_{\mathfrak{q}}}$ and every prime over $\mathfrak{p}$ in $L^{I_{\mathfrak{q}}}$ is totally ramified in L. For this we first show:

Theorem 5.3.10. *The map $D_{\mathfrak{q}} \to \mathrm{Gal}(k_{\mathfrak{q}}/k_{\mathfrak{p}})$ is surjective.*

Proof. Since $k_{\mathfrak{q}}/k_{\mathfrak{p}}$ is a finite extension of finite fields, the primitive element theorem applies and we may write $k_{\mathfrak{q}} = k_{\mathfrak{p}}(\overline{a})$ for some $a \in \mathcal{O}_L$. Then let

$$h(x) = \prod_{\sigma \in D_{\mathfrak{q}}} (x - \sigma(a)) \in \mathcal{O}_{L^{D_{\mathfrak{q}}}}[x]$$

be the minimal polynomial over $L^{D_{\mathfrak{q}}}[x]$. Note that

$$\overline{h} := (h \mod \mathfrak{q}') = \prod_{\sigma \in D_{\mathfrak{q}}} (x - \overline{\sigma}(\overline{a})) \in k_{\mathfrak{p}}[x]$$

since $f(L^{D_{\mathfrak{q}}}/K, \mathfrak{q}') = 1$. Furthermore $\overline{h}(\overline{a}) = 0$ and so the minimal polynomial $p_{\overline{a}}$ divides $\overline{h}$. Now suppose $\tau \in \mathrm{Gal}(k_{\mathfrak{q}}/k_{\mathfrak{p}})$; such an element is determined by where it sends $\overline{a}$, so we just need to show that it sends $\overline{a}$ to $\overline{\sigma}(\overline{a})$ for some σ. But $\tau(\overline{a})$ is a root of $p_{\overline{a}}$ so must be a root of $\overline{h}$, i.e. $\tau(\overline{a}) = \overline{\sigma}(\overline{a})$ for some $\sigma \in D_{\mathfrak{q}}$. □

Definition 5.3.11. The *inertia group* $I_{\mathfrak{q}}$ is the subgroup of $D_{\mathfrak{q}}$ defined by the exact sequence

$$0 \to I_{\mathfrak{q}} \to D_{\mathfrak{q}} \to \mathrm{Gal}(k_{\mathfrak{q}}/k_{\mathfrak{p}}) \to 0.$$

Corollary 5.3.12. $|I_{\mathfrak{q}}| = e_{\mathfrak{p}}$.

Proof. The orbit-stabilizer theorem implies that

$$|D_{\mathfrak{q}}| = \frac{|G|}{[G : D_{\mathfrak{q}}]} = \frac{n}{g_{\mathfrak{p}}} = e_{\mathfrak{p}} f_{\mathfrak{p}}$$

and then

$$|I_{\mathfrak{q}}| = \frac{|D_{\mathfrak{q}}|}{[D_{\mathfrak{q}} : I_{\mathfrak{q}}]} = \frac{|D_{\mathfrak{q}}|}{|\mathrm{Gal}(k_{\mathfrak{q}}/k_{\mathfrak{p}})|} = e_{\mathfrak{p}}.$$

□

Exercise 5.3.13. Show that $\mathfrak{q}'$ is inert in $L^{I_{\mathfrak{q}}}$ with inertia degree $f_{\mathfrak{p}}$ and that $\mathfrak{q} \cap \mathcal{O}_{L^{I_{\mathfrak{q}}}}$ is totally ramified with ramification degree $e_{\mathfrak{p}}$.

5.4. **The Artin symbol.** We assume the setup of the previous section, so that L/K is still Galois. Suppose $\mathfrak{p} \subseteq \mathcal{O}_K$ is unramified in $\mathcal{O}_L$, in other words that $e_{\mathfrak{p}} = 1$. Then by Corollary 5.3.12 we see that $I_{\mathfrak{q}}$ is trivial, so

$$D_{\mathfrak{q}} \xrightarrow{\sim} \mathrm{Gal}(k_{\mathfrak{q}}/k_{\mathfrak{p}}).$$

On the other hand we know that $\mathrm{Gal}(k_{\mathfrak{q}}/k_{\mathfrak{p}})$ is a cyclic group, generated by the *Frobenius automorphism*

$$\begin{aligned} \mathrm{Frob}_{\mathfrak{q}} : k_{\mathfrak{q}} &\to k_{\mathfrak{q}} \\ x &\mapsto x^{\# k_{\mathfrak{p}}}. \end{aligned}$$

Definition 5.4.1. Whenever $\mathfrak{q} \mid \mathfrak{p}$ is unramified, the *Frobenius element* $\sigma_{\mathfrak{q}} \in D_{\mathfrak{q}}$ is the image of $\mathrm{Frob}_{\mathfrak{q}}$ under the isomorphism $D_{\mathfrak{q}} \xrightarrow{\sim} \mathrm{Gal}(k_{\mathfrak{q}}/k_{\mathfrak{p}})$.

Exercise 5.4.2. Show that $\sigma_{\mathfrak{q}}$ is the unique $\sigma \in G$ satisfying $\sigma(x) \equiv x^{\# k_{\mathfrak{p}}} \mod \mathfrak{q}$ for all $x \in k_{\mathfrak{q}}$.

We know that $D_{\mathfrak{q}}$ and $D_{\mathfrak{q}'}$ are conjugate whenever $\mathfrak{q}, \mathfrak{q}' \mid \mathfrak{p}$. The above exercise implies that this conjugacy respects the Frobenius element:

Lemma 5.4.3. *If $\mathfrak{q}' \mid \mathfrak{p}$ then $\sigma_{\mathfrak{q}}$ and $\sigma_{\mathfrak{q}'}$ are conjugate in G.*

Proof. Fix τ such that $\tau(\mathfrak{q}) = \mathfrak{q}'$. Then

$$\sigma_{\mathfrak{q}}(\tau^{-1}(x)) \equiv \tau^{-1}(x)^{\#k_{\mathfrak{p}}} \mod \mathfrak{q}$$
$$\tau(\sigma_{\mathfrak{q}}(\tau^{-1}(x))) \equiv \tau(\tau^{-1}(x)^{\#k_{\mathfrak{p}}}) \equiv x^{\#k_{\mathfrak{q}}} \mod \tau(\mathfrak{q}) = \mathfrak{q}'$$

so Exercise 5.4.2 implies that $\tau\sigma_{\mathfrak{q}}\tau^{-1} = \sigma_{\mathfrak{q}'}$. □

Recall that class field theory seeks to understand finite abelian extensions of K.

Definition 5.4.4. If $\mathrm{Gal}(L/K)$ is an abelian group we say that L/K is *abelian.*

If L/K is abelian, the fact that the $\sigma_{\mathfrak{q}}$ are all conjugate means that they are in fact all equal, so we denote them all by $\sigma_{\mathfrak{p}}$.

Definition 5.4.5. If $\mathfrak{p} \subseteq \mathcal{O}_K$ is unramified in L, then we define *Artin symbol*

$$\left(\frac{L/K}{\mathfrak{p}}\right) := \sigma_{\mathfrak{p}}.$$

Let $S = \{\mathfrak{p} : \mathfrak{p} \text{ ramifies in } \mathcal{O}_L\}$ and let $J_K^S \leq J_K$ denote the subgroup of fractional ideals whose prime decomposition does not contain any prime in S (in other words, the free abelian subgroup generated by the primes away from S). Then we extend the Artin symbol to a map

$$\left(\frac{L/K}{\cdot}\right) : J_K^S \to \mathrm{Gal}(L/K)$$
$$\prod_{i=1}^r \mathfrak{p}_i^{a_i} \mapsto \prod_{i=1}^r \left(\frac{L/K}{\mathfrak{p}_i}\right)^{a_i}.$$

One of the main results of class field theory is that the Artin symbol is surjective, and its kernel contains the subgroup $P_K^S \leq J_K^S$ generated by principal prime ideals. You can think of this as a modified class group.

Exercise 5.4.6. If L/K is the extension $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$ for $D \neq 0, 1$ squarefree and p doesn't divide $d_{\mathbb{Q}(\sqrt{D})}$, compute the element $\left(\frac{\mathbb{Q}(\sqrt{D})/\mathbb{Q}}{p}\right) \in \mathrm{Gal}(\mathbb{Q}(\sqrt{D})/\mathbb{Q})$. The point is that $\mathrm{Gal}(\mathbb{Q}(\sqrt{D})/\mathbb{Q})$ only has two elements in it, so this question is asking: which one is $\left(\frac{\mathbb{Q}(\sqrt{D})/\mathbb{Q}}{p}\right)$?

6. Local Fields

Now we're going to completely switch gears and move from the global setting to the local setting. Thus far we have been studying number fields and their rings of integers. Number fields are an example of *global fields* which by definition are either finite extensions of $\mathbb{Q}$ and $\mathbb{F}_q((t))$[1].

In the ring of integers of a number field there are infinitely many prime ideals, because there are infinitely many prime numbers. This makes the structure of the ring intricate and complex, which is concretely illustrated by the fact that the class group is in general impossible to compute in a straightforward and simple way. But on the other hand, when we studied the splitting behavior of prime ideals (Theorem 5.2.5) we found ourselves working modulo a prime ideal. The definition of the decomposition and inertia groups were also described using mod $\mathfrak{p}$ reduction. So it's worth asking, is there a way to somehow "zoom in" on a single prime ideal, and still get a theory in characteristic 0?

The answer is yes, and is given by the theory of *local fields.* The p-adic numbers are the primary example, which we now introduce.

[1] Although we haven't technically covered the latter at all, almost all of the theory applies. Most of the statements about $\mathcal{O}_K$ generalize to Dedekind domains, and there is a purely algebraic proof of the finiteness of the class group in that case, which actually works for number fields as well, see [Sta21].

6.1. **Localization and completion.** First let's review some general commutative algebra. Most of this will be left as an exercise.

Definition 6.1.1. If A is a ring and $S \subset A$ satisfies $\prod_{s \in S_0} s \in S$ for any finite subset $S_0 \subset S$ (in particular taking $S_0 = \varnothing$ gives $1_A \in S$), then the *localization of A at S* is

$$S^{-1}A = \{(a, s) \in R\} / \sim$$

where $(a_1, s_1) \sim (a_2, s_2)$ if there exists $u \in S$ such that $u(a_1 s_2 - a_2 s_1) = 0$. Elements of $S^{-1}A$ are written a/s instead of (a, s) and thought of as "fractions with denominators in S".

Remark 6.1.2.

Exercise 6.1.3.

(1) Show that $S^{-1}A$ naturally acquires the structure of a commutative ring with identity, and show that $A \to S^{-1}A$ sending $a \mapsto a/1$ is a ring homomorphism.

(2) If A is a nonzero ring, then show that $0 \in S \iff S^{-1}A = 0$. For this reason, we will from now on assume that $0 \notin S$.

(3) Show that if A is an integral domain then the u in the equivalence relation can be taken to be 1_A. Also show that $A \to S^{-1}A$ is injective.

(4) Show that if $s \in S$ then its image in $S^{-1}A$ is invertible.

Lemma 6.1.4. *If $\varphi : A \to B$ is a map of rings such that $\varphi(S) \subset B^\times$ then there is a unique map $S^{-1}A \to B$ making*

$$\begin{tikzcd} A \arrow[rr, "\varphi"] \arrow[dr] & & B \\ & S^{-1}A \arrow[ur, "\exists!"] & \end{tikzcd}$$

commute.

Exercise 6.1.5.

(1) Prove Lemma 6.1.4.

(2) Show that for any ring A the map

$$\mathfrak{p} \mapsto \mathfrak{p}S^{-1} := \{p/s : p \in \mathfrak{p}, s \in S\}$$

induces a bijection

$$\{\text{primes in } A \text{ contained in } A \setminus S\} \xrightarrow{\sim} \left\{\text{primes in } S^{-1}A\right\}.$$

Example 6.1.6.

(1) If $S = \{1\}$ then $S^{-1}A \cong A$.

(2) If A is an integral domain and $S = A \setminus \{0\}$ then $S^{-1}A \cong \operatorname{Frac}(A)$. In fact if $T \subset A$ is any multiplicative set not containing 0 then $T \subset S$ and consequently $T^{-1}A \hookrightarrow \operatorname{Frac}(A)$.

