Chapter 1

Some algebraic number theory

In this chapter I will cover some preliminaries on algebraic number theory that will be important in our study of (quaternion) algebras. I expect some familiarity with algebraic number theory (e.g., number fields, rings of integers, ideal class groups), so I won't start from zero, but I will try not to assume too much (e.g., Part I of Stewart and Tall [ST02] or the first 2 chapters of my Number Theory II notes [Marb] should suffice).

We begin by reviewing some module theory, initially for general rings then specializing to some results for modules over commutative rings. The subsequent sections, on number theory proper, cover p-adic fields, valuations, orders in number fields and the language of adeles. (An *order* is a generalization of the ring of integers in a number fields, which we want to understand because the concept of "the ring of integers" doesn't make sense for quaternion algebras, but the notion of order does.) One of our primary goals for the course is to generalize the theory of ideals and orders to quaternion algebras and beyond.

I will not provide thorough treatments of the topics in the chapter, but enough to use the material later in the course. In particular, I will not prove everything, and leave some standard facts for the reader to check, either as exercises, or from other references. Consequently, you may want to consult additional sources for a deeper understanding of these topics.

The theory of modules can be found in most graduate algebra books, though some books restrict to studying modules over commutative rings. However, this should be sufficient for our purposes, as we will prove what we need to know about modules over noncommutative rings (when the ring is an algebra) in later chapters.

One reference for (almost?) all of the number theoretic content in this chapter (though organized in a very different way) is Neukirch's boook [Neu99]. Neukirch is pretty comprehensive, and a standard text, but the organization and the level of generality prevent it from being a good quick reference for the beginner, so I'll point out some other references as well. (Warning: I have not read all of these myself.)

The theory of p-adic fields is covered in many books on algebraic number theory, e.g., Cohen's "encyclopedia" [Coh07] (without proofs), Fröhlich–Taylor [FT93], Janusz [Jan96], Lang [Lan94], and Kato–Kurokawa–Saito (the first volume [KKS00] has a nice treatment of $\mathbb{Q}_p$ with proofs and the second volume [KKS11] has a summary of more general p-adic fields without proofs). There are also a number of books specifically on p-adic numbers or local fields like Serre's classic *Local Fields* [Ser79], though some books restrict the treatment

to just $\mathbb{Q}_p$—e.g., Serre's *Course in Arithmetic* [Ser73] and Katok [Kat07]. There is also a concise algebraic treatment of the basics of p-adic and number fields in Curtis and Reiner's classic text on representation theory [CR06], which also develops the theory of modules. Most of the references below for adeles also treat p-adic fields.

Adeles/ideles tend to be discussed in books which discuss global class field theory (though [Jan96] is an exception). For instance, besides [Neu99] and [Lan94], references for adeles (plus local fields and class field theory) include classics such as Cassels–Frölich [cas67] and Weil's *Basic Number Theory* [Wei95], as well as more modern books like Childress [Chi09], Kato–Kurokawa–Saito's *Number Theory 2* [KKS11] (without proofs) and Ramakrishnan–Valenza [RV99]. Another reference for both p-adic numbers and adeles is [Kna07], which also covers a lot of algebra that is closely related to things we will do in this course (e.g., Wedderburn–Artin theory, the Brauer group).

On the other hand, the theory of ideals in general orders in number fields is not discussed in most number theory books—[Neu99] is the only number theory text that comes to mind which does this (admittedly, it was also the book I learned from so am less familiar with other books), though some books such as [Cox13] study the case of general orders in quadratic fields.

Actually, there is nothing in the theory of orders of number fields (separate from presumed knowledge of rings of integers) that is a logical prerequisite of our study of algebras. Indeed, the theory of orders of algebra includes the theory of orders of number fields as a special case. (Not that we will necessarily prove everything we state in the number field case—e.g., the class number formula. Also, we will mostly focus on orders in central simple algebras which do not quite include general orders in number fields.) The main reason for the exposition of orders in number fields here is to serve as a preview of what theory we want to generalize to noncommutative algebras.

1.1 The birds and bees of modules

The notion of a module is as fundamental in arithmetic as the notion of vector space is in algebra. Indeed, a vector space is a special type of module and the basic idea of a module is to define something like a vector space, but over rings not just fields. Of course modules are also fundamental in general algebra (e.g., in representation theory), but we will primarily use the language of modules to define arithmetic structures, e.g., rings of integers of number fields and their analogues in quaternion algebras.

First we will give definitions and examples of modules over general rings, then summarize some basic theory over commutative rings, which we will assume from here on. Result we need to know about modules over noncommutative rings will be treated as we need them in later chapters.

1.1.1 Modules over arbitrary rings

Here R denotes a ring, not necessarily commutative, with identity 1, and F will denote a field.

A **(left) R-module** (or **module over** R) is an additive abelian group M with a left R-action $r : M \to M$ for each $r \in R$, denoted ra or $r \cdot a$, satisfying (i) $r(a + b) = ra + rb$,

(ii) $(r+s)a = ra + sa$, (iii) $r(sa) = (rs)a$, and (iv) $1 \cdot a = a$, for all $a, b \in M$ and $r, s \in R$.

One defines right R-modules similarly. If R is commutative, then we can view a left R-module M as a right R-module by defining $ar = ra$. Note if R is not commutative, this does not work in general as then we would have $(rs)a = a(rs) = (ar)s = (ra)s = s(ra)$.

Unless stated otherwise, we will always assume our modules are left modules.

Example 1.1.1. Any abelian group A is a $\mathbb{Z}$-module, where the action of $\mathbb{Z}$ is given by $(-1)a = -a$ and $n \cdot a = (a + a + \cdots + a)$ (n times) for $n \in \mathbb{N}$, $a \in A$.

Example 1.1.2. The trivial group $M = \{0\}$ is an R-module for any ring R, called the zero module or the trivial module.

Example 1.1.3. Let V be a vector space over a field F. Then V is an F-module. In fact, the module axioms are precisely the vector space axioms, so any F-module is a vector space.

Consequently, one often thinks of modules as "vector spaces over rings" and we call the multiplication by R *scalar multiplication*. Though much weirder things can happen, e.g., R may be nonabelian or the action may have *torsion*, i.e., we may have $rm = 0$ for some nonzero $r \in R$ and nonzero $m \in M$. This already happens for $\mathbb{Z}$-modules, e.g., $2 \cdot 2 = 0$ in $M = \mathbb{Z}/4\mathbb{Z}$.

The following type of example is the primary kind we are interested in in this course.

Example 1.1.4. Let A be a ring and R be a subring. Then A is an R-module where the scalar multiplication is just the ring multiplication. Similarly, right multiplication makes A a right R-module. The left and right module actions are the same if and only if every element of R commutes with every element of A, i.e., R lies in the **center** $Z(A) = \{z \in A : az = za \text{ for all } a \in A\}$ of A. For instance, if R is commutative, then R lies in the center of the matrix ring $M_n(R)$ (identifying r with the diagonal matrix rI, where I is the identity matrix).

In particular, R is both a left and right module over itself, and if R is commutative the left and right module actions are the same.

Some texts use notation like ${}_RR$ or R_R to mean R as regarded as left or right module over itself (and similarly with ${}_RA$ and A_R). I personally find this notation cluttered, and will just say in words when we are thinking of of a ring (or later algebra) as a module. However, I won't think less of you if you find this notation helpful to keep things straight.

Regarding R as an R-module gives other examples of modules with torsion, e.g., $\mathbb{Z}/6\mathbb{Z}$ regarded as a module over itself.

A fundamental way of constructing modules, as with vector spaces, is the direct sum: if M and N are two R-modules, their **direct sum**

$$M \oplus N = \{(m, n) : m \in M, n \in N\}$$

is an R-module. Here the addition on $M \oplus N$ is component-wise (so this is the direct product of abelian groups), and R acts diagonally (or by scalars) on the components, i.e., $r(m,n) = (rm, rn)$.

More generally, if I is an ordered index set an M_i is an R-module for each $i \in I$, then we define the **direct sum** $\bigoplus_{i\in I} M_i$ to be the R-module obtained letting R act diagonally on the cartesian product of abelian groups $\prod_{i\in I} M_i$. (We assumed I was ordered just so that $\prod_{i\in I} M_i$ is uniquely defined, and not just defined up to isomorphism.)

Now we want to generalize some other basic notions about vector spaces to modules. Below, M and N denote R-modules.

If $N \subset M$, we say N is an **(R-)submodule** of M if N is a subgroup of M and $RN \subset N$. It's immediate that an R-submodule of a module is also an R-module. In particular, if $R \subset B \subset A$ are rings, then B is an R-submodule of the R-module A.

Suppose we have a map $\phi : M \to N$. We say ϕ is an **R-module homomorphism** if it is a homomorphism of abelian groups that preserves the R-action, i.e., an abelian group homomorphism such that $\phi(r \cdot m) = r \cdot \phi(m)$ for $r \in R$ and $m \in M$. If ϕ is also bijective, i.e., an isomorphism of abelian groups, then we say it is an **R-module isomorphism**, and write $M \simeq N$ or $M \simeq_R N$ to mean M and N are isomorphic as R-modules. (Check the inverse ϕ^{-1}, a priori just an abelian group homomorphism, is also an R-module homomorphism.) In analogy with vector spaces, we sometimes call R-module homomorphisms **R-linear** maps. In particular, any linear map $\phi : V \to W$ of F-vector spaces (F a field) is an F-module homomorphism.

If $\phi : M \to N$ is an R-module homomorphism, one defines the kernel $\ker \phi$ and image $\operatorname{im} \phi$ in the usual way (the kernel and image as abelian group homomorphisms). Then $\ker \phi$ is a submodule of M and $\operatorname{im} \phi$ is a submodule of N.

If N is a submodule of M, one can descent the action of R to the quotient group M/N, which we may view as a module called the **quotient module**.

Exercise 1.1.1. If $\phi : M \to Q$ is a surjective R-module homomorphism, show Q is isomorphic to the quotient module $M/\ker \phi$.

Exercise 1.1.2. Let $M_1, \dots M_n$ be R-modules.
(a) Show $M_i \oplus M_j \simeq M_j \oplus M_i$, as R-modules.
(b) Let $N_1 = M_1$ and $N_i = N_{i-1} \oplus M_i$ for $2 \le i \le n$. Show $N_n \simeq \bigoplus_{i=1}^n M_i$.

The latter exercise says that, up to isomorphism, finite direct sums are commutative and associative and there is no difference between defining a direct sum inductively or as we did directly with an n-fold cartesian product.