(3) If $f \in A$ then we may take $S_f = \left\{1, f, f^2, \dots\right\}$ and we write $A_f := S^{-1}A$. This is an important construction in algebraic geometry, since it gives a generating set of open subsets $\operatorname{Spec} A_f \hookrightarrow \operatorname{Spec} A$ for the Zariski topology.

(4) If $\mathfrak{p} \subset A$ is a prime ideal in any ring A, let $S_\mathfrak{p} = A \setminus \mathfrak{p}$ and write

$$A_\mathfrak{p} := (S_\mathfrak{p})^{-1}A.$$

Note that if A is nonzero then $0 \notin S_\mathfrak{p}$, so $A_\mathfrak{p} \neq 0$. This is the most important example for us. By Exercise 6.1.5 the prime ideals in $A_\mathfrak{p}$ are in bijection with the prime ideals of A contained in $\mathfrak{p}$.

Lemma 6.1.7. *If $\mathfrak{p} \subseteq A$ is a prime ideal, then $A_{\mathfrak{p}}$ is a local ring and* $\mathrm{Frac}(A/\mathfrak{p}) = A_{\mathfrak{p}}/\mathfrak{m}_{\mathfrak{p}}$*, where $\mathfrak{m}_{\mathfrak{p}}$ denotes the unique maximal ideal.*

Proof sketch. The first part follows from Exercise 6.1.5. For the second part see [Neu99, Corollary 11.2]. □

Example 6.1.8. If $A = \mathbb{Z}$ and $\mathfrak{p} = (p)$ then $\mathbb{Z}_{(p)} = \{a/b : a, b \in \mathbb{Z}, p \nmid b\}$. By the above lemma we see that $\mathbb{Z}_{(p)}/\mathfrak{m}_{(p)} = \mathbb{Z}/p$.

6.2. **Discrete valuation rings.** We now want to give an alternate characterization of a Dedekind domain in terms of the local rings. Fix $\mathcal{O}$ a Dedekind domain with fraction field K.

Proposition 6.2.1. *If $S \subset \mathcal{O}$ is a multiplicative subset then $S^{-1}\mathcal{O}$ is a Dedekind domain.*

Proof. First note $S^{-1}\mathcal{O}$ is an integral domain since A is. If $I \subset S^{-1}\mathcal{O}$ is an ideal then one easily shows that note that $(I \cap \mathcal{O})S^{-1}\mathcal{O} = I$. Since $\mathcal{O}$ is Noetherian, the ideal $I \cap \mathcal{O}$ is finitely generated, so the equality shows that I is finitely generated as well. Hence $S^{-1}\mathcal{O}$ is Noetherian. Since prime ideals in $S^{-1}\mathcal{O}$ form a subset of the prime ideals in $\mathcal{O}$ the dimension can only decrease, so $\dim S^{-1}\mathcal{O} \leq 1$. Suppose $x \in K$ satisfies

$$x^n + \frac{a_{n-1}}{s_{n-1}}x^{n-1} + \cdots + \frac{a_0}{s_0} = 0$$

Multiply through by $s = s_1 \cdots s_{n-1}$ to see that sx is integral over $\mathcal{O}$ and thus $sx \in \mathcal{O}$, so $x \in S^{-1}\mathcal{O}$. □

If we take a Dedekind domain $\mathcal{O}$ and localize at a nonzero prime $\mathfrak{p} \subset \mathcal{O}$, then we get a local ring $(\mathcal{O}_{\mathfrak{p}}, \mathfrak{m}_{\mathfrak{p}})$. But $\mathfrak{m}_{\mathfrak{p}}$ is the unique nonzero prime ideal, since $\mathfrak{p}$ has height 1 in $\mathcal{O}$.

Lemma 6.2.2. *If $(R, \mathfrak{m})$ is a local ring then $R^\times = R \setminus \mathfrak{m}$.*

Proof. If $u \in R^\times$ then $(u) = R$ so u does not live in a maximal ideal, in particular does not live in $\mathfrak{m}$, so must live in $R \setminus \mathfrak{m}$. If u is not a unit, then (u) must be contained in $\mathfrak{m}$ by Zorn's lemma. □

Lemma 6.2.3. *$\mathfrak{m}_{\mathfrak{p}}$ is a principal ideal.*

Proof. By Nakayama's lemma, we have $\mathfrak{m}_{\mathfrak{p}} \neq \mathfrak{m}_{\mathfrak{p}}^2$. Pick $\pi \in \mathfrak{m}_{\mathfrak{p}} \setminus \mathfrak{m}_{\mathfrak{p}}^2$. By Proposition 6.2.1 $\mathcal{O}_{\mathfrak{p}}$ is a Dedekind domain, so $\pi\mathcal{O}_{\mathfrak{p}}$ has a prime factorization $\mathfrak{m}_{\mathfrak{p}}^a$ for some a since $\mathfrak{m}_{\mathfrak{p}}$ is the unique nonzero prime in $\mathcal{O}_{\mathfrak{p}}$. By construction $a = 1$. □

The above lemma is sort of remarkable, because in a Dedekind domain $\mathfrak{p}$ does not have to be principal in general. But after localizing, it becomes principal. This situation is so special that we give it a name.

Definition 6.2.4. A *discrete valuation ring (or DVR)* is a principal ideal domain with a unique nonzero maximal ideal.

Now let A be a DVR with maximal ideal $\mathfrak{m}$.

Lemma 6.2.5. *If we pick a generator $\mathfrak{m} = (\pi)$ then every nonzero $a \in A$ can be written uniquely as $a = u\pi^m$ where $u \in A^\times$ and $m \geq 0$.*

Proof. Since A is a PID it is a UFD, so any $a \in A$ which is not a unit can be written as $\prod_{i=1}^n p_i$ where $p_i \in A$ are prime elements. But if p_i is a prime element then (p_i) is a nonzero prime ideal, so it's equal to $\mathfrak{m}_{\mathfrak{p}} = (\pi)$, so $p_i = u\pi$ for some unit u. □

More generally, every element of $\mathrm{Frac}(A)$ can be written $u\pi^n$ for some $n \in \mathbb{Z}$.

Definition 6.2.6. In view of Lemma 6.2.5 we define the *valuation* of $c \in K$ to be the exponent $v(a)$ in the expression

$$c = u\pi^{v(a)}.$$

Exercise 6.2.7. If $K = \operatorname{Frac}(A)$ then show that $v : K^\times \to \mathbb{Z}$ is a group homomorphism.

More interestingly, it satisfies the following inequality:

Lemma 6.2.8. *$v(a+b) \geq \min\{v(a), v(b)\}$ with equality if $v(a) \neq v(b)$.*

Proof. WLOG we can assume $a = u\pi^n$ and $b = \pi^m$ with $n \geq m$. Then $v(u\pi^n + \pi^m) = v(\pi^m(1 + u\pi^{n-m})) = v(\pi^m)v(1 + u\pi^{n-m}) \geq m$. For the equality note that $v(1 + u\pi^x) = 0$ if $x > 0$ since $1 + u\pi^x$ is a unit in this case. □

Proposition 6.2.9. *A Noetherian integral domain A is a Dedekind domain if and only if $A_{\mathfrak{p}}$ is a DVR for all nonzero primes $\mathfrak{p}$.*

Proof. We just showed that if A is a Dedekind domain then $A_{\mathfrak{p}}$ is a DVR for any nonzero prime ideal $\mathfrak{p} \subset A$ in 6.2.3, so we need to show the converse.

Suppose every $A_{\mathfrak{p}}$ is a DVR. Prime ideals in $A_{\mathfrak{p}}$ are in bijection with prime ideals of A contained in $\mathfrak{p}$, so A must be of dimension 1 because there can't be any prime ideals properly contained in the maximal ideal of $A_{\mathfrak{p}}$. For the integrally closed bit, suppose $x \in K$ satisfies a monic polynomial with A coefficients. Then $A \subset A_{\mathfrak{p}}$ and each $A_{\mathfrak{p}}$ is integrally closed (it is a PID) so $x \in \bigcap_{\mathfrak{p}} A_{\mathfrak{p}}$. □

Exercise 6.2.10. Show that if A is a Noetherian integral domain then

$$\bigcap_{\mathfrak{p}} A_{\mathfrak{p}} = A$$

Hint: the intuition is that "if we write $x \in K$ in lowest terms and x is in every $A_{\mathfrak{p}}$ then the denominator must be 1". On the other hand I'm not sure whether "lowest terms" makes sense for an arbitrary integral domain (maybe it does) but regardless you can reason with the ideal $\mathfrak{a} = \{a \in A : ax \in A\}$.

6.3. Norms on a field.

Now given a Dedekind domain A and a prime ideal $\mathfrak{p}$, let's describe how to get the completion $\widehat{K}_{\mathfrak{p}}$.

Definition 6.3.1. An *absolute value* on a field K is a function $|\cdot| : K \to \mathbb{R}_{\geq 0}$ such that

1. $|x| = 0$ if and only if $x = 0$,
2. $|xy| = |x||y|$ for all $x, y \in K$, and
3. $|x+y| \leq |x| + |y|$.

If the stronger inequality

$$|x+y| \leq \max\{|x|, |y|\}$$

is satisfied the then we say that $|\cdot|$ is *nonarchimedean* and *archimedean* otherwise.

Exercise 6.3.2. Show that $|\cdot|$ is nonarchimedean if and only if $\{|n| : n \in \mathbb{N}\}$ is bounded (if you get annoyed by this you can skip it, it's not the most important exercise).

Definition 6.3.3. Two absolute values $|\cdot|_1$ and $|\cdot|_2$ are called *equivalent* if and only if there exists $s \in \mathbb{R}_{>0}$ such that $|\cdot|_1 = |\cdot|_2^s$.

Given a field K and a norm $|\cdot|$ the function

$$d(x,y) = |x-y|$$

defines a metric on K and thus a metric topology generated by the open sets

$$B_r(x) = \{y \in K : |x-y| < r\}$$

Fact 6.3.4. *Two absolute values are equivalent if and only if they generate the same metric topology. We omit the proof.*

Example 6.3.5.

- On any field there is the trivial valuation
$$|x| = \begin{cases} 0 & x = 0 \\ 1 & x \neq 0 \end{cases}.$$
- If K is a number field then we can embed $\iota : K \hookrightarrow \mathbb{C}$ and take the usual absolute value on $\mathbb{C}$. We denote the resulting norm $|\cdot|_\iota$. This norm is archimedean since, e.g. $|2| = 2$.
- If K is a number field we can also take a nonzero prime $\mathfrak{p} \subset \mathcal{O}_K$ and define
$$|x|_\mathfrak{p} := |\mathcal{O}_K/\mathfrak{p}|^{-v_\mathfrak{p}(x)}$$
where $v_\mathfrak{p}$ is the valuation
$$\mathcal{O}_K \to \mathcal{O}_{K,\mathfrak{p}} \to \mathbb{Z}$$
defined in Definition 6.2.6. This is a non-archimedean norm:
  (1) By convention $v_\mathfrak{p}(0) = \infty$ and $v_\mathfrak{p}(x) \in \mathbb{Z}$ otherwise, so $|x|_\mathfrak{p} = 0$ if and only if $x = 0$.
  (2) Multiplicativity follows from the fact that $v_\mathfrak{p} : K^\times \to \mathbb{Z}$ is a group homomorphism.
  (3) Finally, the nonarchimedean property follows from Lemma 6.2.8.

  If $K = \mathbb{Q}$ and $q \neq p$ then $|q|_p = 1$ and $|p|_p = 1/p$.

Theorem 6.3.6 (Ostrowski's Theorem)**.** *Every nontrivial absolute value on a number field K is either equivalent to $|\cdot|_\iota$ for some ι or $|\cdot|_\mathfrak{p}$ for some $\mathfrak{p}$.*

Proof. We'll do the nonarchimedean case for $K = \mathbb{Q}$ and skip the archimedean case. If $|\cdot|$ is nonarchimedean then the strong triangle inequality implies $|n| = |1 + \cdots + 1| \leq 1$. We want to find the prime number p which makes $|\cdot|$ equivalent to $|\cdot|_p$. Note we must have $|p| < 1$ for some p, otherwise by prime factorization $|\cdot|$ would be trivial. So let

$$I = \{a \in \mathbb{Z} : |a| < 1\}.$$

Note that for any n we have $|n| \leq \max(|1|, \ldots, |1|) = 1$. Therefore I is an ideal satisfying $(p) \subset I$. But note $1 \notin I$ so I is a proper ideal so $I = (p)$ by maximality. But that means that $|n| = 1$ for any $n \notin (p)$ and since $|p| < 1$ we have

$$|p|^s = p^{-1}$$

for some $s > 0$.

The proof for the general nonarchimedean case is similar, but one needs to show that $|a| \leq 1$ for a an algebraic integer. □

Remark 6.3.7. Note the close relationship between the valuation and the discrete valuation ring.

$$\mathcal{O}_{K,\mathfrak{p}} = \{x \in K : |x|_\mathfrak{p} \leq 1\}$$
$$\mathcal{O}_{K,\mathfrak{p}}^\times = \{x \in K : |x|_\mathfrak{p} = 1\}$$
$$\mathfrak{m}_\mathfrak{p} = \{x \in K : |x|_\mathfrak{p} < 1\}$$

Exercise 6.3.8. More generally suppose that K is a field with a nonarchimedean norm $|\cdot|$ which is *discrete* in the sense that $|K| \cong \mathbb{Z}$. Then show that

$$A_{|\cdot|} := \{x \in K : |x| \leq 1\}$$

is a DVR with unit group

$$A_{|\cdot|}^{\times} := \{x \in K : |x| = 1\}$$

and maximal ideal

$$\mathfrak{m}_{|\cdot|} := \{x \in K : |x| < 1\}.$$

Before defining completion, let's record a few distinctive properties of a nonarchimedean norm.

Remark 6.3.9. Let K be a field with nonarchimedean norm $|\cdot|$.

- If $x \in K$ and $r > 0$ and $y \in B_r(x)$, then $B_r(x) = B_r(y)$. To see this, note that if $z \in K$ and $|x - z| < r$ then
$$|y - z| = |(y - x) + (x - z)| \leq \max(|y - x|, |x - z|) < \max(r, r) = r.$$
In other words, a nonarchimedean ball has no well-defined center! Every point is the center. Weird!
- Also, every open ball is closed and every closed ball is open. This is because $|K|$ is discrete.
- In fact K with the topology defined by $|\cdot|$ is *totally disconnected*, which means that the connected components of K are single points.

6.4. Completions.

Fact 6.4.1. *If $|\cdot|$ is a norm on a field then the following maps are continuous for the metric topology on K induced by $|\cdot|$ and the product/subspace topologies:*

$$K \times K \xrightarrow{(x,y)\mapsto x+y} K$$

$$K \times K \xrightarrow{(x,y)\mapsto xy} K$$

$$K^{\times} \xrightarrow{x\mapsto x^{-1}} K$$

In other words, K is a topological field.

Proof. For example, we need to show that if $x_n \to x$ and $y_n \to y$ then $x_n + y_n \to x + y$. But

$$\lim_{n\to\infty} |x_n - x + y_n - y| \leq \lim_{n\to\infty} |x_n - x| + |y_n - y| = 0$$

and I'll skip the rest. □

Recall that if M is a metric space then one can define its *completion* by taking equivalence classes of Cauchy sequences in M with respect to the metric. This contains M as a subset, identified with the classes of the constant sequence.

Definition 6.4.2. If K is a field and $|\cdot|$ is a valuation then we denote by $\widehat{K}_{|\cdot|}$ the completion of K with respect to the metric induced by $|\cdot|$. There is a natural injection $K \to \widehat{K}_{|\cdot|}$ given by sending $c \in K$ to the equivalence class of the constant sequence $(c, c, \dots)$.

Example 6.4.3.

- The map $K \to \widehat{K}_{|\cdot|_{\mathrm{triv}}}$ is an isomorphism, since every Cauchy sequence for the trivial norm must eventually be constant.
- If $|\cdot| = |\cdot|_\infty$ is the usual absolute value on $\mathbb{Q}$ then $\widehat{\mathbb{Q}}_{|\cdot|_\infty} = \mathbb{R}$.

- If $|\cdot| = |\cdot|_{\mathfrak{p}}$ where K is a number field and $\mathfrak{p} \subset \mathcal{O}_K$ a prime then we get a field $K_{\mathfrak{p}} := \widehat{K}_{|\cdot|_{\mathfrak{p}}}$ which is the field of $\mathfrak{p}$-*adic numbers.*

Proposition 6.4.4. *$\widehat{K}_{|\cdot|}$ is a complete topological field with respect to pointwise addition and multiplication of Cauchy sequences.*

Proof. Checking the field axioms is straightforward: for example, for division take an equivalence class $[(a_n)] \neq [(0)]$ and pick a representative (a_n) such that $a_n \neq 0$ for all n. Then the inverse is $[(a_n^{-1})]$. For the topology, given a sequence $(a_1, a_2, \dots) \in \widehat{K}_{|\cdot|}$ we can define

$$|(a_1, a_2, \dots)| = \lim_{n\to\infty} |a_n|.$$

One checks that this is a well-defined absolute value, and thus induces a metric topology on $\widehat{K}_{|\cdot|}$. We omit the proof that this makes $\widehat{K}_{|\cdot|}$ into a topological field; it's similar to showing the same property of K. We also omit completeness. □

6.5. **Non-archimedean completions.** Let's focus our attention on non-archimedean completions. Fix K a field, $|\cdot|$ a discrete non-archimedean norm coming from a valuation v, and K_v its completion. First we record a nice feature of non-archimedean norms, which tells us that despite the fact that they break our intuition, they actually have less pathologies, in some sense.

Proposition 6.5.1. *$\sum_{n=0}^{\infty} x_n$ converges if and only if $\lim_{n\to\infty} x_n = 0$.*

Proof. If $\sum_{n=0}^{\infty} x_n$ converges then

$$x_{m+1} = (\sum_{n=0}^{m+1} x_n) - (\sum_{n=0}^{m} x_n) \xrightarrow{m\to\infty} 0$$

Conversely if $\lim_{n\to\infty} x_n = 0$ and $\epsilon > 0$ then pick N such that $|x_n| < \epsilon$ for all $n > N$. Then if $m > n > N$ we have

$$|\sum_{i=n}^{m} x_i| \leq \max_{i\in[n,m]} |x_i| < \epsilon.$$

□

Exercise 6.5.2. More generally, show that a sequence (a_n) is Cauchy if and only if $\lim_{n\to\infty} |a_{n+1} - a_n| = 0$.

Lemma 6.5.3. $|K_v| = |K|$ *(note this is not true for archimedean norms!).*

Proof. If $(a_1, a_2, \dots)$ is a Cauchy sequence which does not converge to 0 then we show that $(|a_1|, |a_2|, \dots)$ is eventually constant. Since it doesn't converge to 0 there exists some N such that $|x_n| > \epsilon$ for every $n > N$. On the other hand after possibly enlarging N we have that $|x_n - x_m| < \epsilon$ for any $n, m > N$ as well. Thus $|x_n - x_m| < |x_n|$. But if $|x_n| \neq |x_m|$ then $|x_n - x_m| = \max(|x_n|, |x_m|)$, a contradiction. □

By Exercise 6.3.8 we see that $A_v = \{x \in K_v : |x| \leq 1\}$ is a DVR. In fact since A is a closed subspace of a complete metric space, it is itself complete as well. Let $A = \{x \in K : |x| \leq 1\}$; this is a subring of A_v which is in general not complete.

Proposition 6.5.4. *There is an isomorphism of topological rings*

$$A_v \xrightarrow{\sim} \varprojlim_i A/\pi^i A$$

where π is a generator of the maximal ideal in A.

Proof. Note first that even though A_v is in general bigger than A, there is still a map $A_v \to A/\pi^n A$. To see this, note that if $[(a_1, a_2, \dots)] \in A$ then eventually we have that $|a_n - a_m|$ is very small, which equivalently means that $v(a_n - a_m)$ is very large, or equivalently $a_n - a_m \in (\pi^N)$ for N very large. But that means that eventually $a_n \equiv a_m \mod \pi^i$ for $n, m > N$, so we can define the image of $[(a_1, a_2, \dots)]$ in $A/\pi^i A$ to be $\overline{a_N}$ for N large enough.

This map $A_v \to A/\pi^i A$ is actually continuous (with the discrete topology on $A/\pi^i A$) because the preimage of a point $\bar{b} \in A/\pi^i A$ is

$$\left\{x \in A_v : x \equiv b \mod \pi^i\right\} = \left\{x \in A_v : |x - b| \leq |\pi|^{-i}\right\}$$

which is an open ball. Furthermore one can check that maps $A_v \to A/\pi^i A$ are compatible as we vary i, so we get a map

$$A_v \to \varprojlim_i A/\pi^i A.$$

Since each $A_v \to A/\pi^i A$ is surjective and each $A/\pi^{i+1} A \to A/\pi^i A$ is too, the map to the limit is as well. Furthermore the kernel is

$$\bigcap_{i \geq 1} \pi^i A_v = 0$$

So the map is an isomorphism. It remains to check that the inverse map is continuous, which we omit. □

Exercise 6.5.5. Fill in the missing details from the proof above.

Why is this a useful thing to note? Let's specialize to the case of $F = \mathbb{Q}$ and $|\cdot|_p$ and consider the completion $\mathbb{Q}_p$. Then $A_v = \mathbb{Z}_p$ in this case is the ring of p-adic integers, which is a complete DVR with uniformizer π, and

$$\mathbb{Z}_p \xrightarrow{\sim} \varprojlim_i \mathbb{Z}/p^i\mathbb{Z}.$$

So to construct some $a \in \mathbb{Z}_p$, you first need to take a number in $\mathbb{Z}/p\mathbb{Z}$, which can be represented by $a_0 \in \{0, \dots, p-1\}$. Then you a number $a_1' \in \mathbb{Z}/p^2\mathbb{Z}$ such that $a_1' \equiv a_0 \mod p$. But this means that $a_1' = a_0 + pa_1$ for some $a_1 \in \{0, \dots, p-1\}$. Similarly you then need $a_2' \in \mathbb{Z}/p^3\mathbb{Z}$ which is written as $a_2' = a_0 + pa_1 + p^2 a_2$. So on and so forth, so that the number we construct is eventually

$$a = \sum_{n=0}^{\infty} a_n p^n.$$

In particular any p-adic integer can be written uniquely in this form. Any p-adic *number* (i.e. an element of $\mathbb{Q}_p$) can be written uniquely as

$$a = \sum_{n \geq N} a_n p^n$$

for some $N \in \mathbb{Z}$ for the same reason.

6.6. **Hensel's Lemma.**

Suppose you take a complete[2] DVR A with maximal ideal $\mathfrak{m}$ and residue field $k = A/\mathfrak{m}$. For instance this could be $A = \mathbb{Z}_p$, but could also be something like $\mathbb{C}[[t]]$, a one variable power series ring over $\mathbb{C}$. In algebraic number theory we care about solving polynomial equations over number fields, so what about over local fields? Given $f(x) \in A[x]$, when does $f(x)$ have a root? A priori this looks like a difficult problem, given that the p-adic numbers are somewhat complex. But when you work with the real numbers, you can use derivatives and Newton's method to solve equations. It turns out that you can do this in the world of complete DVRs as well.

Definition 6.6.1. If $f = \sum_{i=0}^n a_i x^i \in R[x]$ is a polynomial over any ring R, then its *formal derivative* is

$$f' = \sum_{i=1}^{n} i a_i x^{i-1}$$

[2] for the metric topology induced by the norm defined by the valuation

Exercise 6.6.2. Show that the formal derivative satisfies, for all $a, b \in R$ and $f, g \in R[x]$:

$$\begin{aligned}(af+bg)' &= af' + bg'\\ (fg)' &= f'g + fg'\\ (f\circ g)' &= (f'\circ g)g'.\end{aligned}$$

Roots and derivatives of these polynomials behave in the same way you expect from the real case.

Exercise 6.6.3. Show that if $f \in R[x]$ is a polynomial (R is still any commutative ring) and $a \in R$ then

$$f(x) = f(a) + f'(a)(x-a) + g(x)(x-a)^2$$

with $g(x) \in R[x]$ (the point of this exercise is to show that even though the Taylor expansion usually involves dividing by $n!$, if f is a polynomial then $g(x)$ has coefficients in R itself).

Assume now that A is a complete DVR with maximal ideal $\mathfrak{m}$ and residue field $k = A/\mathfrak{m}$.