Any finite-dimensional vector space V over F is isomorphic to $F^n = \oplus_{i=1}^n F$ for some n. So the most similar kind of modules to finite-dimensional vector spaces are the following:

For any $n \in \mathbb{N}$, $R^n = \bigoplus_{i=1}^n R$ is an R-module, called the **free module of rank** n. More generally, if $M \simeq R^n$ (as R-modules), we say M is a free module of rank n.[1]

[1] You probably think the rank is obviously an invariant of a free module M. Insanely, it's not! So it can

If M is a free module of rank n, n is the obvious analogue of dimension for vector spaces. However, due to issues of torsion, the notion of dimension is more murky for modules which are not free. For instance $\mathbb{Z}/2\mathbb{Z}$ is a $\mathbb{Z}$-module, but should it have dimension 0 or 1? Even if we make a choice here, things will get hairier for more complicated rings: e.g., $\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}$ can be viewed as $R = \mathbb{Z} \oplus \mathbb{Z}$-modules (work out an action!), so for the notions dimension over $\mathbb{Z}$ and dimensions over R to be compatible, you might want $\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z}$ to have dimension $\frac{1}{2}$ or 0 over R. Thus module theory gets more delicate here than the case of vector spaces, and there are different notions of dimension one can consider (e.g., Krull dimension, projective dimension, injective dimension, flat dimension).

At present, we will content ourselves with coarser notions of dimensions for non-free modules.

Exercise 1.1.3. Let $X = \{m_1, \dots m_n\} \subset M$, an R-module. Check that

$$R\langle m_1, \dots, m_n \rangle := Rm_1 + \cdots + Rm_n = \{r_1 m_1 + \cdots + r_n m_n : r_i \in R\}$$

is a submodule, called the submodule generated by X.[2]

We say M is **finitely generated** if there is a finite set $\{m_1, \dots m_n\}$ such that $M = R\langle m_1, \dots m_n \rangle$. This is the analogue what it means for a vector space to be finite dimensional. Recall that all minimal generating sets of a vector space have the same size, but this is not true for modules: e.g., $\{1\}$, $\{2, 3\}$ and $\{6, 10, 15\}$ are all minimal generating sets for $\mathbb{Z}$ as a $\mathbb{Z}$-module. If $M = Rm$ is generated by a single element m, then we say M is **cyclic**. For instance, any cyclic abelian group is a cyclic $\mathbb{Z}$-module.

For the rest of this section, we assume our modules are finitely generated.

With this assumption, if $R = F$, any module M is just a finite-dimensional vector space.

Now we can try to decompose modules into direct sums $M_1 \oplus M_2 \oplus \cdots \oplus M_n$, where each M_i is "irreducible." A couple of ideas for how to define irreducible might be to ask that it is not (isomorphic to) the direct sum of two proper modules, or to just ask that it has no proper submodules. It turns out that these are different notions in general, and using the latter gives more basic objects and it suitable for many purposes, including ours. (The former notion is called *indecomposable*.) Note both of these notions, as well that of cyclicity, are different analogues of being one dimensional (and these notions do not determine modules up to isomorphism, or even distinguish between finite and infinite cardinality in the basic case of $\mathbb{Z}$-modules).[3]

We say M is **simple** (or **irreducible**) if it has no nonzero proper submodules. For instance, if $R = F$ then the simple submodules of any finite dimensional F-vector space

happen that M is a free R-module of rank 2, but also one of rank 77. (Many people would not even use the word rank in this case.) See Remark 1.1.4. Fortunately, this does not happen if we work with reasonable rings R, such as any commutative ring or the algebras we will work with.

[2] My notation $R\langle m_1, \dots, m_n \rangle$ is not standard, though the $Rm_1 + \cdots + Rm_n$ notation is fairly so.

[3] Dimension is a very subtle concept in mathematics. For instance, Manin's article *The notion of dimension in geometry and algebra* (Bull. AMS) gives arguments for thinking of the dimension of the set of primes, Spec $\mathbb{Z}$, as being 1, 3, and ∞.

$V = M$ are just the 1-dimensional subspaces. If $R = \mathbb{Z}$, then M is an abelian group, which is simple if and only if it has no nontrivial proper subgroups, i.e., M is cyclic of prime order. (Since any subgroup of an abelian group is normal, this coincides with the definition of simple for abelian groups.)

We say M is **semisimple** if it is a direct sum of (a necessarily finite number of) simple modules. For instance, any finite-dimensional vector space over a field is semisimple. Any abelian group of squarefree order is semisimple as a $\mathbb{Z}$-module, as they break up as direct products (as groups) of cyclic pieces of prime order. Note that other finite abelian groups give us an easy source of non-semisimple modules.

> **Example 1.1.5.** The cyclic group (which is also cyclic as a module) $\mathbb{Z}/4\mathbb{Z}$ is not semisimple as a $\mathbb{Z}$-module. To see this, note that it contains $2\mathbb{Z}/4\mathbb{Z}$ as a unique nonzero proper submodule. Thus it is neither simple nor a direct sum of proper submodules, whence not semisimple. (It is however indecomposable.)

So we cannot always decompose a module into a direct sum of simple modules. Even when we cannot, we can still study non-simple modules by looking at exact sequences like

$$0 \to N \to M \to M/N \to 0$$

where N is simple and/or M/N is simple, and using homological algebra. However most of the modules we are interested in this course will be semisimple (which are more analogous to finite-dimensional vector spaces than arbitrary modules), and thus it typically suffices to understand the simple modules.

We will describe the simple modules of a ring in Section 2.3—they are just modules isomorphic to the ring modulo a maximal ideal (Lemma 2.2.2, though technically it is only stated in the context of algebras).

1.1.2 Modules over commutative rings

Here we recall without proof some basic results about modules over commutative rings. Throughout this section, R denotes a commutative ring and M a finitely-generated R-module.

First, a general structure result. While we cannot always decompose modules into simple modules as the example of $\mathbb{Z}/4\mathbb{Z}$ (Example 1.1.5) shows, we have a nice decomposition theorem when R is a PID.

Theorem 1.1.1. *Any module M over a PID R is a direct sum of cyclic modules:*

$$M = Rm_1 + \cdots + Rm_n$$

for some $\{m_1, \ldots, m_n\} \in M$. Furthermore, each cyclic module is of the form $R/\mathcal{I}_i$ for some (possibly zero) ideal $\mathcal{I}_i$. We may assume $\mathcal{I}_1 \supset \cdots \supset \mathcal{I}_n$, and such a decomposition is unique.

(I used $+$ instead of $\oplus$ because M is actually equal to the "internal direct sum," whereas only isomorphic to the "external" direct sum (direct sum as we defined above).)

Using this, one can show

Corollary 1.1.2. *If M is torsion free over a PID R (i.e., $rm = 0$ for $r \in R$, $m \in M$ implies $r = 0$ or $m = 0$), then M is a free module of finite rank.*

We say $\{e_1, \dots, e_n\}$ is an **(R-)basis** for M if $M = R\langle e_1, \dots, e_n \rangle$ and $e_1, \dots, e_n$ are linearly independent over R, i.e.,

$$r_1 e_1 + \cdots + r_n e_n = 0 \implies r_1 = \cdots = r_n = 0 \quad \text{for} \quad r_1, \dots, r_n \in R.$$

Note being a basis is a stronger condition than being a minimal generating set, e.g., $\{2, 3\}$ is a minimal generating set for $\mathbb{Z}$ over itself, but not a basis.

Proposition 1.1.3. *If M has a basis $\{e_1, \dots, e_n\}$, then any other basis has the same number of elements. Moreover, M is a free module of rank n, i.e., $M \simeq R^n$.*

Remark 1.1.4. When R is not commutative, it need not be the case that the rank is a well-defined invariant of free modules—it may happen that $R^m \simeq R^n$ for $m \neq n$. These rings are said to not have *invariant basis number* (IBN). The above proposition says commutative rings have IBN. "Reasonable" noncommutative rings do as well, such as noetherian and artinian rings, which include our rings of primary interest. Examples of (noncommutative) rings without IBN can be constructed using infinite-dimensional matrices. There have also been some interesting somewhat recent constructions of rings without IBN using Leavitt path algebras, which are certain algebras associated to graphs.

Proposition 1.1.5. *Let M be a free $\mathbb{Z}$-module, i.e., a torsion-free abelian group. If N is a submodule of M, then N is also a free $\mathbb{Z}$-module, and the rank of N is at most the rank of M.*

This is also true for non-finitely-generated modules over PIDs, but over general commutative rings it is not even true for finitely-generated modules.

Note that M and N (as above) can have the same rank even if $M \neq N$, e.g., $M = \mathbb{Z}$ and $N = 2\mathbb{Z}$. However, we can give the following characterization of M and N having the same rank.

Proposition 1.1.6. *Let M and N be free $\mathbb{Z}$-modules of ranks m and n, with N a submodule of M. Then $[M : N] < \infty$ if and only if $m = n$.*

One important construction of modules that we will use is *tensor products*. One way to motivate them is via bilinear maps. Let M, N be R-modules and $\phi : M \times N \to R$ an R-bilinear map. This means

$$\begin{aligned} \phi(m_1 + m_2, n) &= \phi(m_1, n) + \phi(m_2, n), \\ \phi(m, n_1 + n_2) &= \phi(m, n_1) + \phi(m, n_2), \\ \phi(rm, n) &= \phi(m, rn) = r\phi(m, n), \end{aligned}$$

for $m, m_1, m_2 \in M$, $n, n_1, n_2 \in N$ and $r \in R$.

Now define the **tensor product** of M and N (over R) to be the space $M \otimes N = M \otimes_R N$. Constructed as follows. Consider the free abelian group $\mathbb{Z}\langle M \times N \rangle$ of formal finite integer

linear combinations of symbols $m \otimes n$, where $(m, n) \in M \times N$. Let $M \otimes N$ be the quotient of $\mathbb{Z}\langle M \times N \rangle$ by the relations

$$\begin{aligned}(m_1 + m_2) \otimes n &= m_1 \otimes n + m_2 \otimes n \\ m \otimes (n_1 + n_2) &= m \otimes n_1 + m \otimes n_2 \\ (rm) \otimes n &= m \otimes (rn).\end{aligned}$$

(Here m, m_1, m_2, etc are as above.) Then $M \otimes N$ is a finitely-generated abelian group which we make into an R-module by

$$r \cdot \sum m_i \otimes n_i = \sum (rm_i) \otimes n_i.$$

By the third relation above, $r(m \otimes n) = (rm) \otimes n = m \otimes (rn)$, so we can just denote such expressions by $rm \otimes n$ without ambiguity.

The tensor product is defined so that any R-linear map $\ell : M \otimes N \to R$ gives a bilinear map ϕ on $M \times N$ via composition:

$$\phi : M \times N \to M \otimes N \xrightarrow{\ell} R.$$

Here the first map is given by $(m, n) \to m \otimes n$ so $\phi(m, n) := \ell(m \otimes n)$. E.g., the first tensor product condition $(m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n$ implies that the first bilinearity condition $(m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n$ is satisfied, and so on. The last bilinearity condition $\phi(m, rn) = r\phi(m, n)$ follows from the R-linearity of ϕ.

Conversely, given any bilinear map $\phi : M \otimes N \to R$, it factors through the tensor product $M \otimes N$ as a linear map, and one can define the tensor product in the category of R-modules by this universal property.[4]

A naive way to compute tensor products is to observe that if $\{m_i\}$ is a generating set for M and $\{n_j\}$ is a generating set for N, then $\{m_i \otimes n_j\}$ generates $M \otimes N$.

You should work out a few examples of tensor products if this is new to you:

Exercise 1.1.4. Let $n \in \mathbb{N}$. Show $\mathbb{Z}^n \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{Q}^n$ but $(\mathbb{Z}/n\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Q} = 0$.

Exercise 1.1.5. Let G and H be finite abelian groups. Describe $G \otimes_{\mathbb{Z}} H$.

Exercise 1.1.6. For an R-module M, show $M \otimes R \simeq R \otimes M \simeq M$. (In the tensor product, we view R as an R-module.)

Tensor products behave nicely:

[4] Chern's joke[5]: tensor products replace bilinear maps by linear maps.

[5] It's better aurally, or orally.

Proposition 1.1.7. *Suppose M_1, M_2 and M_3 are R-modules. Then*

$$M_1 \otimes M_2 \simeq M_2 \otimes M_1,$$
$$(M_1 \otimes M_2) \otimes M_3 \simeq M_1 \otimes (M_2 \otimes M_3),$$
$$(M_1 \oplus M_2) \otimes M_3 \simeq (M_1 \otimes M_3) \oplus (M_2 \otimes M_3).$$

Combining this with the previous exercise, this says isomorphism classes of R-modules form a commutative monoid[6] under tensor product, with identity being R. Since R-modules also form a commutative monoid under direct sum (with identity being the zero module), and we have a distributive property between direct sums and direct product, this means isomorphism classes of R-modules form an algebraic structure like a commutative ring, but without additive inverses. This structure is called a commutative *semiring*.

Note the proposition combined with the Exercise 1.1.4 shows that tensoring a finitely-generated abelian group A (over $\mathbb{Z}$) gives us a $\mathbb{Q}$-vector space, whose dimension is the free rank r of A (i.e., the rank of the free part, i.e., r such that $A \simeq \mathbb{Z}^r \oplus A_{\text{tors}}$, where A_{tors} denotes the finite abelian group consisting of all torsion (finite order) elements).

This observation will be the reason why tensor products are so important for us—given a module of a subring, tensoring up give us modules of the superring:

Proposition 1.1.8. *Let R be a commutative subring of the (not necessarily commutative) ring S, and M a R-module. Then $M \otimes S = M \otimes_R S$ is an S-module, called the* **extension of scalars** *of M by S.*

Note, by exer:tensor-id, the extension of scalars of R by S is just S.

The extension of scalars $M \otimes S$ can be described by a universal property, if you're into that sort of thing, because tensor products can. In particular, M can be embedded into an S-module if and only if the map $m \mapsto (m \otimes 1)$ from M to $M \otimes S$ is injective. Morally, the idea with extension of scalars is that, when this map is injective, $M \otimes S$ should be the "smallest" S-module containing M as an R-submodule. (Note $M \otimes S$ is also an R-module.)

Exercise 1.1.7. Let $R = \mathbb{Z}$, $M = \mathbb{Z}[\sqrt[n]{d}]$ where $d \in \mathbb{Z}$ and $S = \mathbb{Q}$. Show $K := M \otimes \mathbb{Q} \simeq \mathbb{Q}(\sqrt[n]{d})$, which is the smallest number field (in the sense of smallest degree over $\mathbb{Q}$) containing M. (Note M may or may not be the full ring of integers of K.)

Exercise 1.1.8. Let R be a commutative subring of a ring S. Show $R^n \otimes S \simeq S^n$.

In particular, we conclude the following about tensor products of vector spaces. First, if V is an n-dimensional F-vector space, and K a field containing F, then $V \otimes_F K \simeq (F^n) \otimes_F K \simeq K^n$. Similarly, if $V \simeq F^n$ and $W \simeq F^m$ are n- and m-dimensional F-vector spaces, then $V \otimes_F W \simeq W^n \simeq F^{mn}$ is a vector space of dimension mn. (Here, to apply the

[6] Recall a monoid is a set with an associative binary operation and identity. Informally, you can think of this as a group without inverses. If you also leave out the identity, you get a *semigroup*. If you also leave out the associativity, you have a *magma*. If you leave out the binary operation, you have a *set*. If you leave out the set, you have *nirvana*.

exercise, we regard $W \simeq \oplus_{i=1}^m F$ as a ring with $+$ and $\cdot$ defined component-wise, and $F \subset W$ a subring via diagonal embedding.) Thus the direct sum of vector spaces adds dimensions and tensor product multiplies dimensions.

The last exercise also immediately yields:

Corollary 1.1.9. *Let R be a commutative subring of a ring S. If M is a free R-module of rank n, then $M \otimes_R S$ is a free S-module of rank n. In particular, if K/F is an extension of fields and V is an n-dimensional F-vector space, then $V \otimes_F K$ is an n-dimensional K-vector space.*

We remark one can define tensor products over noncommutative rings as well, with minor additional technicalities. However, tensor products over commutative rings will suffice for our purposes.

1.2 p-adic fields

1.2.1 The fields $\mathbb{Q}_p$

Let p be a prime. The set of **p-adic integers** $\mathbb{Z}_p$ is the inverse (or projective) limit of the sequence of natural projections

$$\cdots \to \mathbb{Z}/p^3\mathbb{Z} \to \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}.$$

This means an $a \in \mathbb{Z}_p$ is a sequence $(a_1, a_2, \ldots)$ where the $a_n \in \mathbb{Z}/p^n\mathbb{Z}$ are compatible, in the sense that $a_{n+1} \equiv a_n \bmod p^n$. Alternatively, we can think of $a \in \mathbb{Z}_p$ as a formal power series

$$a = b_0 + b_1 p + b_2 p^2 + \cdots$$

where $b_i \in \{0, \ldots, p-1\}$. Indeed, given such an a in the latter representation, we can inductively set $a_n = b_0 + b_1 p + \cdots + b_{n-1}p^{n-1}$ (as an element of $\mathbb{Z}/p^n\mathbb{Z}$) and then we will have $a_{n+1} \equiv a_n \bmod p^n$. It is clear that $\mathbb{Z}_p$ is a ring (operations component-wise in the inverse limit representation) and moreover it is an integral domain, i.e., a commutative ring with no zero divisors.

We view $\mathbb{Z} \subset \mathbb{Z}_p$ in the obvious way—in the inverse limit formulation,

$$a = (a \bmod p, a \bmod p^2, \ldots).$$

Alternatively, we can write $a \in \mathbb{Z}$ as a power series with a finite number of terms $a = b_0 + b_1 p + \cdots + b_n p^n$.

In fact, $\mathbb{Z}_p$ contains many other rational numbers. Since $\mathbb{Z}_p$ is an integral domain containing $\mathbb{Z}$, to determine when a rational number lies in $\mathbb{Z}_p$ it suffices to determine when $\frac{1}{s} \in \mathbb{Z}_p$ for $s \in \mathbb{N}$. (By a rational number in reduced form $\frac{m}{n}$ lying in $\mathbb{Z}_p$, formally we mean there exists $a \in \mathbb{Z}_p$ such that $na = m$—such an a must be unique if it exists by virtue of $\mathbb{Z}_p$ being an integral domain.) The answer is obvious using the inverse limit representation, since $s \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ if and only if $p \nmid s$. Namely, this observation shows:

Lemma 1.2.1. *Define the* **localization** $\mathbb{Z}_{(p)}$ *of $\mathbb{Z}$ at p to be the set of $\frac{m}{n} \in \mathbb{Q}$ (in reduced form) such that $p \nmid n$. Then $\mathbb{Q} \cap \mathbb{Z}_p = \mathbb{Z}_{(p)}$.*

This implies that any $n \in \mathbb{Z}$ is invertible in $\mathbb{Z}_p$ if and only $p \nmid n$. In fact, the collection (multiplicative group) of invertible elements is easy to describe:

Exercise 1.2.1. Show $a = (a_n) = \sum b_n p^n \in \mathbb{Z}_p^\times$ if and only if $a_1 \neq 0$ if and only if $b_0 \neq 0$.

The following result is extremely useful for studying equations over $\mathbb{Z}_p$. (There are many different forms of this result—ours is not the most general.)

Lemma 1.2.2. (Hensel) *Let $f(x) \in \mathbb{Z}[x]$ and $n \in \mathbb{N}$. If $p = 2$ assume $n \geq 2$. Suppose $f(a) \equiv 0 \bmod p^n$ for some $a \in \mathbb{Z}$, but $p \nmid f'(a)$. Then there exists a unique $b \in \mathbb{Z}/p^{n+1}\mathbb{Z}$ such that $f(b) \equiv 0 \bmod p^{n+1}$ and $b \equiv a \bmod p^n$.*

Here $f'(x)$ is the formal derivative of $f(x)$, in other words, the derivative as a real polynomial.