Lemma 6.6.4. *We have $f(a) = f'(a) = 0$ if and only if $(x-a)^2 \mid f$.*

Proof. The reverse direction is clear. For the forward direction, we Taylor expand around a:

$$f(x) = f(a) + f'(a)(x-a) + g(x)(x-a)^2$$

□

Lemma 6.6.5 (Hensel's Lemma)**.** *If $f \in A[x]$ is monic such that $\overline{f} \in k[x]$ has a simple root $\overline{a} \in k$, then $\overline{a}$ can be lifted to $a \in A$ with $f(a) = 0$.*

Proof. We proceed, as in Newton's method, by picking some arbitrary lift and then then fixing it over and over again, making it get closer to an actual solution.

Pick an arbitrary lift $a_0 \in A$ of $\overline{a}$. Then $f(a_0)$ might not be zero, but at least $\overline{f(a_0)} = 0$. This means that $|f(a_0)| < 1$. But on the other hand $\overline{f'(a_0)} \neq 0$, so $|f'(a_0)| = 1$. Now to correct a_0, we recursively define

$$a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)}.$$

We will prove by induction that

1. $|a_n| \leq 1$, so that $a_n \in A$
2. $|a_n - a_0| < 1$ so that $\overline{a_n} = \overline{a}$
3. $|f'(a_n)| = 1$ so that a_{n+1} is well-defined
4. $|f(a_n)| \leq |f(a_0)|^{2^n} < 1$ so that $f(a_n) \xrightarrow{n\to\infty} 0$

For $n = 0$ each of these properties is immediate. Assume (1)-(4) for n. Then:

1. By properties (3) and (4) we have
$$|a_{n+1} - a_n| = |f(a_n)/f'(a_n)| \leq |f(a_0)|^{2^n} < 1$$
so by property (1) we have $|a_{n+1}| \leq \max(|a_{n+1} - a_n|, |a_n|) \leq 1$.
2. By property (2) we have $|a_{n+1} - a_0| \leq \max(|a_{n+1} - a_n|, |a_n - a_0|) < 1$.
3. If you Taylor expand f' around a_n and plug in a_{n+1} you get
$$f'(a_{n+1}) = f'(a_n) - f''(a_n)\frac{f(a_n)}{f'(a_n)} + g(a_{n+1})\left(\frac{f(a_n)}{f'(a_n)}\right)^2$$
But the second and third term have norm < 1 while the first has norm 1, so $|f'(a_n)| = 1$ by the ultrametric inequality.

(4) If you Taylor expand f around a_n and plug in a_{n+1} you get
$$f(a_{n+1}) = f(a_n) - f'(a_n)\frac{f(a_n)}{f'(a_n)} + h(a_{n+1})\left(\frac{f(a_n)}{f'(a_n)}\right)^2 = h(a_{n+1})\left(\frac{f(a_n)}{f'(a_n)}\right)^2.$$
and thus $|f(a_{n+1})| \le |f(a_n)|^2 \le |f(a_0)|^{2^{n+1}}$.

But now $|a_{n+1} - a_n| = |f(a_n)/f'(a_n)| \le |f(a_0)|^{2^n} \xrightarrow{n\to\infty} 0$ so Exercise 6.5.2 implies that (a_n) is a Cauchy sequence, which must converge in A to some value $a = \lim_{n\to\infty} a_n$. Since f is continuous it satisfies $f(a) = \lim_{n\to\infty} f(a_n) = 0$. Note that
$$|a - a_0| = \lim_{n\to\infty} |a_n - a_0| < 1$$
so $a - a_0 \in \mathfrak{m}$, which means that the reduction of a mod $\mathfrak{m}$ is $\overline{a}$ as desired. □

Exercise 6.6.6.

- Modify the proof of Hensel's lemma so that it only requires $|f(a_0)| < |f'(a_0)|^2$.
- Prove that the lift in Hensel's lemma is unique.

Note that in the proof of Hensel's lemma, we showed that $|f(a_n)| \le |f(a_0)|^{2^n}$. Recall that $|\cdot| = c^{-v(\cdot)}$ for some real number $c > 1$, where v is the valuation on A. So if we translate into the language of valuations, the condition becomes $v(f(a_n)) \ge 2^n v(f(a_0))$. But this then means that
$$f(a_n) \equiv 0 \mod \pi^{2^n v(f(a_0))}.$$
where $\mathfrak{m} = (\pi)$. So in every step of Hensel's lemma, you get deeper and deeper congruences.

Example 6.6.7. So for instance, let's say you want to solve the equation $x^2 - 7$ in the ring $\mathbb{Z}_3$. Note first that $x^2 - 7$ reduces to $x^2 - 1$ in $\mathbb{F}_3$, which has two distinct simple roots. Applying Hensel's lemma to each of them gives you solutions not only to $x^2 - 7$ in $\mathbb{Z}_3$, but also each step gives you solutions to $x^2 - 7$ in $\mathbb{Z}/3^{2^n}\mathbb{Z}$.

Exercise 6.6.8. Using Hensel's lemma, find all of the solutions to $x^2 - 7$ in $\mathbb{Z}/27\mathbb{Z}$.

6.7. **Local fields.** Finally, we state the definition of a local field and sketch a bit of the theory.

Definition 6.7.1. A *local field* is a locally compact non-discrete Hausdorff topological field (c.f. Fact 6.4.1).

Given a local field, one can define a norm $|\cdot|_K : K \to \mathbb{R}_{\ge 0}$ by taking a Haar measure μ (a translation invariant non-trivial measure on the underlying locally compact Hausdorff abelian group for which compact sets have finite measure, which is unique up to scalar multiple) and setting
$$|x|_K = \frac{\mu(aX)}{\mu(X)}$$
for any measurable X such that $0 < \mu(X) < \infty$. One can then show that $|\cdot|_K$ is an absolute value which induces the topology on K, and therefore we may equivalently define:

Definition 6.7.2. A *local field* is a field K with a nontrivial absolute value $|\cdot|_K$ which is locally compact for the topology induced by $|\cdot|_K$.

Example 6.7.3. So for instance, $\mathbb{R}$ and $\mathbb{C}$ are both local fields: take a closed ball around any point, and this will be compact. Also $\mathbb{Q}_p$ is a local field. To see this, note that $\mathbb{Z}_p$ is a profinite ring (it's the inverse limit of finite rings) and is thus compact, and furthermore $\mathbb{Q}_p = \bigcup_{n\in\mathbb{Z}} p^n\mathbb{Z}_p$ and each $p^n\mathbb{Z}_p$ is compact as well since multiplication by p^n is continuous (because $\mathbb{Q}_p$ is a topological field). For the same reason $\mathbb{F}_p((t))$ with the t-adic topology is a local field (note $\mathbb{F}_p[[t]] = \varprojlim_n \mathbb{F}_p[t]/t^n$).

Eventually we will see that these are basically the only examples, up to taking finite extensions. But in order to see this, we need to rule out some other possibilities.

Lemma 6.7.4. *If K is a local field then every closed ball in K is compact.*

Proof. The point $0 \in K$ lies in a compact open neighborhood U, which must contain $B_s(0)$ for some s by definition of the metric topology. Note $B_s(0)$ is compact because it is closed in U. Now take $\alpha \in K^\times$ with $|\alpha| > 0$. Then since multiplication by α is continuous it follows that αU is compact and thus $\alpha^n B_s(0) = B_{|\alpha|^n s}(0)$ is compact as well for all $n > 0$. But if $r > 0$ then $B_r(0) \subset B_{|\alpha|^n s}(0)$ is a closed subspace for n large enough, so $B_r(0)$ is compact. Finally since translation in K is continuous we can transport this argument to any basepoint and thus every $B_r(x)$ is compact. □

Lemma 6.7.5. *A local field K is complete with respect to $|\cdot|_K$.*

Proof. Pick a Cauchy sequence $(x_n) \subset K$. For some $\epsilon > 0$ there exists N so that $x_n \in B_{\leq\epsilon}(x_N)$ for $n > N$. But this is a closed and hence compact ball, so it contains a subsequence $(x_{n_m})_m$ which converges to something in K. □

Definition 6.7.6. If K is a topological field (c.f. Fact 6.4.1) then a vector space V endowed with a topology is a *topological K-vector space* if the addition map $V \times V \xrightarrow{(v,w)\mapsto v+w} V$ and the scalar multiplication map $K \times V \xrightarrow{(k,v)\mapsto k\cdot v} V$ are both continuous.

Finally, the following lemma, whose proof is omitted, rules out infinite extensions of $\mathbb{R}, \mathbb{Q}_p$, or $\mathbb{F}_p((t))$.

Lemma 6.7.7. *If K is a local field and V is a locally compact topological K-vector space then $\dim_K V < \infty$.*

We deduce the classification as a corollary of Ostrowski's theorem (see Theorem 6.3.6).

Theorem 6.7.8. *If K is a local field and its norm is archimedean, then K is either $\mathbb{R}$ or $\mathbb{C}$. If non-archimedean, then K is a finite extension of $\mathbb{Q}_p$ or $\mathbb{F}_p((t))$.*

Proof. Suppose $\operatorname{char} K = 0$. Then K contains $\mathbb{Q}$ and the restriction of $|\cdot|_K$ to $\mathbb{Q}$ must be either $|\cdot|_p$ for some prime p or $|\cdot|_\infty$, the usual archimedean norm. But since K is complete it must be that $\widehat{\mathbb{Q}}_{|\cdot|} \subset K$, so either K contains $\mathbb{Q}_p$ for some p or it contains $\mathbb{R}$.

If $\operatorname{char} K = p$ then K must contain $\mathbb{F}_p$. But note that K must also contain some transcendental element over $\mathbb{F}_p$ because every nonzero element of $\overline{\mathbb{F}_p}$ has finite order and thus has norm 1, but $|\cdot|_K$ was assumed nontrivial. So K contains $\mathbb{F}_p(s)$ for some transcendental element s. One can show that every completion of $\mathbb{F}_p(s)$ is of the form $\mathbb{F}_p((t))$.

Finally note that Lemma 6.7.7 implies $[K : \widehat{\mathbb{Q}}_{|\cdot|}] < \infty$. □

Exercise 6.7.9. Show that in Theorem 6.7.8 the restriction of $|\cdot|_K$ to $\mathbb{Q}$ cannot be the trivial norm.

In the next section we will show that in fact every finite extension of $\mathbb{Q}_p$ is in fact a local field, and that the norm $|\cdot|$ is discrete.

7. Local field extensions

7.1. **Extending norms.** Now let $K/\mathbb{Q}_p$ be a (non-archimedean) local field with valuation v, norm $|x|_K := c^{-v(x)}$ for some $c \in \mathbb{R}$, valuation ring $\mathcal{O}_K$ and uniformizer π_K and residue field $k_K := \mathcal{O}_K/\pi$.

Suppose L/K is a finite extension of degree n. We want to study the problem of extending the norm from K to L. One obvious thing to try is to push elements of L down to K and take the norm, and the most natural way to do this is to define

$$|x|_L := |N_{L/K}(x)|_K^{1/n}$$

Exercise 7.1.1. Show that $|\cdot|_L : L \to \mathbb{R}_{\geq 0}$ is a norm.

We will need the following lemma, whose proof we omit.

Definition 7.1.2. If K is a field with an absolute value $|\cdot|_K$ and V is a K-vector space, then a *norm on* V is a map $\|\cdot\| : V \to \mathbb{R}_{\geq 0}$ satisfying

- $\|v\| = 0 \iff v = 0$,
- $\|\lambda \cdot v\| = |\lambda|_K \|v\|$ for all $\lambda \in K$ and $v \in V$, and
- $\|v + w\| \leq \|v\| + \|w\|$ for all $v, w \in V$.

Lemma 7.1.3. *If V is a finite dimensional vector space over a local field K, then every norm on V induces the same topology on V.*

Theorem 7.1.4.

(1) $|\cdot|_L$ is the unique norm satisfying $|x|_L = |x|_K$ for all $x \in K$ (i.e. which "extends $|\cdot|_K$),

(2) L is complete with respect to $|\cdot|_L$, and

(3) the valuation ring $\mathcal{O}_L = \{x \in L : |x|_L \leq 1\}$ is the integral closure of $\mathcal{O}_K$ in L.

Proof. If $x \in K$ then $N_{L/K}(x) = x^n$, so $|x|_L = |x|_K$. It is a fact that any two norms on a finite dimensional vector space induce the same topology, which means they must be equivalent. But there exists some $x \in K$ such that $|x|_K \neq 1$ so if $|\cdot|_1$ and $|\cdot|_2$ both extend $|\cdot|_K$ then they are equivalent and thus $|x|_1 = |x|_2^a$ but then $a = 1$ since we can take $x \in K$ such that $|x|_K \neq 1$.