Proof. The Taylor series for $f(x)$ (regarded as a function of a real variable x) about $x = a$ is

$$f(x) = f(a) + f'(a)(x-a) + \frac{f''(a)(x-a)^2}{2!} + \cdots + \frac{f^{(d)}(a)(x-a)^d}{d!}$$

where d is the degree of $f(x)$. Write $b = a + p^n y$ for some y. Then we have

$$f(b) = f(a) + f'(a)p^n y + \frac{f''(a)p^{2n}y^2}{2!} + \cdots + \frac{f^{(d)}p^{dn}y^d}{d!}$$

By induction on j, it is easy to see for $j \geq 2$ (or $j \geq 3$ if $p = 2$) that p^{n+1} divides $\frac{p^{jn}}{j!}$. In other words, we can have

$$f(b) \equiv f(a) + f'(a)p^n y \bmod p^{n+1}.$$

Since $f(a) \equiv 0 \bmod p^n$, we can write $f(a) = a_0 p^n$ so

$$f(b) \equiv a_0 p^n + f'(a) y p^n \equiv (a_0 + f'(a)y)p^n \bmod p^{n+1}.$$

Since $f'(a)$ is nonzero mod p, there is a unique $0 \leq y < p$ such that $a_0 + f'(a)y \equiv 0 \bmod p$. Then $f(b) \equiv 0 \bmod p^{n+1}$ and b is determined uniquely $\bmod p^{n+1}$. □

Starting with $n = 1$ (or 2 if $p = 2$) and applying this inductively, we see that if we have a root a of a one-variable polynomial $f(x)$ mod p (or mod 4), it lifts to a root a_n mod p^n for all n, provided $f'(a) \neq 0$. Moreover, these roots a_n can be chosen to be compatibly so that $(a_n) \in \prod \mathbb{Z}/p^n\mathbb{Z}$ lies in $\mathbb{Z}_p$. Note that the proof of Hensel's lemma constructs an explicit solution, so one can explicitly compute these a_n's.

Example 1.2.1. Suppose p is odd and a is a nonzero square in $\mathbb{Z}/p\mathbb{Z}$, i.e., $f(x) := x^2 - a$ has a root in $\mathbb{Z}/p\mathbb{Z}$. Then $p \nmid f'(a) = 2a$, so by Hensel's lemma we get a solution in $\mathbb{Z}/p^n\mathbb{Z}$ for all n. Hence a is a square in $\mathbb{Z}_p$. Thus for p odd, to check if an element of $\mathbb{Z}_p^\times$ is a square, it suffices to check mod p.

The **p-adic (rational) numbers** $\mathbb{Q}_p$ is the field of fractions of $\mathbb{Z}_p$. By Exercise 1.2.1, to construct $\mathbb{Q}_p$, we only need to adjoin the inverse of p to $\mathbb{Z}_p$, i.e., $\mathbb{Q}_p = \mathbb{Z}_p[\frac{1}{p}]$. Consequently, we can think of p-adic numbers as formal Laurent expansions

$$a = b_n p^n + b_{n+1} p^{n+1} + \cdots,$$

where again each $b_i \in \{0, \dots, p-1\}$ and $n \in \mathbb{Z}$. This was in fact Hensel's original point of view in defining the p-adic numbers—they are a number theoretic analogy of a field of meromorphic functions (replacing p with a complex variable z in the above formal series gives a meromorphic function, which is analytic on the unit disc minus the origin). The restriction on the b_i's guarantees the set of finite formal Laurent expansion $b_n p^n + \cdots + b_N p^N$ are in 1-1 correspondence with $\mathbb{Z}[\frac{1}{p}]$, the ring of rational numbers with p-power denominator via evaluating the sum.

Exercise 1.2.2. Compute the power series expansion of $\frac{1}{2}$ in $\mathbb{Z}_3$ and the Laurent series expansion of $\frac{1}{6}$ in $\mathbb{Q}_3$.

We can also describe $\mathbb{Q}_p$ as the extension of scalars of $\mathbb{Z}_p$ by $\mathbb{Q}$ (which means that $\mathbb{Q}_p$ should be the smallest field containing $\mathbb{Z}_p$):

Exercise 1.2.3. Show $\mathbb{Q}_p \simeq \mathbb{Z}_p \otimes_{\mathbb{Z}} \mathbb{Q}$.

For a in the above form, if $b_n \neq 0$, we put $v_p(a) = \mathrm{ord}_p(a) = n$, which is called the **$p$-adic order** or **(exponential) valuation** of a. (A proper definition of valuation will be given in Section 1.3.) Here n can be positive or negative, so $\mathrm{ord}_p(a)$ is an arbitrary integer for $a \neq 0$. We formally define $\mathrm{ord}_p(0) = \infty$. Using this, we define the **p-adic absolute value** (or **multiplicative valuation**)[7]

$$|a|_p = p^{-v_p(a)} = p^{-n},$$

with n as above if $a \neq 0$. (When $a = 0$, we set $|0|_p = 0$.)

Exercise 1.2.4. Check that $|\cdot|_p$ and v_p satisfy
(i) $|a|_p = 0$ if and only if $v_p(a) = \infty$ if and only if $a = 0$,
(ii) $|ab|_p = |a|_p |b|_p$ and $v_p(ab) = v_p(a) + v_p(b)$; and
(iii) [strong triangle inequality] $|x+y|_p \leq \max\{|x|_p, |y|_p\}$ and $v_p(x+y) \geq \min\{v_p(x), v_p(y)\}$.

This exercise says $|\cdot|_p$ (resp. v_p) is a *nonarchimedean* absolute value (resp. valuation) on $\mathbb{Q}_p$ (see Section 1.3 for formal definitions). Property (ii) combined with $|1|_p = 1$ and $v_p(1) = 0$ says that $|\cdot|_p : \mathbb{Q}_p^\times \to \mathbb{R}_{>0}$ and $v_p : \mathbb{Q}_p^\times \to \mathbb{Z}$ are group homomorphisms.

[7] Usually when I say valuation, I will mean exponential valuation, but because of the relation between $|\cdot|_p$ and v_p, it doesn't really matter which one we work with. They give us exactly the same information—it just depends whether we want to work with a homomorphism $|\cdot|_p : \mathbb{Q}_p^\times \to p^{\mathbb{Z}}$ into a multiplicative group or one $v_p : \mathbb{Q}_p^\times \to \mathbb{Z}$ into an additive group.

Note that a p-adic number has small absolute value if it is divisible by a high power of p. So two p-adic numbers are close if their difference is highly p-divisible. Precisely, one uses the absolute value to define a metric $d(x,y) = |x-y|_p$ on $\mathbb{Q}_p$. This makes $\mathbb{Q}_p$ a topological space. With this topology, $|\cdot|_p$ is a continuous map from $\mathbb{Q}_p$ to $\mathbb{R}_{\geq 0}$. (Note the image of $|\cdot|_p$ is discrete.) Since the valuation is discrete (the image in $\mathbb{R}_{\geq 0}$ is discrete away from 0) all subsets of the form

$$\Omega_n = \left\{a \in \mathbb{Q}_p : |a|_p \leq p^{-n}\right\} = \{a \in \mathbb{Q}_p : v_p(a) \geq n\}$$

are both open and closed for all $n \in \mathbb{Z}$. In particular, observe

$$\Omega_0 = \{a \in \mathbb{Q}_p : |a|_p \leq 1\} = \{a \in \mathbb{Q}_p : v_p(a) \geq 0\} = \mathbb{Z}_p, \tag{1.2.1}$$

so we have

$$\Omega_n = p^n \mathbb{Z}_p. \tag{1.2.2}$$

For $n \geq 0$, note $p^n\mathbb{Z}_p$ is an ideal in $\mathbb{Z}_p$.

Exercise 1.2.5. Show $p\mathbb{Z}_p$ is the unique maximal ideal in $\mathbb{Z}_p$, and every nonzero ideal in $\mathbb{Z}_p$ is of the form $p^n\mathbb{Z}_p$. In particular, $\mathbb{Z}_p$ is a PID.

(Similarly, one can consider fractional ideals and the set of all nonzero fractional ideals is precisely the collection of Ω_n where $n \in \mathbb{Z}$.)

This exercise says that $\mathbb{Z}_p$ is a **discrete valuation ring (DVR)**, i.e., a PID with a unique maximal ideal.[8]

Now let's describe subsets with a specific valuation. Again, by discreteness, we see that for each $n \in \mathbb{Z}$, the set

$$\omega_n = \left\{a \in \mathbb{Q}_p : |a|_p = p^{-n}\right\} = \{a \in \mathbb{Q}_p : v_p(a) = n\}$$

is also open and closed. Again, these sets have a simple description.

Exercise 1.2.6. Show $\omega_n = p^n\mathbb{Z}_p^\times$, so

$$\mathbb{Q}_p^\times = \bigsqcup_{n \in \mathbb{Z}} p^n \mathbb{Z}_p^\times.$$

In particular, the group of units $\mathbb{Z}_p^\times$ of $\mathbb{Z}_p$ is precisely the set of elements of additive valuation 0 (or absolute value 1). In fact the decomposition of $\mathbb{Q}_p^\times$ into translates of the unit group $\mathbb{Z}_p^\times$ yields an isomorphism:

$$\begin{array}{ccc} \mathbb{Q}_p^\times & \simeq & \mathbb{Z} \times \mathbb{Z}_p^\times \\ a & \mapsto & (v_p(a), |a|_p a). \end{array} \tag{1.2.3}$$

[8] Yes, it's strange that the term DVR does not just mean a ring with a discrete valuation, but it is true that DVRs are rings with discrete valuations, i.e., valuations with discrete image.

To further understand the structure of $\mathbb{Q}_p^\times$, we then need to understand the structure of $\mathbb{Z}_p^\times$. We will do this to some extent in the more general case of p-adic fields in the next sections.

The following two exercises explain some similarities and differences of the topology on $\mathbb{Q}_p$ and $\mathbb{R}$.

Exercise 1.2.7. Consider $\mathbb{Q}$ equipped with an absolute value $|\cdot|$. Recall that $\mathbb{R}$ is the completion of $\mathbb{Q}$ with respect to the usual absolute value, i.e., the collection of Cauchy sequences modulo equivalence. Show that the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$ is $\mathbb{Q}_p$.

Exercise 1.2.8. Show that $\mathbb{Q}_p$ is totally disconnected, i.e., its connected components are the singleton sets. Despite this, it has some similarities with $\mathbb{R}$ as a topological space: show both $\mathbb{Q}_p$ and $\mathbb{R}$ are Hausdorff and locally compact (every point has a compact neighborhood), but not compact.

Exercise 1.2.9. Is $\mathbb{Q}_p$ countable or uncountable?

The reason to look at p-adic numbers is that many problems in number theory have *local-global phenomena*. For instance, certain equations over $\mathbb{Z}$ (e.g., $x^2 = a$) will have solutions in $\mathbb{Z}$ if and only if they do over $\mathbb{Z}/p^n\mathbb{Z}$ for all p, n as well as over $\mathbb{R}$. (This is called a *local-global* or *Hasse principle*.) The ring $\mathbb{Z}_p$ puts together all the $\mathbb{Z}/p^n\mathbb{Z}$ at once, and so one can just study the $\mathbb{Z}_p$. For instance, one has the following result (which we will not use):

Proposition 1.2.3. *Let $f \in \mathbb{Z}[x_1, \dots, x_m]$. Then $f(x_1, \dots, x_m) \equiv 0$ has a solution mod p^n for all n if and only if it has a solution in $\mathbb{Z}_p$.*

Proof. See, e.g., [Kat07, Thm 1.42] or [Neu99, Prop II.1.4]. □

The ring $\mathbb{Z}_p$ is better to work with than the individual $\mathbb{Z}/p^n\mathbb{Z}$'s because (for $n > 1$) the latter are not integral domains, and so one can work inside the field $\mathbb{Q}_p$. Then many statements will be true over $\mathbb{Q}$ if and only if they are true over each $\mathbb{Q}_p$ and over $\mathbb{R}$—in fact local-global statements for $\mathbb{Q}$ are easier to come by than ones for $\mathbb{Z}$.