(2) is an exercise.

For (3) note that $|\alpha| \leq 1$ if and only if $|N_{L/K}(\alpha)| \leq 1$ so it suffices to show that $\alpha \in L$ is integral over $\mathcal{O}_K$ if and only if $N_{L/K}(\alpha) \in \mathcal{O}_K$. So suppose $\alpha \in L$ is integral over $\mathcal{O}_K$. Then the proof of Proposition 2.3.8 shows that

$$N_{L/K}(\alpha) = (-1)^n p_\alpha(0)^{[L:K(\alpha)]}$$

which lies in $\mathcal{O}_K$ since $p_\alpha \in \mathcal{O}_K[x]$ by assumption. Conversely if $N_{L/K}(\alpha) \in \mathcal{O}_K$ then note $p_\alpha(0)$ is a root of $x^{[L:K(\alpha)]} - (-1)^n N_{L/K}(\alpha) \in \mathcal{O}_K[x]$ and $\mathcal{O}_K$ is integrally closed, so $p_\alpha(0) \in \mathcal{O}_K$. But one can show using Hensel's lemma that a monic irreducible polynomial with constant coefficient in $\mathcal{O}_K$ must live in $\mathcal{O}_K[x]$, so α is integral over $\mathcal{O}_K$. □

Exercise 7.1.5. Show that if K is a local field and $V \cong K^n$ is a finite dimensional topological K-vector space then it is complete for the sup norm

$$\|v\| = \max_{i=1,\ldots,n} |v_i|.$$

In view of the fact that any two norms on a topological K-vector space induce the same topology, conclude part (2) of Theorem 7.1.4.

Note that $|\cdot|_L$ is nonarchimedean, since it's nonarchimedean when restricted to K, and discrete since its value group is at worst generated by nth roots of elements in the value group of K. Thus $\mathcal{O}_L$ is a (complete) DVR by Exercise 6.3.8. In particular $\mathcal{O}_L$ and $\mathcal{O}_K$ are Dedekind domains, but note that there is no prime splitting in the extension $\mathcal{O}_L/\mathcal{O}_K$ because each has a unique maximal ideal. Hence we have

$$(\pi_K)\mathcal{O}_L = (\pi_L)^{e_{L/K}}$$

for some $e_{L/K}$ which we call the *ramification index of* L/K and

$$f_{L/K} := [\mathcal{O}_L/\pi_L : \mathcal{O}_K/\pi_K] = [k_L : k_K],$$

the *inertia degree of* L/K.

In particular since $|\cdot|_L$ extends $|\cdot|_K$ we have

$$|x|_L = c^{-v(x)/e_{L/K}}$$

Exercise 7.1.6. If E/F is a finite extension of number fields and $\mathfrak{q}$ is a prime in E with $\mathfrak{p} := \mathfrak{q} \cap \mathcal{O}_F$, show that one naturally gets an induced field extension $E_{\mathfrak{q}}/F_{\mathfrak{p}}$ and

$$e_{\mathfrak{q}/\mathfrak{p}} = e_{E_{\mathfrak{q}}/F_{\mathfrak{p}}}$$

and

$$f_{\mathfrak{q}/\mathfrak{p}} = f_{E_{\mathfrak{q}}/F_{\mathfrak{p}}}$$

Note that $[L : K] = e_{L/K} f_{L/K}$, so we now study what happens when one of the terms is 1.

7.2. Unramified extensions.

Let $L/K/\mathbb{Q}_p$ be finite extensions.

Definition 7.2.1. If $e_{L/K} = 1$ then L/K is *unramified.*

Note that if L/K is unramified then $[L : K] = [k_L : k_K]$. In other words, a degree n unramified extension of K gives a degree n extension of k_K. Furthermore, we know the classification of finite fields, so we know exactly what k_L and k_K are as soon as we know the degrees $[K : \mathbb{Q}_p]$ and $[L : K]$.

So what about the converse? First we state (without proof) an equivalent (but stronger looking) form of Hensel's Lemma.

Lemma 7.2.2 (Hensel's Lemma II)**.** *If A is a complete DVR with residue field k and $f \in A[x]$ such that $\overline{f} = \overline{g}\overline{h}$ with $\overline{g}, \overline{h} \in k[x]$ coprime, then there exist lifts $g, h \in A[x]$ of $\overline{g}$ and $\overline{h}$ such that $f = gh$.*

Next, we note the following.

Lemma 7.2.3. *If $K/\mathbb{Q}_p$ is a finite extension then every root of unity in K is contained in $\mathcal{O}_K$, and furthermore if $|k_K| = q$ there is a isomorphism of groups $\mu_{q-1}(K) \xrightarrow{\sim} \mu_{q-1}(k_K)$ given by reduction mod ϖ_K.*

Proof. We can write $k_K = \mathbb{F}_q$ for some $q = p^n$. Then the elements of k_K are the roots of $x^q - x$, whose derivative is zero, so these are all simple roots. Then by Hensel's lemma each lifts uniquely to a root of $x^q - x$ in $\mathcal{O}_K$ and thus the group homomorphism $\mu_{q-1}(K) \to \mu_{q-1}(k_K)$ is both injective and surjective. □

Proposition 7.2.4. *Given a finite extension k/k_K, which we can write $\mathbb{F}_{q^n}/\mathbb{F}_q$, the extension $L = K(\zeta_{q^n-1})/K$ is unramified with $k_{K(\zeta_{q^n-1})} \cong k$. Every unramified extension is of this form.*

Proof. First write $k_K = \mathbb{F}_q$. If $[k : k_K] = n$ then k is the splitting field of $x^{q^n} - x$ over $\mathbb{F}_q$. Let $L = K(\zeta_{q^n-1})$, the splitting field of $x^{q^n} - x$ over K.

First we should show that the residue field of L is $\mathbb{F}_{q^n}$. The $(q^n - 1)$th roots of unity have norm 1, so they are all contained in $\mathcal{O}_L$, and thus reduce to $(q^n - 1)$th roots of unity mod $\mathfrak{m}_L$. Let $\alpha \in \mathcal{O}_L$ denote a primitive $q^n - 1$th root of unity. If its reduction $\overline{\alpha} \in k_L$ is not primitive, then it satisfies $\overline{\alpha}^{q^m-1} - 1 = 0$ for some $m < n$, and thus by Hensel's lemma it admits a lift to a $(q^m - 1)$th root of unity $\beta \in \mathcal{O}_L$. But β also satisfies the polynomial $x^{q^n-1} - 1 = 0$, so by uniqueness of lifts we must have $\beta = \alpha$, which is a contradiction since α was primitive. Therefore, k_L contains $\mathbb{F}_{q^n}$ and thus $[k_L : k_K] \geq n$.

In view of the fact that $[L : K] = e_{L/K}[k_L : k_K]$, to see that L/K is unramified it suffices to show that $[L : K] = n$. Let $f = x^{q^n} - x \in \mathcal{O}_K[x]$. Note $\overline{f}' = -1 \in k_K[x]$ so $\overline{f}$ is separable and thus if we write $f = f_1 \cdots f_n$ with f_i monic irreducible then each $\overline{f_i}$ must be monic irreducible; if not then you get a contradiction to Lemma 7.2.2. The minimal polynomial of ζ_{q^n-1} over K is equal to one of the f_i, and since its reduction mod ϖ is the minimal polynomial of $\overline{\zeta_{q^n-1}}$ (which is still a primitive root by Lemma 7.2.3) it has degree n, so f_i must have dimension n as well.

Now suppose L/K is some unramified extension of degree n. Then k_L/k_K is the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$, so let $\overline{\alpha} \in \mathbb{F}_{q^n}^\times$ denote a generator. If we view $x^{q^n} - x \in \mathcal{O}_L[x]$, its reduction in $k_L[x]$ has $\overline{\alpha}$ as a simple root, so by Lemma 6.6.5 we can lift it uniquely to a solution $\alpha \in \mathcal{O}_L$. But then α is a primitive q^{n-1}th root of unity and thus $K(\zeta_{q^n-1}) \subseteq L$, which by degree considerations is an equality. □

Note that if K has residue field $k_L \cong \mathbb{F}_q$ then $K(\zeta_{q^n-1})$ is the splitting field of $x^{q^n} - x$ over K and thus is Galois and its Galois group is

$$\mathrm{Gal}(K(\zeta_{q^n-1})/K) \cong \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) = \mathbb{Z}/n\mathbb{Z},$$

the cyclic group of order n generated by Frobenius. Consequently if we let $\mathbb{Q}_p^{\mathrm{unr}}$ denote the maximal unramified extension of $\mathbb{Q}_p$, then

$$\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{unr}}/\mathbb{Q}_p) = \varprojlim_n \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^n-1})/\mathbb{Q}_p) = \varprojlim_n \mathbb{Z}/n\mathbb{Z} \cong \widehat{\mathbb{Z}}.$$

Exercise 7.2.5. Using Lemma 7.2.2 show that if $p \nmid m$ then $K(\zeta_m)/K$ is unramified. Can you determine the n for which $K(\zeta_{q^n-1}) = K(\zeta_m)$?

7.3. **Local Dedekind-Kummer.** To study ramified field extensions, we need an analogue of the Dedekind-Kummer theorem in the local setting.

Lemma 7.3.1. *If $(R, \mathfrak{m})$ is a local Noetherian ring and $g \in R[x]$, let $S = R[x]/(g)$. Then every maximal ideal of S contains $\mathfrak{m}S$.*

Proof. Suppose $\mathfrak{n} \subset S$ is a maximal ideal which does not contain $\mathfrak{m}S$. Then $\mathfrak{n} + \mathfrak{m}S = S$ by maximality. Note $\mathfrak{n}$ is a finitely generated R-module so take a set $x_1, \ldots, x_m$ which generates $\mathfrak{n}$ as an R-module. Then since $\mathfrak{n} + \mathfrak{m}S = S$, the images of x_i under the map $S \to S/\mathfrak{m}S$ generate $S/\mathfrak{m}S$ as a vector space over $R/\mathfrak{m}$. By Nakayama's lemma, the x_i must actually generate S as an R-module. But then $\mathfrak{n} = S$, which is a contradiction. □

In other words the map $S \to S/\mathfrak{m}S$ induces a bijection on maximal ideals.

Corollary 7.3.2 (Local Dedekind-Kummer)**.** *If $(R, \mathfrak{m})$ is a local Noetherian ring and $g \in R[x]$, then write $\overline{g_1}, \cdots, \overline{g_n}$ for the distinct irreducible factors of $\overline{g} \in R/\mathfrak{m}[x]$. Then the maximal ideals in $S = R[x]/(g)$ are of the form $(\mathfrak{m}, g_i(x))$ where g_i is an arbitrary lift of $\overline{g_i}$.*

Proof. It suffices to describe the maximal ideals in $S/\mathfrak{m}S$. But

$$S/\mathfrak{m}S = R[x]/(\mathfrak{p}, g(x)) = (R/\mathfrak{m})[x]/(\overline{g})$$

so the result follows from the Chinese Remainder Theorem. □

7.4. **Ramified extensions.** Let's say a bit about ramified extensions.

Suppose L/K is ramified of degree e. Then $\mathfrak{m}_L^e = \mathfrak{m}_K$. So $(\pi_L)^e = (\pi_K)\mathcal{O}_L$, or in other words $u\pi_K = \pi_L^e$ for some $u \in \mathcal{O}_L^\times$. As we will see, this implies that $L = K(\pi_L)$. If $u = 1$, this means that $L = K(\pi_K^{1/e})$. But in general if $u \neq 1$, π_L will solve $x^e - u\pi_K = 0$. This is an example of an *Eisenstein polynomial.*

Definition 7.4.1. If $K/\mathbb{Q}_p$ is a p-adic local field, then a monic polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathcal{O}_K[x]$ is *Eisenstein* if $\pi_K \mid a_i$ for $i = 0, \ldots, n-1$ and $\pi_K^2 \nmid a_0$. In other words a_0 generates $\mathfrak{m}_K$.