In analogy with algebraic geometry, $\mathbb{Q}$ (or more generally a number field) is called a *global field* and $\mathbb{Q}_p$ (or finite extensions and $\mathbb{R}$ and $\mathbb{C}$) are called *local fields*. (This is not the definition of global and local fields, but all global and local fields of characteristic 0 are of this type. The general definition of a **local ring** is an integral domain with a unique maximal ideal and a **local field** is a field with a discrete valuation which is locally compact—valuations are defined in greater generality below.) Number fields are like curves in this analogy, and the local fields are like points on the curve.[9] The point is knowing

[9] This analogy may seem far-fetched if you haven't seen any algebraic geometry. Here one can associate to an algebraic curve a ring A of functions on the curve, and this A is like our $\mathbb{Z}$. Then points on the curve correspond to prime ideals in the ring A, and consequently the localizations of A at various prime ideals, which are like our various $\mathbb{Z}_p$.

something (e.g., about solutions to an equation) in a local field only tells you part of the information for the global analogue, but often you can "paste" all your local information together to get a global solution. Since problems are often easier over local fields (because the ring of integers has a unique maximal ideal), we will frequently use this local-global approach.

1.2.2 Extensions of $\mathbb{Q}_p$

Since we want to work in the context of arbitrary number fields, rather than just $\mathbb{Q}$, we need to also understand finite extensions of $\mathbb{Q}_p$, which will be completions number fields with respect to p-adic absolute values.

By a **p-adic field** F, we mean a finite extension of $\mathbb{Q}_p$.[10] For the rest of this section, F denotes a degree n extension of $\mathbb{Q}_p$.

Regarding F as a finite-dimensional vector space over $\mathbb{Q}_p$, we define the **ring of integers** $\mathcal{O}_F$ of F to be the set of $x \in F$ such that the minimal polynomial of x has coefficients in $\mathbb{Z}_p$, in analogy with defining rings of integers for number fields. This means $\mathcal{O}_F$ is the integral closure of $\mathbb{Z}_p$ in F (integral closure will be recalled in Section 4.1), and thus $\mathcal{O}_F$ is indeed a ring (see Corollary 4.1.4).

We will use the p-adic valuation/absolute value on $\mathbb{Q}_p$ to define one on F, and use the valuation to study properties of F and $\mathcal{O}_F$.

First, to relate F to $\mathbb{Q}_p$, we want a norm map, which is a local analogue of norms for number fields. Given $x \in F$, left multiplication on F defines a $\mathbb{Q}_p$-linear transformation $L_x : F \to F$, thinking of F as an n-dimensional vector space over $\mathbb{Q}_p$. Define the **norm** $N = N_{F/\mathbb{Q}_p} : F \to \mathbb{Q}_p$ by $N(x) = N_{F/\mathbb{Q}_p}(x) = \det L_x$. It is clear it is multiplicative and for $a \in \mathbb{Q}_p$, we have $N(a) = a^n$. If $F/\mathbb{Q}_p$ is Galois, one can check the norm is the product of the Galois conjugates.

Now, for $x \in F$, we define the **(normalized) $\mathfrak{p}$-adic absolute value** by

$$|x|_{\mathfrak{p}} = |N(x)|_p.$$

It is clear that (i) $|x|_{\mathfrak{p}} = 0$ if and only if $x = 0$ and (ii) $|xy|_{\mathfrak{p}} = |x|_{\mathfrak{p}}|y|_{\mathfrak{p}}$. This does not yet show that $|\cdot|_{\mathfrak{p}}$ is an absolute value—we still need the triangle inequality (cf. Exercise 1.2.4 or Section 1.3). As with the case of $\mathbb{Q}_p$, in fact we have the strong triangle inequality. This will follow from:

Proposition 1.2.4. *The ring of integers is given by*

$$\mathcal{O}_F = \{x \in F : N(x) \in \mathbb{Z}_p\} = \{x \in F : |x|_{\mathfrak{p}} \leq 1\}.$$

Proof. Note the second equality follows from (1.2.1) and the definition of $|\cdot|_{\mathfrak{p}}$. The first equality is contained in the proof of [Neu99, Thm II.4.8]—we will just sketch the proof. Take $\alpha \in F^\times$ and let $f(x) = x^m + c_{m-1}x^{m-1} + \cdots + c_0$ be the minimal polynomial. By definition of

[10] To some people, p-adic field means $\mathbb{Q}_p$, not a finite extension, and they instead prefer to say the mouthful "nonarchimedean local field of characteristic zero." However, sometimes people get lazy and omit nonarchimedean or characteristic zero when they mean it, and I personally think p-adic is more clear. To be even more clear, you can say $\mathfrak{p}$-adic field to mean an extension of $\mathbb{Q}_p$, but I don't know how to pronounce German letters so I just say p-adic.

$\mathcal{O}_F$, we have $c_i \in \mathbb{Z}_p$ for all $0 \le i < m$. However a generalization of Hensel's lemma implies that $c_i \in \mathbb{Z}_p$ for all $0 \le i < m$ if and only if $c_0 \in \mathbb{Z}_p$. Now the characteristic polynomial of x has constant term $\pm N(x)$, but also equals $f(x)^r$ for some r. Thus $N(x) = \pm c_0^r \in \mathbb{Z}_p$ if and only if $c_0 \in \mathbb{Z}_p$, which gives the first equality. □

Corollary 1.2.5. *For $x, y \in F$, we have $|x+y|_\mathfrak{p} \le \max\{|x|_\mathfrak{p}, |y|_\mathfrak{p}\}$.*

This is the desired strong triangle inequality.

Proof. We may assume $x, y \in F^\times$ and $|x|_\mathfrak{p} \le |y|_\mathfrak{p}$. Then dividing by y shows it suffices to prove: if $|1+x|_\mathfrak{p} \le 1$ when $|x|_\mathfrak{p} \le 1$, which by the previous proposition just says $1+x \in \mathcal{O}_F$ when $x \in \mathcal{O}_F$. This is true as $\mathcal{O}_F$ is a ring. □

As in the case of $\mathbb{Q}_p$ (Exercise 1.2.3), one can check that $F \simeq \mathcal{O}_F \otimes_\mathbb{Z} \mathbb{Q} \simeq \mathcal{O}_F \otimes_\mathbb{Z} \mathbb{Q}_p$.

Now we want an analogue of the element p in $\mathcal{O}_F$. In $\mathbb{Z}_p$, p generates the unique prime ideal $p\mathbb{Z}_p$, but in $\mathcal{O}_F$, $p\mathcal{O}_F$ may not be prime. In terms of absolute values, we have $|p|_p = p^{-1}$. In fact, if we take any $a \in \mathbb{Z}_p$ such that $|a|_p = p^{-1}$, it will generate the prime ideal $p\mathbb{Z}_p$. (This follows from the description in terms of valuations (1.2.2) together with multiplicativity of absolute values.)

A **uniformizer** (or **uniformizing element**) of $\mathcal{O}_F$ is an element $\varpi \in \mathcal{O}_F$ such that $|\varpi|_\mathfrak{p} < 1$ is maximal. Fix a uniformizer ϖ. This will play the role of p for a general p-adic field. (Note ϖ is a cursive π, for prime, not an ω).

We can write $N(\varpi) = up^f$ for some unit $u \in \mathbb{Z}_p^\times$ and a unique $f \in \mathbb{N}$. Note f does not depend upon the choice of uniformizer ϖ. Then

$$q := |\varpi|_\mathfrak{p}^{-1} = p^f.$$

Since $|p|_\mathfrak{p}^{-1} = p^n$, we immediately see $f \le n$, i.e., $q \le p^n$, by definition of ϖ. The quantity f is an important invariant of the extension $F/\mathbb{Q}_p$, and we will study it momentarily.

First we obtain a structural analogue of Exercise 1.2.6.

Proposition 1.2.6. *The unit group satisfies $\mathcal{O}_F^\times = \{x \in F : |x|_\mathfrak{p} = 1\}$, and we have the decomposition $F^\times = \varpi^\mathbb{Z}\mathcal{O}_F^\times = \bigsqcup_{m\in\mathbb{Z}} \varpi^m \mathcal{O}_F^\times$.*

Proof. For the first assertion, note for $x \in F^\times$, we have $x \in \mathcal{O}_F^\times$ if and only if $x \in \mathcal{O}_F$ and $x^{-1} \in \mathcal{O}_F$. By the previous proposition, this means $x \in \mathcal{O}_F^\times$ if and only if $|x|_\mathfrak{p} \le 1$ and $|x^{-1}|_\mathfrak{p} \le 1$. However, multiplicativity implies $|x^{-1}|_\mathfrak{p}|x|_\mathfrak{p} = |1|_\mathfrak{p} = 1$, i.e., $|x^{-1}|_\mathfrak{p} = |x|_\mathfrak{p}^{-1}$. This implies $\mathcal{O}_F^\times = \{x \in F : |x|_\mathfrak{p} = 1\}$.

Next we observe $|\cdot|_\mathfrak{p}$ is a group homomorphism from $F^\times$ to $q^\mathbb{Z}$. By multiplicativity, it suffices to show the image of $|\cdot|_\mathfrak{p}$ is $q^\mathbb{Z}$. If not, there exists $x \in F^\times$ such that $N(x) = up^k$ where $u \in \mathbb{Z}_p^\times$ but $f \nmid k$. Then there exists $m \in \mathbb{Z}$ such that $0 < k - mf < f$, which says $1 > |\varpi^{-m}x|_\mathfrak{p} = p^{mf-k} > q^{-1}$, contradicting the maximality in the definition of unifomizers.