Fact 7.4.2. *Eisenstein polynomials are irreducible in both $\mathcal{O}_K[x]$ and $K[x]$.*

Lemma 7.4.3. *If $f \in \mathcal{O}_K[x]$ is Eisenstein then $S = \mathcal{O}_K[x]/(f)$ is a DVR with uniformizer x.*

Proof. Note $\overline{f} = x^{\deg f}$ so by Corollary 7.3.2 the ring S has a unique maximal ideal $(\mathfrak{m}_K, x)$. But f is Eisenstein, so $f(0)$ generates $\mathfrak{m}_K$, so the maximal ideal of S is $(f(0), x)$. But $0 = f(x) = f(0) + x(\cdots)$, so actually the maximal ideal is just (x). Now note S is Noetherian by construction, a domain by Fact 7.4.2, and is local with nonzero principal maximal ideal. This implies that it is a DVR. □

Exercise 7.4.4. Show that an integral domain R is a DVR if and only if R is a Noetherian local ring which is not a field and whose maximal ideal is principal.

Proposition 7.4.5. *Fix an extension L/K of p-adic local fields of degree n and fix $\pi_L \in L$ a uniformizer. Then L/K is totally ramified if and only if $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$ and p_{π_L} is Eisenstein.*

Proof. If $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$ with p_{π_L} Eisenstein then as in the above lemma we have

$$\mathcal{O}_L/\mathfrak{m}_L = \mathcal{O}_K[x]/(p_{\pi_L}(0), x) = \mathcal{O}_K/(p_{\pi_L}(0)) = \mathcal{O}_K/\mathfrak{m}_K = k_K$$

so $f_{L/K} = 1$ and thus L is totally ramified.

Conversely if L/K is any totally ramified extension then $\{1, \pi_L, \ldots, \pi_L^{n-1}\}$ is linearly independent over K. To see this note that $v_L(\pi_L^i)$ are all distinct and if

$$\sum_{i=0}^{n-1} a_i \pi_L^i = 0$$

then we must have $v_L(a_i\pi_L^i) = v_L(a_j\pi_L^j)$ for some $i \neq j$. But this can't happen because $v_L(a_i\pi_L^i) = nx + i$ while $v_L(a_j\pi_L^j) = ny + j$ which aren't congruent mod n. So $L = K(\pi_L)$.

The proof that p_{π_L} is Eisenstein is left as an exercise. But Lemma 7.4.3 implies that $\mathcal{O}_K[\pi_L]$ is a DVR contained in the DVR $\mathcal{O}_L$. But since DVRs are Dedekind domains and thus integrally closed, we must have $\mathcal{O}_K[\pi_L] = \mathcal{O}_L$. □

Exercise 7.4.6. In the above proof, show that the minimal polynomial p_{π_L} is Eisenstein. Hint: you know that $v_L(\pi_L) = 1$. Consider the valuations of the coefficients.

Definition 7.4.7. An extension L/K of p-adic local fields is

- *tamely ramified* if $p \nmid e_{L/K}$,
- *wildly ramified* if $p \mid e_{L/K}$,
- *totally tamely ramified* if it's totally ramified and tamely ramified
- *totally wildly ramified* if it's totally ramified and $e_{L/K}$ is a power of p.

Exercise 7.4.8. Show that L/K is totally tamely ramified of degree n if and only if $L = K(\pi_K^{1/n})$ for some uniformizer $\pi_K \in \mathcal{O}_K$. (hint: Hensel's lemma will be useful)

7.5. **Tower.** In a manner completely analogous to the global setting, suppose we have a finite extension L/K of p-adic local fields and let $G_{L/K} = \mathrm{Gal}(L/K)$. Furthermore let

$$I_{L/K} := \ker(G_{L/K} \twoheadrightarrow \mathrm{Gal}(k_L/k_K)).$$

Then the intermediate subfield $L^{\mathrm{unr},K} := L^{I_{L/K}}$ is the maximal unramified extension of K contained in L, and $L/L^{\mathrm{unr},K}$ is totally ramified. It turns out that there is an extension $L^{\mathrm{tame},K}/L^{\mathrm{unr},K}$ which is tamely ramified and such that $L/L^{\mathrm{unr},K}$ is totally wildly ramified. In fact $L^{\mathrm{tame},K}$ is the maximal tamely ramified extension of K (or equivalently $L^{\mathrm{unr},K}$) contained in L. We define the *wild inertia subgroup*

$$P_{L/K} := \mathrm{Gal}(L/L^{\mathrm{tame},K}) \subset G_{L/K}$$

which is a p-group. In fact, $P_{L/K}$ can be identified with the p-Sylow subgroup of $G_{L/K}$.

In summary, there is a tower

$$K \subset L^{\mathrm{unr},K} \subset L^{\mathrm{tame},K} \subset L$$

which corresponds to the tower of subgroups

$$0 \leq P_{L/K} \leq I_{L/K} \leq G_{L/K}.$$

Similarly, there is a tower

$$K \subset K^{\mathrm{unr}} \subset K^{\mathrm{tame}} \subset \overline{K}$$

corresponding to a tower of subgroups

$$0 \leq P_K \leq I_K \leq G_K := \mathrm{Gal}(\overline{K}/K).$$

Here I_K is the *inertia subgroup* and P_K is the *wild inertia subgroup*, which is a pro-p-group.

The reason we separate out the tame and wild parts of inertia is that the tame (and unramified) parts are relatively easy to describe in view of Exercise 7.4.8, whereas the wild part is, well, much wilder and harder to write down explicitly. But what we can say is that $\mathrm{Gal}(K^{\mathrm{tame}}/K)$ is topologically generated by two elements σ, τ which satisfy the equation

$$\sigma\tau\sigma^{-1} = \tau^q$$

where $q = |k_K|$. The point is that:

- $$\mathrm{Gal}(K^{\mathrm{unr}}/K) \xrightarrow{\sim} \mathrm{Gal}(\overline{k_K}/k_K) \cong \widehat{\mathbb{Z}}$$
  which is pro-cyclic and generated by some element σ and
- since the tamely ramified extensions are constructed by taking nth roots of π_K for $(n,p) = 1$,
  $$\mathrm{Gal}(K^{\mathrm{tame}}/K^{\mathrm{unr}}) \xrightarrow{\sim} \varprojlim_{(n,p)=1} \mathbb{Z}/n\mathbb{Z} \cong \prod_{\ell \neq p} \mathbb{Z}_\ell.$$
  which is itself pro-cyclic and generated by some element τ.

7.6. **Product Formula.** Now that we've defined some natural norms on local fields, let's prove a formula which ties together the norms in a neat way.

For this we need a few facts.

Lemma 7.6.1. *If E/F is a finite extension of number fields and $\mathfrak{q} \subset \mathcal{O}_E$ is a prime lying over $\mathfrak{p} \subset \mathcal{O}_F$ then*

$$|x|_{\mathfrak{q}} = |N_{E_{\mathfrak{q}}/F_{\mathfrak{p}}}(x)|_{\mathfrak{p}}.$$

Proof. If $E_{\mathfrak{p}} = F_{\mathfrak{q}}$ then there is nothing to prove. If not then without loss of generality we can assume that $x = \pi_{E_{\mathfrak{q}}}^{w(x)}$ for some $w(x)$, since this doesn't change the norm. But

$$|\pi_{E_{\mathfrak{q}}}^{w(x)}|_{\mathfrak{q}} = |\mathcal{O}_E/\mathfrak{q}|^{-w(x)} = |\mathcal{O}_F/\mathfrak{p}|^{-f_{\mathfrak{q}/\mathfrak{p}}w(x)}$$

and

$$|N_{E_{\mathfrak{q}}/F_{\mathfrak{p}}}(\pi_{E_{\mathfrak{q}}}^{w(x)})|_{\mathfrak{p}} = |N_{E_{\mathfrak{q}}/F_{\mathfrak{p}}}(\pi_{E_{\mathfrak{q}}})|_{\mathfrak{p}}^{w(x)} = |\pi_{F_{\mathfrak{p}}}^{f_{\mathfrak{q}/\mathfrak{p}}}|_{\mathfrak{p}}^{w(x)} = |\mathcal{O}_F/\mathfrak{p}|^{-f_{\mathfrak{q}/\mathfrak{p}}w(x)}$$

where the second equality follows from the fact that $N_{E_{\mathfrak{q}}/F_{\mathfrak{p}}}(\mathfrak{q}\mathcal{O}_{E_{\mathfrak{q}}}) = \mathfrak{p}^{f_{\mathfrak{q}/\mathfrak{p}}}$. □

Exercise 7.6.2. Show that if $\nu : E \hookrightarrow \mathbb{C}$ extends $\iota : F \hookrightarrow \mathbb{R}$ then

$$|\nu(x)|_\infty = |N_{E_{|\cdot|_\nu}/F_{|\cdot|_\iota}}(\nu(x))|_\infty$$

Theorem 7.6.3. *If F is a number field and $x \in F^\times$ then*

$$1 = \prod_{\mathfrak{p} \textit{ prime in } F} |x|_{\mathfrak{p}}$$

where we regard all complex-conjugate pairs of embeddings $\iota : F \hookrightarrow \mathbb{C}$ as primes as well as the prime ideals $\mathfrak{p} \subset \mathcal{O}_F$.

Proof. First we reduce to the case where $F = \mathbb{Q}$. For this, note that

$$F \otimes_{\mathbb{Q}} \mathbb{Q}_p = \prod_{\mathfrak{p}|p} F_{\mathfrak{p}}$$

where we implicitly include the archimedean prime $p = \infty$ by letting $\mathbb{Q}_\infty = \mathbb{R}$ and taking all equivalence classes of archimedean norms of F in the product. By virtue of these isomorphisms,

$$N_{F/\mathbb{Q}}(x) = \prod_{\mathfrak{p}|p} N_{F_{\mathfrak{p}}/\mathbb{Q}_p}(x)$$

But then

$$\begin{aligned}\prod_{\mathfrak{p} \text{ prime in } F} |x|_{\mathfrak{p}} &= \prod_{p \text{ prime in } \mathbb{Q}} \prod_{\mathfrak{p}|p} |x|_{\mathfrak{p}} \\ &= \prod_{p \text{ prime in } \mathbb{Q}} \prod_{\mathfrak{p}|p} |N_{F_{\mathfrak{p}}/\mathbb{Q}_p}(x)|_p \\ &= \prod_{p \text{ prime in } \mathbb{Q}} |N_{F/\mathbb{Q}}(x)|_p\end{aligned}$$

and so it suffices to check the proof for $\mathbb{Q}$.

But if $x \in \mathbb{Q}^\times$ then

$$x = \pm p_1^{v_1} \cdots p_n^{v_n}$$

and thus

$$\prod_{p \in \mathbb{Z} \text{ prime}} |x|_p \times |x|_\infty = (p_1^{-v_1} \cdots p_n^{-v_n}) \times (p_1^{v_1} \cdots p_n^{v_n}) = 1.$$

□

7.7. **Krasner's Lemma.** Thus far we've been talking about finite extensions of local fields. But what about infinite extensions? For instance, what can we say about $\overline{\mathbb{Q}}_p$, the algebraic closure of $\mathbb{Q}_p$? For instance, by Theorem 7.1.4 every finite extension of $\mathbb{Q}_p$ is complete. What about $\overline{\mathbb{Q}}_p$? It turns out the answer is no; writing down an explicit Cauchy sequence which does not converge is possible, but a bit complicated to do, so we omit this here.

Here's another thought. By Theorem 7.1.4 every finite extension of $\mathbb{Q}_p$ has a unique norm extending its norm.

Exercise 7.7.1. Using Theorem 7.1.4, show that $\overline{\mathbb{Q}}_p$ has a unique norm extending the norm on $\mathbb{Q}_p$. Hint: use compatibility of the norm maps $N_{L/K}$. Show furthermore that this norm restricts to the unique norm on any finite extension.

So for instance, this norm restricts to the norm on $\mathbb{Q}_p(p^{1/n})$. As such, the set $\left\{p^{1/n}\right\} \subset |\overline{\mathbb{Q}}_p|$ so the norm on $\overline{\mathbb{Q}}_p$ is not discrete.

So $\overline{\mathbb{Q}}_p$ has a norm, but it's non-discrete and $\overline{\mathbb{Q}}_p$ isn't complete.

Remark 7.7.2. Note that this is different than for the archimedean norm. Namely, the algebraic closure of $\mathbb{R}$ is $\mathbb{C}$, which is complete. This is intimately related to the fact that $\mathbb{C}$ is a finite extension of $\mathbb{R}$.

But we can still complete; in analogy with the archimedean case let $\mathbb{C}_p$ denote the completion of $\overline{\mathbb{Q}}_p$.

Theorem 7.7.3. *$\mathbb{C}_p$ is algebraically closed.*

Before proving this, we prove a few general lemmas. Let K denote a field of characteristic 0 complete with respect to a non-archimedean absolute value. For instance, K could be $\mathbb{Q}_p$, any finite extension of $\mathbb{Q}_p$, or $\mathbb{C}_p$.

Lemma 7.7.4. *For all $x \in \overline{K}$ and $\sigma \in \mathrm{Gal}(\overline{K}/K)$, we have $|\sigma(x)| = |x|$.*

Proof. If p_x is the minimal polynomial of x over K then

$$|x| = |N_{K(\alpha)/K}(x)|_p^{1/\deg p_x} = |p_x(0)|_p = |N_{K(\alpha)/K}(\sigma(x))|_p^{1/\deg p_x} = |\sigma(x)|.$$

□

Lemma 7.7.5 ("Krasner's Lemma"). *If $\alpha, \beta \in \overline{K}$ are such that $|\beta - \alpha| < |\sigma(\alpha) - \alpha|$ for all $\sigma \in G_K$ such that $\sigma(\alpha) \neq \alpha$, then $K(\alpha) \subset K(\beta)$.*

Proof. Suppose $\alpha \notin K(\beta)$. Then $K(\alpha, \beta)/K(\beta)$ is a non-trivial extension, so there exists some non-trivial $\sigma \in \mathrm{Gal}(\overline{K}/K(\beta))$ such that $\sigma(\alpha) \neq \alpha$ (just lift some non-trivial automorphism in $\mathrm{Aut}_{K(\beta)}(K(\alpha, \beta))$). Then by Lemma 7.7.4

$$|\beta - \alpha| = |\sigma(\beta - \alpha)| = |\sigma(\beta) - \sigma(\alpha)| = |\beta - \sigma(\alpha)| = \max(|\beta - \alpha|, |\alpha - \sigma(\alpha)|)$$

where equality follows from the fact that by assumption $|\beta - \alpha| < |\sigma(\alpha) - \alpha|$. But the above line says that $|\beta - \alpha| \geq |\alpha - \sigma(\alpha)|$, a contradiction. □

In other words, if an automorphism of $\overline{K}$ fixes an element in a small enough neighborhood around α then it must also fix α.

In fact we can upgrade this slightly into a statement about polynomials which are sufficiently close. What do we mean by close? Suppose we restrict our attention to polynomials over K of degree $\leq n$; these form an $n + 1$-dimensional K-vector space, so there is an obvious norm on this vector space.

Proposition 7.7.6. *If f is a monic irreducible polynomial of degree n and g is another monic polynomial of degree n such that $|f - g|$ is sufficiently small, then g is also irreducible. Furthermore, if $\alpha_1, \ldots, \alpha_n$ are the roots of f and $\beta_1, \ldots, \beta_n$ are the roots of g then up to reordering,*

$$K(\alpha_i) = K(\beta_i).$$

Proof. Well, just pick $\gamma < |\alpha_i - \alpha_j|$ for all i, j, and define "sufficiently small" to mean that $|\alpha_i - \beta_i| < \gamma$: since the roots of a polynomial vary continuously with respect to its coefficients, this translates to a smallness condition on the coefficients. But then by assumption we have

$$|\alpha_i - \beta_j| < |\alpha_i - \alpha_j|$$

for all j, so by Krasner's lemma we have $K(\alpha_i) \subset K(\beta_i)$. But on the other hand

$$[K(\beta_i) : K] \leq \deg g = n = \deg f = [K(\alpha_i) : K]$$

so in fact $K(\alpha_i) = K(\beta_i)$, which further implies that g is irreducible. □

In other words, two polynomials which are sufficiently close have the same splitting field.

Now we return attention to $K = \mathbb{C}_p$.

Corollary 7.7.7. *$\mathbb{C}_p$ is algebraically closed.*

Proof. If α is algebraic over $\mathbb{C}_p$ with minimal polynomial $p_\alpha \in \mathbb{C}_p[x]$ then by construction we can pick $f(x) \in \overline{\mathbb{Q}}_p[x]$ such that $|p_\alpha - f|$ is sufficiently small so that Proposition 7.7.6 applies with $K = \mathbb{C}_p$. But then $\mathbb{C}_p(\alpha) = \mathbb{C}_p(\beta)$ for β a root of f. But $\beta \in \overline{\mathbb{Q}}_p$, so we're done. □

As another application, we now show that any finite extension of $\mathbb{Q}_p$ can be obtained by completing some number field.

Proof. If $K/\mathbb{Q}_p$ is a finite extension, let $K = \mathbb{Q}_p(\alpha)$ with minimal polynomial α. Since $\mathbb{Q}$ is dense in $\mathbb{Q}_p$, choose some $f \in \mathbb{Q}[x]$ and β a root of f such that $\mathbb{Q}_p(\alpha) = \mathbb{Q}_p(\beta)$. Note $\beta \in \overline{\mathbb{Q}}$, so consider the number field $F = \mathbb{Q}(\beta)$. The norm on $K = \mathbb{Q}_p(\alpha) = \mathbb{Q}_p(\beta)$ restricts to a non-trivial norm on F. Furthermore, we have $F \subset \widehat{F} \subset K$. But since F is dense in K, it follows that $\widehat{F} = K$. □

8. Class field theory

Up to this point we've studied the general theory of finite (algebraic) extensions of p-adic local fields and number fields. An obvious question to then ask is:

what are all of these extensions?

Or, said differently in the context of number fields,

describe every algebraic number.

(1) In the case of local fields, we gave a partial description of how to do this. If $K/\mathbb{Q}_p$ is a finite extension, we constructed a tower of infinite extensions
$$K \subset K^{\mathrm{unr}} = \bigcup_n K(\zeta_{p^n-1}) \subset K^{\mathrm{tame}} = \bigcup_{(m,p)=1} K^{\mathrm{unr}}(\pi_K^{1/m}) \subset \overline{K}.$$
The only part we couldn't give an explicit description of was the last extension, whose Galois group is a pro-p group called the *wild inertia group.*

(2) In the case of number fields, things are much more complicated than for local fields; this is partly because there are infinitely many primes in a number field, whereas there is only *one* in a local field. Said differently, the ring theory of a general Dedekind domain is much more complicated than that of a DVR.

In general, giving a clean and explicit description of every algebraic extension is extremely hard and completely wide open in general, probably infeasible in any reasonable sense.

On the other hand, we can simplify the problem a bit by considering only *abelian* extensions.

Definition 8.0.1. A finite Galois extension E/F is *abelian* if $\mathrm{Gal}(E/F)$ is an abelian group.

Exercise 8.0.2. Show that if E/F and H/F are two abelian extensions then the composite EH/F is Galois and abelian.

In particular, by taking the compositum of all abelian extensions of a field F inside $\overline{F}$, we obtain F^{ab}, the *maximal abelian extension of* F. Letting $G_K := \mathrm{Gal}(\overline{F}/F)$, it then follows from the formalism of infinite Galois theory that
$$\mathrm{Gal}(F^{\mathrm{ab}}/F) \cong G_F/\overline{[G_F, G_F]},$$
where the bar denotes topological closure for the profinite topology.

Theorem 8.0.3 (Kronecker–Weber)**.** *Every abelian extension of* $\mathbb{Q}$ *is a subfield of a cyclotomic field. In other words,*
$$\mathbb{Q}^{\mathrm{ab}} = \bigcup_{n>0} \mathbb{Q}(\zeta_n).$$

Since this is one of the possible final paper topics, I will not present the proof here.

Important note: there is, in general, no generalization of the Kronecker–Weber theorem to arbitrary $F/\mathbb{Q}$! In other words, we don't have a general recipe for constructing the maximal abelian extension of a number field. An old result, which is part of the theory of complex multiplication:

Theorem 8.0.4. *Suppose* F *is an imaginary quadratic field and* $E/\mathbb{Q}$ *is an elliptic curve whose endomorphism ring is* $\mathrm{End}(E) \cong \mathcal{O}_F$*. Then*
$$F^{\mathrm{ab}} = F(j(E)) \cup \bigcup_{n\geq 1} F(w(E[n]))$$
where $E[n]$ *denotes the* n*-torsion points of* E *in* $\overline{Q}$*.*

There is also a similar description of F^{ab} for F a totally real field due to recent work of Dasgupta–Kakde, which has a much different flavor and involves p-adic integration.

The significance of the $\mathbb{Q}(\zeta_n)$ is the fact that they are *ray class fields* for $\mathbb{Q}$. To form a ray class field for $\mathbb{Q}$, simply pick a positive integer n. Then the ray class field for n is[3] the largest extension of $\mathbb{Q}$ unramified away from n and with a ramification condition at $p \mid n$ which depends on the exponent of p in n; this ray class field ends up being $\mathbb{Q}(\zeta_n)$.

If $F/\mathbb{Q}$ is a general number field, then instead of picking $n > 0$, one picks[4] an ideal $\mathfrak{m} \subset \mathcal{O}_F$; they ray class field is then the largest abelian extension unramified at primes away from $\mathfrak{m}$ and with certain prescribed ramification conditions at primes dividing $\mathfrak{m}$, depending on the exponent. It is a general result of class field theory that F^{ab} is the union of the ray class fields for F. Describing them is a harder task.

Example 8.0.5. The first nontrivial example of a ray class field is the one corresponding to the trivial ideal 1. This gives the maximal abelian unramified extension of F, called the *Hilbert class field*. For instance, if $F = \mathbb{Q}$, then this ends up being $\mathbb{Q}$ itself! For F imaginary quadratic and E an elliptic curve over $\mathbb{Q}$ with complex multiplication by $\mathcal{O}_F$, the Hilbert class field is $F(j(E))$. The Hilbert class field H/F is always a finite extension and a consequence of class field theory tells us that

$$\mathrm{Cl}(F) \xrightarrow{\sim} \mathrm{Gal}(H/F).$$

In fact this map is exactly the one induced by the Artin symbol defined earlier in Definition 5.4.5.

More generally, the Artin symbol induces isomorphisms

$$\mathrm{Cl}^{\mathfrak{m}}(F) \xrightarrow{\sim} \mathrm{Gal}(F(\mathfrak{m})/F)$$

where the $\mathrm{Cl}^{\mathfrak{m}}(F)$ are the so-called *ray class groups*, which are again finite groups.

All of this suggests an intimate relationship between the structure of (fractional) ideals in a number field, and the abelian Galois extensions. This is exactly what class field theory aims to systematize.

In fact, for global fields this is done by defining something called the *idèle class group*, which knows about all of the ray class groups at once.

8.1. **Local class field theory.** Thus far we've said a few words about class field theory for number fields, specifically mentioning the Hilbert class fields and ray class fields, more generally.

But for local fields, one can ask the same question; how do you classify the finite abelian extensions of a local field?

For $\mathbb{Q}_p$ the Kronecker–Weber theorem still holds.

Theorem 8.1.1. *Every finite abelian extension of K is contained in $\mathbb{Q}_p(\zeta_n)$ for some n.*

The proof, which we will not include, reduces to treating the prime power degrees of $K/\mathbb{Q}_p$, and then using explicit case-by-case arguments. More generally, one can use Lubin–Tate theory to do explicit local class field theory; this will be covered next semester.

Now, much like in the case of number fields, we want to be able to describe $\mathrm{Gal}(\overline{K}/K)$ in terms of data that is more intrinsic to the field. For number fields this is done by comparing with ray class groups, but in the local case it is even simpler.

Theorem 8.1.2. *For $K/\mathbb{Q}_p$ a finite extension, there is a unique map $\mathrm{rec}_K : K^\times \to G_K^{\mathrm{ab}}$ such that*

- *if $\pi_K \in K^\times$ is a uniformizer and L/K is finite unramified, then $\mathrm{rec}_K(\pi_K)|_L$ acts on L as the Frobenius automorphism.*

[3] strictly speaking this is for $n \cdot \infty$, but ignore this subtlety for now.

[4] again, one also picks a subset of the real places, but ignore this for now

- *if L/K is finite abelian, then letting* $\mathrm{rec}_{L/K}$ *denote the composite* $K^\times \xrightarrow{\mathrm{rec}_K} G_K^{\mathrm{ab}} \twoheadrightarrow \mathrm{Gal}(L/K)$*, we have that* $\ker \mathrm{rec}_{L/K} = N_{L/K}K^\times$ *and induces*

$$K^\times / N_{L/K}L^\times \xrightarrow{\sim} \mathrm{Gal}(L/K).$$

Moreover, this induces an isomorphism

$$\widehat{K^\times} \xrightarrow{\sim} \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

The proof goes by constructing isomorphisms for finite extensions and then gluing them together. For the finite extensions, we will see next semester that one reinterprets the isomorphism as a cup product in Galois cohomology.