So given any $x \in F^\times$, there exists a (unique) n such that $|\varpi^{-m}x|_\mathfrak{p} = 1$, i.e., such that $x = \varpi^m u$ where $|u|_\mathfrak{p} = 1$, i.e., $u \in \mathcal{O}_F^\times$. □

Note each $\varpi^m\mathcal{O}_F^\times$ in the decomposition is precisely the set of $x \in F^\times$ such that $|x|_\mathfrak{p} = q^{-m}$. In particular, the above proposition implies that the set of uniformizers is just $\varpi\mathcal{O}_F^\times$ for

some choice of uniformizer ϖ, i.e., all uniformizers are obtained from others by multiplication by units. Since the choice of uniformizer usually does not matter, it is common to abuse terminology and say ϖ is *the* uniformizer of $\mathcal{O}_F$ (or just of F).

In the future, if F is a p-adic field we may write ϖ_F without further explanation to denote a uniformizer of F.

As an alternative to working with absolute values, we can work with exponential valuations as for $\mathbb{Q}_p$. Define the **(normalized) $\mathfrak{p}$-adic valuation**[11] on F to be

$$v_\mathfrak{p} : F \to \mathbb{Z} \cup \{\infty\}, \qquad v_\mathfrak{p}(x) = \frac{1}{f} v_p(N(x)).$$

Then, as in the case of $\mathbb{Q}_p$, we have the relation

$$|x|_\mathfrak{p} = q^{-v_\mathfrak{p}(x)}. \tag{1.2.4}$$

Consequently, we can describe $\mathcal{O}_F = \{x \in F : v_\mathfrak{p}(x) \geq 0\}$, $\mathcal{O}_F^\times = \{x \in F : v_\mathfrak{p}(x) = 0\}$ and a uniformizer is precisely an element of $\mathcal{O}_F$ such that $v_\mathfrak{p}(\varpi) = 1$.

Let's see what happens when we restrict our absolute value/valuation to $\mathbb{Q}_p$. For $a \in \mathbb{Q}_p$, we have $N_{F/\mathbb{Q}_p}(a) = a^n$ (recall $n = [F : \mathbb{Q}_p]$), so

$$|a|_\mathfrak{p} = |a^n|_p = |a|_p^n,$$

or equivalently

$$v_\mathfrak{p}(a) = \frac{1}{f} v_p(a^n) = \frac{n}{f} v_p(a). \tag{1.2.5}$$

Note (1.2.5) implies $f|n$. In fact, f can be any divisor of n as F ranges over degree n extensions of $\mathbb{Q}_p$ (see Theorem 1.2.10).

Let me explain the reason for the term "normalized" in our definitions of $\mathfrak{p}$-adic absolute value and valuation. Given a field extension K/F, where F has an absolute value/valuation, you can ask whether one can extend the absolute value/valuation to K. Our work above implies this is true for p-adic fields with $\mathfrak{p}$-adic valuations, however $v_\mathfrak{p}$ and $|\cdot|_\mathfrak{p}$ are not quite extensions of v_p and $|\cdot|_p$ in general—they are off by factors of $\frac{n}{f}$ and a power of n respectively. In many treatments of $\mathfrak{p}$-adic fields, one starts off by showing the valuations from $\mathbb{Q}_p$ extend to F, and then normalize those extended valuations because it is nicer to have the image of $v_\mathfrak{p}$ being $\mathbb{Z}$ rather than $\frac{f}{n}\mathbb{Z}$.

Now, to finish the analogy with p and ϖ, we will generalize Exercise 1.2.5 and see that ϖ generates the maximal ideal of $\mathcal{O}_F$.

Proposition 1.2.7. *$\mathcal{O}_F$ is a DVR with unique maximal ideal*

$$\mathfrak{p} := \varpi\mathcal{O}_F = \{x \in \mathcal{O}_F : v_\mathfrak{p}(x) \geq 1\} = \{x \in F : |x|_\mathfrak{p} < 1\},$$

and every nonzero ideal in $\mathcal{O}_F$ is of the form $\mathfrak{p}^m = \varpi^m\mathcal{O}_F$. Moreover, $\mathfrak{p}^m/\mathfrak{p}^{m+j} \simeq \mathcal{O}_F/\mathfrak{p}^j$ (as abelian groups or $\mathcal{O}_F$-modules).

[11] Just like my convention for p-adic fields, I may sometimes say p-adic absolute value or p-adic valuation instead of $\mathfrak{p}$-adic. However, in this section, I will try to restrict to using $\mathfrak{p}$-adic for clarity.

Proof. Let $\mathcal{I}$ be a nonzero ideal in $\mathcal{O}_F$, and let $x \in \mathcal{I}$ be an element of minimal valuation. Say $v_{\mathfrak{p}}(x) = m$. Then $xu \in \mathcal{I}$ for any $u \in \mathcal{O}^\times$, so $\mathcal{I}$ contains every element of valuation m. More generally, $x\varpi^j\mathcal{O}^\times \subset \mathcal{I}$ implies $\mathcal{I}$ contains every element of valuation $m+j$ for $j \geq 0$. Thus $\mathcal{I} = \varpi^m\mathcal{O}_F$. (It is clear that $\varpi^m\mathcal{O}_F$ is an ideal for each $m \geq 0$.)

This classifies the ideals of $\mathcal{O}_F$, and they are nested

$$\mathcal{O}_F \supset \varpi\mathcal{O}_F \supset \varpi^2\mathcal{O}_F \supset \cdots,$$

so $\mathfrak{p}$ is the unique maximal ideal.

The isomorphism then follows from applying the $\mathcal{O}_F$-module homomorphism $x \mapsto \varpi^m x$ from $\mathcal{O}_F$ to $\mathfrak{p}^m$ and taking quotients. □

A basic question in number theory is to understand how primes behave along extensions of fields. We could consider this for a general extension of p-adic fields K/F, but for simplicity. Since p-adic fields are DVRs, it is pretty to easy to understand what is going on, as there is only one prime ideal. For simplicity though, we will just consider extensions $F/\mathbb{Q}_p$.

The prime ideal of $\mathbb{Z}_p$ is just $p\mathbb{Z}_p$, and the basic question in this case is to describe the prime ideal factorization of $p\mathcal{O}_F$ in $\mathcal{O}_F$. By the above, we have

$$p\mathcal{O}_F = \varpi^e\mathcal{O}_F$$

for some e. We call e the **ramification index** of $F/\mathbb{Q}_p$. If $e > 1$ we say $F/\mathbb{Q}_p$ is **ramified** in F, otherwise $F/\mathbb{Q}_p$ is **unramified**.

Both p and ϖ^e must be elements of minimal valuation of $p\mathcal{O}_F$, so we get the **local fundamental identity**

$$n = ef. \tag{1.2.6}$$

In addition, the quotient $\mathcal{O}_F/\mathfrak{p}$ is a finite field, called the **residue field** of F. This is a finite extension of $\mathbb{Z}_p/p\mathbb{Z}_p$ and its order is determined by the quantity f:

Proposition 1.2.8. *We have*

$$f = [\mathcal{O}_F/\mathfrak{p} : \mathbb{Z}_p/p\mathbb{Z}_p],$$

i.e.,

$$\mathcal{O}_F/\mathfrak{p} \simeq \mathbb{F}_q = \mathbb{F}_{p^f}.$$

Proof. See, e.g., [Neu99, Prop II.6.8], [Neu99, Prop I.8.2] or [RV99, Prop 4-23]. □

We call f the **inertia degree** of $F/\mathbb{Q}_p$. Note if $f = n$ so $q = p^n$, then by the local fundamental identity $F/\mathbb{Q}_p$ is unramified.

So the local fundamental identity (1.2.6) is a relation between the ramification index, inertia degree and the degree of an extension of p-adic fields, and this theory extends to arbitrary p-adic extensions K/F. We remark that (1.2.6) is not usually it is not called the fundamental identity until we interpret f as the inertia degree—in fact, we defined things in a way which is backwards to what is usual. Namely, it's typical to *define* f as the inertia degree.

Now that we have some idea of the additive and ideal structure of $\mathcal{O}_F$, let's consider the structure of the unit group $\mathcal{O}_F^\times$. Just like one has the filtration $\mathcal{O}_F \supset \mathfrak{p} \supset \mathfrak{p}^2 \supset \cdots$ of ideals, we have a filtration of **higher unit groups**

$$\mathcal{O}_F^\times \supset 1+\mathfrak{p} \supset 1+\mathfrak{p}^2 \supset 1+\mathfrak{p}^3 \supset \cdots .$$

The group $1+\mathfrak{p}$ is called the **principal unit group**. Some authors denote the higher unit groups $1+\mathfrak{p}^m$ by $U^{(m)}$ or U_m or $\mathcal{O}_F^{(m)}$. We will occasionally use $\mathcal{O}_F^{(m)}$ where $\mathcal{O}_F^{(0)} = \mathcal{O}_F^\times$. (This is mainly when we want to discuss the unit groups including $\mathcal{O}_F^\times$ in a uniform way, simply because we cannot write $\mathcal{O}_F^\times$ in the form $1+\mathfrak{p}^m$.)

Proposition 1.2.9. *$\mathcal{O}_F^\times/(1+\mathfrak{p}) \simeq \mathbb{F}_q^\times$ and $(1+\mathfrak{p}^m)/(1+\mathfrak{p}^{m+1}) \simeq \mathbb{F}_q$ for $m \geq 1$.*

Proof. Note the mod $\mathfrak{p}^m$ homomorphism $\mathcal{O}_F^\times \to (\mathcal{O}_F/\mathfrak{p}^m)^\times$ is surjective with kernel $1+\mathfrak{p}^m$, i.e.,

$$\mathcal{O}_F^\times/(1+\mathfrak{p}^m) \simeq (\mathcal{O}_F/\mathfrak{p}^m)^\times.$$

Now apply Proposition 1.2.8 to $\mathcal{O}_F^\times/(1+\mathfrak{p})$ and Proposition 1.2.7 to $(\mathcal{O}_F^\times/(1+\mathfrak{p}^m))/(\mathcal{O}_F^\times/(1+\mathfrak{p}^{m+1}))$. □

Now we can refine our decomposition Proposition 1.2.6 to get the refined structural result

$$F^\times = \varpi^{\mathbb{Z}}\mathcal{O}_F^\times \simeq \mathbb{Z} \times \mathbb{F}_q^\times \times (1+\mathfrak{p}). \tag{1.2.7}$$

In the case $F = \mathbb{Q}_p$, this gives

$$\mathbb{Q}_p^\times = p^{\mathbb{Z}}\mathbb{Z}_p^\times \simeq \mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z})^\times \times (1+p\mathbb{Z}_p), \tag{1.2.8}$$

which refines (1.2.3).

In particular, we see that $\mathbb{Z}_p^\times$ contains the $(p-1)$-th roots of unity. One can show that, for $p > 2$, $1+p\mathbb{Z}_p$ does not contain any nontrivial roots of unity, For instance, the exponential map (which is defined by a power series, but we will not explain) gives an isomorphism of the multiplicative group $1+p\mathbb{Z}_p$ with the (torsion-free) additive group $\mathbb{Z}_p$ for $p > 2$. For $p = 2$, one gets an isomorphism of $1+4\mathbb{Z}_2$ with $\mathbb{Z}_2$). Thus the group of roots of unity in $\mathbb{Q}_p^\times$ is $(\mathbb{Z}/p\mathbb{Z})^\times$ if p is odd and $\{\pm 1\}$ if $p = 2$, and we can rewrite (1.2.8) as

$$\mathbb{Q}_p^\times \simeq \begin{cases} \mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z})^\times \times \mathbb{Z}_p & p \text{ odd} \\ \mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}_2 & p = 2. \end{cases}$$

While we do not need the following result (not the full result anyway, though will make use of the much simpler result Proposition 1.2.12 for quadratic fields), you should know the following classification result for p-adic fields. Denote by $\mathbb{Q}_p^{\times n}$ the subgroup of n-th powers in $\mathbb{Q}_p^\times$.

Theorem 1.2.10. *(a) Any extension $\mathbb{Q}_p$ of degree n is of the form $\mathbb{Q}_p[\sqrt[n]{a}]$ for some $a \in \mathbb{Z}_p$.*

(b) For each n, there are only finitely many extensions $F/\mathbb{Q}_p$ (up to isomorphism) of degree n. There is a unique such extension which is unramified, and the unramified extension is cyclic. Moreover all possible ramification types occur, i.e., given n and any $e|n$, there is a degree n extension of $\mathbb{Q}_p$ with ramification index e.

Proof. (a) This follows from [Ser79, Prop III.12].

(b) Note part (a) says that the number of extensions $F/\mathbb{Q}_p$ of degree n (up to isomorphism) is bounded by the number of n-th power classes $a \in \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times n}$. Then the finiteness follows from the finiteness of $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times n}$, which can be deduced from the structure result (1.2.8). The existence, uniqueness and cyclicity of unramified extensions follows from [Ser79, Thm III.2], using that $\mathbb{F}_{p^n}/\mathbb{F}_p$ is cyclic. Now we can construct an extension $F/\mathbb{Q}_p$ of degree n with any ramification index $e|n$ and inertia degree $f = \frac{n}{e}$ by first taking K to be the unramified extension of degree f, and then $F = K(\sqrt[e]{p})$. □

By the structure result (1.2.7), the unramified extension of $\mathbb{Q}_p$ of degree n must contain the $q-1 = p^n - 1$ roots of unity, thus it can be constructed by adjoining the primitive $p^n - 1$ roots of unity to $\mathbb{Q}_p$, i.e., it is the splitting field of $x^{p^n} - x$ over $\mathbb{Q}_p$.

All this theory of ramification and inertia for extensions $F/\mathbb{Q}_p$ is valid for general extensions of p-adic fields K/F, with very minor modifications. We briefly discuss this when talking about norms below.

Squares and quadratic extensions

Now let's examine the case of quadratic extensions of $\mathbb{Q}_p$ in more detail, where part (a) of the theorem above is just a consequence of the quadratic formula, and we can describe the square classes by elementary methods.

Lemma 1.2.11. *An element in $u \in \mathbb{Z}_p^\times$ is a square if and only if u is a square in $\mathbb{Z}/p\mathbb{Z}$ (resp. $\mathbb{Z}/8\mathbb{Z}$) where p is odd (resp. $p = 2$).*

Proof. If $u \in \mathbb{Z}_p^\times$ is a square, it is necessary that u is a square in $\mathbb{Z}/p^n\mathbb{Z}$ for each n, so we just need to show the "if" direction.

We already did the case of p odd with Hensel's lemma in Example 1.2.1. When $p = 2$, the form of Hensel's lemma we gave is not quite strong enough because 2 divides the derivative of $f(x) = x^2 - u$. One could prove a more general version of Hensel's lemma that would apply in this case, but this specific case is simple and we do it directly.

It suffices to show the following: if $a \in \mathbb{Z}$ is a square mod 2^n, then a is a square mod 2^{n+1} for any $n \geq 3$. Or, equivalently: if $0 < a < 2^n$ is a square mod 2^n then a and $a + 2^n$ are squares mod 2^{n+1} for any $n \geq 3$ (i.e., all lifts of nonzero squares are nonzero squares). Let $0 < a < 2^n$. Suppose $x \in \mathbb{Z}$ such that $x^2 \equiv a \bmod 2^n$. Then

$$(x + 2^{n-1}y)^2 \equiv x + 2^n y + 2^{2n-2}y^2 \equiv x^2 + 2^n y \bmod 2^{n+1}$$

provided $n \geq 3$. Taking $y \in \{0, 1\}$, we see both a and $a + 2^n$ are squares mod 2^{n+1}. □

Proposition 1.2.12. *(i) If p is odd, there are 3 quadratic extensions of $\mathbb{Q}_p$. Namely, if u is a nonsquare in $\mathbb{Z}_p^\times$, they are given by $\mathbb{Q}_p(\sqrt{u})$ (the unramified extension), $\mathbb{Q}_p(\sqrt{p})$ and $\mathbb{Q}_p(\sqrt{up})$.*

(ii) There are 7 quadratic extensions of $\mathbb{Q}_2$.

Proof. To understand the quadratic extensions of $\mathbb{Q}_p$, note that $\mathbb{Q}_p(\sqrt{a}) = \mathbb{Q}_p(\sqrt{b})$ for $a, b \in \mathbb{Q}_p^\times$ if and only if a and b differ (multiplicatively) by a square. So we want to

understand the square classes $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$ in $\mathbb{Q}_p^\times$. The isomorphism $\mathbb{Q}_p^\times \simeq \mathbb{Z} \times \mathbb{Z}_p^\times$ from (1.2.3) tells us $\mathbb{Q}_p^{\times 2} \simeq 2\mathbb{Z} \times \mathbb{Z}_p^{\times 2}$. (Clearly, the valuation of any square is even.) Hence

$$\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_p^\times/\mathbb{Z}_p^{\times 2}.$$

The nontrivial ($\neq \mathbb{Q}_p^{\times 2}$) square classes give the distinct quadratic extensions of $\mathbb{Q}_p$. When p is odd, the previous lemma says we have 2 square classes in $\mathbb{Z}_p^\times$, and thus 4 square classes in $\mathbb{Q}_p^\times$.

When $p = 2$, one can use the above lemma to check there are 8 square classes in $\mathbb{Q}_2^\times$. (You should check this as part of the next exercise.) □

Exercise 1.2.10. Write down explicitly the 3 quadratic extensions of $\mathbb{Q}_7$ and the 7 quadratic extensions of $\mathbb{Q}_2$.

It is easy to describe the rings of integers in the quadratic extensions of $\mathbb{Q}_p$, particularly if p is odd.

Exercise 1.2.11. Suppose p is odd and $E = \mathbb{Q}_p(\sqrt{d})$ is a quadratic extension where $v_p(d) \in \{0, 1\}$. Show $\mathcal{O}_E = \left\{a + b\sqrt{d} : a, b \in \mathbb{Z}_p\right\}$.

$\mathfrak{p}$-adic topology

Finally, we briefly discuss the topology of p-adic fields. As with $\mathbb{Q}_p$, now that we have an absolute value $|\cdot|_\mathfrak{p}$ on F, we have a metric on F given by $|x - y|_\mathfrak{p}$, and thus can endow F with the metric space topology. Note the open ball of radius r around x is

$$B_r(x) = \{y \in F : |x - y|_\mathfrak{p} < r\} = \{x + z \in F : |z|_\mathfrak{p} < r\} = x + \varpi^m \mathcal{O}_F$$

where m is the smallest integer such that $q^{-m} < r$. In particular, the open balls in F around 0 are just the sets $\varpi^m\mathcal{O}_F$, i.e., the fractional ideals $\mathfrak{p}^m$ for $m \in \mathbb{Z}$. Since the image of $|\cdot|_\mathfrak{p} : F^\times \to q^\mathbb{Z}$ is discrete (i.e., $v_\mathfrak{p}$ is a discrete valuation), the open balls are also closed—namely, $B_r(x)$ is also equal to the closed ball of radius r about x whenever $r \notin q^\mathbb{Z} \cup \{0\}$.

Thus the sets $B_r(x)$ for a basis of (open or closed) neighborhoods for the topology on F. Since F is a metric space, it is Hausdorff (i.e., T_2—in fact T_6). It is also complete:

Proposition 1.2.13. *Any $\mathfrak{p}$-adic field is complete with respect to $|\cdot|_\mathfrak{p}$.*

Proof. This follows as the topology on F will be the same as the product topology on F viewed as a vector space over $\mathbb{Q}_p$. See, e.g., [Neu99, Thm II.4.8] or [cas67, Cor II.10.2]. □

However, as a result of the strong triangle inequality, unlike euclidean spaces, balls of radius r do not have well defined centers. Namely,

$$B_r(x) = B_r(y) \iff x - y \in B_r(0).$$

Exercise 1.2.12. Show that F is totally disconnected, i.e., the (nonempty) connected components are the singleton sets, but the topology on F is not the discrete topology.

Exercise 1.2.13. Show any ball $B_r(x)$ in F is compact.

This implies F is locally compact, i.e., any point has a compact neighborhood.

Exercise 1.2.14. Show $|\cdot|_{\mathfrak{p}} : F \to \mathbb{R}_{\geq 0}$ is a continuous map.

We also want to understand something about the topology on $F^\times$, given the subspace topology. A basis of open neighborhoods about 1 are given by the higher unit groups $\mathcal{O}_F^{(m)}$, $m \geq 0$. One can check that $F^\times$ is a topological group, i.e., a topological space which is also a group such that multiplication and inversion are continuous maps, and therefore a basis of open neighborhoods around any $x \in F^\times$ are given by the sets $x\mathcal{O}_F^{(m)}$.

The higher unit groups are compact open subgroups of $F^\times$, and this provides an alternative way of proving $\mathcal{O}_F^{(m)}/\mathcal{O}_F^{(m+1)}$ is finite, by the following exercise.

Exercise 1.2.15. Let G be a compact topological group and $H \subset G$ an open subgroup. Show $[G : H] < \infty$.