What can we say about the reciprocity map? Note that $K^\times$ has a natural filtration by subgroups of the unit group:

$$K^\times \supset \mathcal{O}_K^\times \supset 1 + \mathfrak{m}_K \supset 1 + \mathfrak{m}_K^2 \supset \cdots$$

So a natural question to ask is which subgroups of the Galois group does this correspond to? The answer can be described in terms of something called the "ramification filtration" on $G = G_K^{\mathrm{ab}}$. For instance $G_{-1} = G$, G_0 is the inertia group, and the next groups in the filtration generalize the inertia subgroup; this will be explained in more detail next semester.

9. Analytic class number formula

For the last part of the class we're going to switch gears a bit and do something a bit more analytic. First, let's discuss the Riemann zeta function.

Definition 9.0.1. Let

$$\zeta_{\mathbb{Q}}(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

where $s \in \mathbb{C}$ is a complex number.

This function is of incredible importance in number theory. Some properties:

(1) The usual p-series convergence arguments imply that $\zeta_{\mathbb{Q}}(s)$ converges for $\mathrm{Re}(s) > 1$.

(2) On the other hand, it admits an *integral representation*

$$\zeta_{\mathbb{Q}}(s) = \frac{1}{\Gamma(s)} \int_0^\infty \frac{x^{s-1}}{e^x - 1} \mathrm{d}x.$$

for $\mathrm{Re}(s) > 1$. Riemann used a similar integral (in fact, a contour integral) to extend $\zeta_{\mathbb{Q}}(s)$ to the entire complex plane, with a simple pole at $s = 1$.

(3) $\zeta_{\mathbb{Q}}(s)$ admits an Euler product

$$\zeta_{\mathbb{Q}}(s) = \prod_p \frac{1}{1 - p^{-s}}$$

obtained by an application of the fundamental theorem of arithmetic and the formula for a geometric series.

(4) $\zeta_{\mathbb{Q}}(s)$ satisfies a functional equation

$$\zeta_{\mathbb{Q}}(s) = 2^s \pi^{s-1} \sin(\pi s/2) \Gamma(1-s) \zeta(1-s)$$

which in particular (along with some properties of the Γ function) implies that $\zeta(s)$ vanishes at $-2, -4, -6, \ldots$. These are called the trivial zeros.

Easy corollary: there are infinitely many prime numbers.

If you are an an analytic number theorist, then this function has an extremely interesting link to the distribution of prime numbers; specifically the Riemann hypothesis predicts that the non-trivial zeros of this function lie on the line $\mathrm{Re}(s) = 1/2$, and that these zeros can be used to reconstruct (a slightly modified verison of) the prime counting function.

This sort of interplay between algebra, number theory and analysis has been vastly generalized to the theory of *L-functions*. If you want to learn more about this theory and more modern perspectives, talk to Yiannis.

So why would an algebraic number theorist care? Well, we put $\mathbb{Q}$ in the notation for a reason. Notably, there is a natural generalization to an arbitrary number field.

Definition 9.0.2. If F is a number field, then its *Dedekind ζ-function* is

$$\zeta_F(s) = \sum_{0 \subsetneq I \subset \mathcal{O}_F} \frac{1}{N(I)^s} = \prod_{\mathfrak{p} \subset \mathcal{O}_F} \frac{1}{1 - N(\mathfrak{p})^{-s}}$$

The second equality follows from unique factorization in Dedekind domains and the formula for geometric series. Hecke proved that $\zeta_F(s)$ also admits a meromorphic continuation to all of $\mathbb{C}$, again with a unique pole at $s = 1$ of order 1.

9.1. **Special values.** The Riemann zeta function displays some very remarkable special values. For instance

$$\zeta(2) = \pi^2/6.$$

The reciprocal can be interpreted as the probability that two randomly chosen integers are coprime. Apéry's constant

$$\zeta(3) \cong$$

shows up in quantum physics and thermodynamics. Don't ask me how. The value

$$\zeta(-1) = -\frac{1}{12}(= 1 + 2 + 3 + \cdots)$$

apparently shows up in string theory.

$$\zeta(2n) = \frac{(-1)^{n+1} B_{2n} (2\pi)^{2n}}{2(2n)!}$$

where B_{2n} is the $2n$th Bernoulli number and

$$\zeta(-n) = (-1)^n \frac{B_{n+1}}{n+1}$$

Remark 9.1.1. These identities may look random and slightly bewildering, and one of the goals of modern mathematics is to take identities of this form and restate them in more intuitive ways. Doing this, however, requires diving deep into some of the most elaborate and intricate mathematical subjects.

Now let's state the result we want to investigate.

Theorem 9.1.2 (Analytic class number formula)**.**

$$\lim_{z \to 1^+} (z-1)\zeta_F(s) = \frac{2^r (2\pi)^s h_F R_F}{w_F \sqrt{|D_F|}}$$

where

- *r is the number of real places of F*
- *s is the number of complex conjugate pairs of complex places of F*
- $h_F = |\,\mathrm{Cl}_F\,|$

- *R_F is the regulator, which roughly measures the size of the free part of $\mathcal{O}_F^\times$*
- *$w_F = |(\mathcal{O}_F^\times)_{\mathrm{tors}}|$ is the number of roots of unity in F*
- *D_F is the discriminant of $F/\mathbb{Q}$.*

This is a truly stunning formula: it shows that a very simple-to-define analytic function actually combines all of the most important arithmetic invariants of the field! Let's define the regulator in order to prove it for $F = \mathbb{Q}$.

Definition 9.1.3. Consider the map

$$\begin{aligned} F_{\mathbb{R}}^\times &\to \mathbb{R}^{r+s} \\ (x_v)_v &\mapsto (\log \|x_v\|_v)_v \end{aligned}$$

Remark 9.1.4. In the above definition we are viewing $F_{\mathbb{R}} = \mathbb{R}^r \times \mathbb{C}^s$, which is why the target of the map is $\mathbb{R}^{r+s}$ rather than $\mathbb{R}^{r+2s}$. In particular, we index x_v by the real embeddings and pairs of complex conjugate embeddings.

One can show that $\mathcal{O}_F^\times \to F_{\mathbb{R}}^\times \to \mathbb{R}^{r+s}$ lands in the hyperplane $\{(c_v) : \sum_v c_v = 0\}$. Moreover, Dirichlet's unit theorem says that the rank of $\mathcal{O}_F^\times$ is $r+s-1$, and one can show that its image is a full lattice under the logarithm.

Definition 9.1.5. The *regulator* is the covolume of the image of $\mathcal{O}_F^\times$.

Example 9.1.6. So now take $F = \mathbb{Q}$. Then the right side becomes

$$\frac{2^1 \cdot (2\pi)^0 \cdot 1 \cdot 1}{2 \cdot 1} = 1$$

The left hand side can be computed completely analytically, and is also equal to 1; the trick is to show that

$$\zeta_{\mathbb{Q}}(s) = \frac{1}{s-1} + \phi(s)$$

where $\phi(s)$ is holomorphic at 1.

9.2. **Imaginary quadratic case.** Now let's consider an imaginary quadratic field $F = \mathbb{Q}(\sqrt{D})/\mathbb{Q}$. For simplicity we will assume that $D \equiv 2, 3 \mod 4$ so that $\mathcal{O}_F = \mathbb{Z}[\sqrt{D}]$.

In this case $r = 0$ and $s = 1$. This means that the regulator is the covolume of a lattice in $\mathbb{R}^{r+s-1} = \mathbb{R}^0$, so $R_F = 1$ again. Moreover, the discriminant $D_F = 4D$ so the formula becomes

$$\lim_{z \to 1^+} (z-1)\zeta_F(s) = \frac{\pi h_F}{w_F \sqrt{|D|}}$$

We can slightly simplify the left hand side by noting that $\zeta_F(s)$ can be expressed using $\zeta_{\mathbb{Q}}(s)$ and a *Dirichlet L-function* associated with a character that cuts out the field F.

Definition 9.2.1. If $\chi : (\mathbb{Z}/N)^\times \to \mathbb{C}^\times$ is a Dirichlet character, then we define

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p \frac{1}{1 - \chi(p)p^{-s}}$$

Definition 9.2.2. Let χ_F denote the Dirichlet character of order $4D$ which is defined on prime numbers $p \in \mathbb{Z}$ by

$$\chi_F(p) = \left(\frac{4D}{p}\right)$$

and extended multiplicatively to all integers. In particular χ_F descends to a character $\chi_F : (\mathbb{Z}/4D\mathbb{Z})^\times \to \mathbb{C}^\times$. This is called the *quadratic character associated to F*.

Remark 9.2.3. One can show that $F \subset \mathbb{Q}(\zeta_{4D})$, and moreover that χ_F can be computed as

$$\chi_F : (\mathbb{Z}/4D)^\times \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\zeta_{4D})/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(K/\mathbb{Q}) \xrightarrow{\sim} \{\pm 1\}\,.$$

One can compute this directly, but it also falls out more easily as a consequence of class field theory.

Proposition 9.2.4. *There is a decomposition*

$$\zeta_F(s) = \zeta_{\mathbb{Q}}(s) L(\chi_F, s).$$

Proof. It suffices to show that

$$\prod_{\mathfrak{p} | p\mathcal{O}_F} 1 - N(\mathfrak{p})^{-s} = (1 - p^{-s})(1 - \chi_F(p)p^{-s}).$$

We split into cases:

- If $\chi_F(p) = 1$, then the right hand side is $(1 - p^{-s})^2$. Also $4D$ is a square mod p so D is a square mod p, so $p\mathcal{O}_F$ splits into two primes, each of norm p, so the left hand side is the same.
- If $\chi_F(p) = -1$ then the right hand side is $(1 - p^{-2s})$. Also D is not a square mod p, so $p\mathcal{O}_F$ is inert and thus has norm p^2.
- If $\chi_F(p) = 0$ then the right side is $(1 - p^{-s})$. Also $p\mathcal{O}_F = \mathfrak{p}^2$, and the norm of $\mathfrak{p}$ is still p.

□

So the formula simplifies to

$$L(\chi_F, s) = \frac{\pi h_F}{w_F \sqrt{|D|}}$$

I won't actually prove this now; the proof can be reduced to estimating the number of lattice points in a disk, which is an analytic number theory question.

Let's see some consequences, though. By much more elementary methods, one can show:

Proposition 9.2.5.

$$L(\chi_F, 1) = -\frac{\pi}{8|D|^{3/2}} \sum_{r=1}^{4|D|-1} \chi_F(r) r$$

But this is a completely explicit formula! The only complicated thing is this formula is $\chi_F(r)$, but you can program a computer to compute this pretty easily.

Exercise 9.2.6. Use this formula to write a computer program which computes the class number of $\mathbb{Q}(\sqrt{D})$ for $D \equiv 2, 3 \mod 4$.

For instance, if $D = -1$ then this becomes

$$\frac{\pi h_F}{4} = L(\chi_F, 1) = -\frac{\pi}{8}(\chi_F(1) + 2\chi_F(2) + 3\chi_F(3)) = -\frac{\pi}{8}(1 - 3)$$

so $h_F = 1$.

References

[BM40] Becker, M. F. and MacLane, S. "The minimum number of generators for inseparable algebraic extensions". In: *Bull. Amer. Math. Soc.* 46 (1940), pp. 182–186. ISSN: 0002-9904. URL: https://doi.org/10.1090/S0002-9904-1940-07169-1 (cit. on p. 7).

[Cla66] Claborn, Luther. "Every abelian group is a class group". In: *Pacific J. Math.* 18 (1966), pp. 219–222. ISSN: 0030-8730. URL: http://projecteuclid.org/euclid.pjm/1102994263 (cit. on p. 19).

[Neu99] Neukirch, Jürgen. *Algebraic number theory.* Vol. 322. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. Springer-Verlag, Berlin, 1999, pp. xviii+571. ISBN: 3-540-65399-6. URL: https://doi.org/10.1007/978-3-662-03983-0 (cit. on pp. 28, 30, 36).

[Sta21] Stasinski, Alexander. "A uniform proof of the finiteness of the class group of a global field". In: *Amer. Math. Monthly* 128.3 (2021), pp. 239–249. ISSN: 0002-9890. URL: https://doi.org/10.1080/00029890.2021.1855036 (cit. on p. 34).