This topological method of proving finiteness of quotients is important for us—this idea can be used in an adelic proof of the finiteness of the class group of number fields, which can be adapted to the setting of (quaternion) algebras. Of course, this coarse argument does not give the precise result in Proposition 1.2.9. However one can refine such topological argument in the language of measure theory to determine the size of quotients such as $\mathcal{O}_F^{(m)}/\mathcal{O}_F^{(m+1)}$.[12]

General extensions and image of norm maps

Just like absolute values are very important in studying the arithmetic of integers (e.g., in the division algorithm), norms are very important in the study of extension of number fields and p-adic fields.

For an arbitrary extension of number fields K/F, we can define a norm map $N_{K/F} : K \to F$ in the same way that we define it in the case $F = \mathbb{Q}_p$. View K as an F-vector space and associate to $x \in K$ the F-linear operator L_x given by left multiplication by x. Then set $N_{K/F}(x) = \det L_x$. If K/F is Galois, then $N_{K/F}(x) = \prod x^\sigma$ is the product of Galois conjugates x^σ for $\sigma \in \mathrm{Gal}(K/F)$.

The norm map is multiplicative and $N_{K/F}(x) = 0$ if and only if $x = 0$, so it restricts to a map $N_{K/F} : K^\times \to F^\times$. Let $K/E/F$ be a chain of extension of p-adic fields. Then norms behave nicely under composition

$$N_{K/F} = N_{E/F} \circ N_{K/E}.$$

[12] I'm not sure if there is an argument to compute $\mathcal{O}_F^{(m)}/\mathcal{O}_F^{(m+1)}$ using measures but avoiding the idea of Proposition 1.2.9.

The above facts are elementary, and should be none too surprising if you are familiar with the number field case. However, in the p-adic case, the image of the norm map is much easier to understand. This will be important for us later. The description is in terms of ramification and inertia, so we will briefly summarize the theory for general p-adic extensions, extending what we explained for $F/\mathbb{Q}_p$ above.

Suppose K/F is an extension of p-adic fields, $\mathfrak{p}$ the unique prime ideal in $\mathcal{O}_F$ and $\mathfrak{P}$ the unique prime ideal in $\mathcal{O}_K$. Denote uniformizers by ϖ_F and ϖ_K. Then

$$N_{K/F}(\varpi_K) \in \varpi_F^{f_{K/F}} \mathcal{O}_F^\times$$

for some $f_{K/F} \in \mathbb{N}$, which we call the **inertia degree**, and

$$f_{K/F} = [(\mathcal{O}_K/\mathfrak{P}) : (\mathcal{O}_F/\mathfrak{p})].$$

The **ramification index** $e_{K/F}$ is the unique natural number such that $\mathfrak{p}\mathcal{O}_K = \mathfrak{P}^{e_{K/F}}$. Again, we have a **local fundamental identity**

$$n = [K : F] = e_{K/F} f_{K/F}.$$

As a consequence of Theorem 1.2.10, there are only finely many extensions K/F of degree n. Analogously, all possible ramification types occur and there is a unique **unramified** extension K/F of degree n, i.e., with $e_{K/F} = 1$. (The unramified extension K/F will be the unique unramified extension of degree $[K : \mathbb{Q}_p]$ over $\mathbb{Q}_p$ if and only if $F/\mathbb{Q}_p$ is unramified.)

We know the image of the norm map $N_{K/F} : K^\times \to F^\times$ lies in $\bigsqcup_{m\in\mathbb{Z}} \varpi_F^{mf_{K/F}} \mathcal{O}_F^\times$ by multiplicativity. To determine its exact image, it suffices to determine what is the image when restricted to units $N_{K/F} : \mathcal{O}_K^\times \to \mathcal{O}_F^\times$.

Theorem 1.2.14. *Let K/F be a cyclic extension of p-adic fields, i.e., K/F is Galois with cyclic Galois group. Then*

$$[\mathcal{O}_F^\times : N_{K/F}(\mathcal{O}_K^\times)] = e_{K/F}.$$

This determines the image completely if $e_{K/F} = 1$, i.e., if K/F is unramified. This is one reason why unramified extensions are nice to work with. The above result in the case of quadratic extensions, which are necessarily cyclic, will be useful in classifying local quaternion algebras. Specifically,

Corollary 1.2.15. *Let K/F be an unramified quadratic extension of p-adic fields, with $\mathfrak{p}$ denoting the prime of F. Then, for $x \in F^\times$, we have $x \in N_{K/F}(K^\times)$ if and only if $x \in \mathfrak{p}^{2m}\mathcal{O}_F^\times$ for some $m \in \mathbb{Z}$, i.e., if and only if $v_\mathfrak{p}(x)$ is even.*

1.3 Valuations and completions of number fields

Let v be a **(nonarchimedean) valuation** on a field F, i.e., a function $v : F \to \mathbb{R} \cup \{\infty\}$ such that for all $a, b \in F$ we have (i) $v(a) = \infty$ if and only if $a = 0$, (ii) $v(ab) = v(a) + v(b)$, and (iii) $v(a + b) \geq \min(v(a), v(b))$ with equality when $v(a) \neq v(b)$.

We say a valuation v is **discrete** if image of v restricted to $F^\times$ is a discrete subset of $\mathbb{R}$.

Example 1.3.1. Let F be any field. The function $v(0) = \infty$ and $v(x) = 0$ for $x \in F^\times$ defines a discrete, nonarchimedean valuation on F, called the **trivial valuation**.

Example 1.3.2. If F is a p-adic field with prime ideal $\mathfrak{p}$ (i.e., a prime ideal of $\mathcal{O}_F$), then the $\mathfrak{p}$-adic valuation $v_\mathfrak{p}$ defined in the previous section is a discrete (nonarchimedean) valuation.

Note that if v is a valuation, so is λv for any $\lambda \in \mathbb{R}_{>0}$. We say two valuations v and w are **equivalent** if $w = \lambda v$ for some $\lambda \in \mathbb{R}_{>0}$.

Valuations give rise to absolute values, as we saw for p-adic fields in Section 1.2.

By an **absolute value**[13] on F, we mean a function $|\cdot| : F \to \mathbb{R}_{\geq 0}$ such that the following hold for all $a, b \in F$: (i) $|a| = 0$ if and only if $a = 0$, (ii) $|ab| = |a||b|$, and (iii) there exists $\kappa > 0$ such that $|a + b| \leq \kappa \max\{|a|, |b|\}$ for all $a, b \in F$.You may be more familiar with a more strict definition of absolute value which requires the usual triangle inequality (iii') $|a + b| \leq |a| + |b|$ for all a, b. We allow the generalized triangle inequality (iii) because we want to consider powers $|\cdot|$ of usual absolute values to also be absolute values.

Exercise 1.3.1. Let $|\cdot| : F \to \mathbb{R}_{\geq 0}$ be a function satisfying (i) and (ii) above. Show that (iii) holds with $\kappa = 2$ if and only if the usual triangle inequality (iii') holds.[14] (*Hint:* For one direction, show $|a_1 + \cdots + a_n| \leq 2n \sum |a_i|$ and use the binomial theorem on $|a + b|^n$.)

We always have the trivial absolute value given by $|a| = 1$ for $a \neq 0$. If $|\cdot|$ is an absolute value, so is $|\cdot|^s$ for any $s > 0$. We say two absolute values $|\cdot|_1$ and $|\cdot|_2$ are **equivalent** if $|\cdot|_2 = |\cdot|_1^s$ for some $s > 0$. You can check that every absolute value, as we have defined it, is equivalent to one with $\kappa = 2$, from which one can deduce the usual triangle inequality (iii'). (You might now think our more general notion of an absolute value with (iii) instead of (iii') is silly, but it makes the correspondence between valuations and absolute values cleaner. We will also define a complex absolute value below that is not an absolute value in the stricter sense of requiring (iii').)

The generalized triangle inequality (iii) with $\kappa = 1$, i.e.,

$$|a + b| \leq \max\{|a|, |b|\} \quad \text{for all } a, b \in F,$$

is called the **ultrametric** (or **strong triangle**) **inequality** If the ultrametric inequality holds for $|\cdot|$, we say $|\cdot|$ is **nonarchimedean** or **ultrametric**. Otherwise, $|\cdot|$ is **archimedean**.[15]

[13] Some authors call absolute values "(multiplicative) valuations" and what we call valuations "exponential valuations." We will see that valuations correspond to (nonarchimedean) absolute values so there is not a serious discrepancy in this terminology.

[14] More generally, (iii') holds if and only if (iii) holds for some $\kappa \leq 2$, because (iii) holding with $\kappa \leq 2$ means it holds for $\kappa = 2$.

[15] This terminology comes from the archimedean property: given any $x \in \mathbb{R}$, there exists $n \in \mathbb{N}$ such that $|nx| > 1$. You may remember using this in analysis. This is clearly not true for p-adic (or more generally ultrametric) absolute values, hence the term nonarchimedean.

Exercise 1.3.2. Show that any absolute value is equivalent to one with satisfying the usual triangle inequality (iii'). Show this is not true if we replace (iii') by the ultrametric inequality, but that if two absolute values are equivalent, then one satisfies the ultrametric inequality if and only if the other one does.

Now you can work out the correspondence between valuations and absolute values.

Exercise 1.3.3. Let v be a valuation on F and $\beta \in \mathbb{R}_{>1}$. Show $|a|_v = \beta^{-v(a)}$ is an absolute value, and replacing β by some $\beta' > 1$ results in an equivalent absolute value. Further, show this construction gives a one-to-one correspondence between equivalence classes of valuations and equivalence classes of nonarchimedean absolute values.

One can try to define (exponential) archimedean valuations to extend the correspondence to include all absolute values, but I am not aware of a clean way to do this and it wouldn't really be that useful anyway—it would only provide a convenience for terminology purposes.[16] (The usual definition of an (exponential, not necessarily nonarchimedean) valuation is to loosen (iii) in our definition by not requiring $v(a+b) = \min\{v(a), v(b)\}$ when $v(a) \neq v(b)$—this stronger condition is what makes a nonarchimedean valuation. However, the usual definition is not broad enough to allow for things like $v(a) = -\log|a|$ on $\mathbb{R}$, which is something we would want for a correspondence between archimedean valuations and absolute values.)

We define a **prime** or **place** of F to be an equivalence class of absolute values. Since being archimedean or not is a property of equivalence classes, we likewise call primes/places archimedean or nonarchimedean. We often denote places of F by the letter v (both in the nonarchimedean case where v corresponds to an equivalence class of valuations and in the archimedean case where we haven't defined archimedean valuations).

Now let's specialize to the case of number fields, which will explain the use of the term prime for an equivalence class of absolute values.

Let F be a number field and $\mathcal{O}_F$ its ring of integers. Fix $\mathfrak{p}$ be a nonzero prime ideal in $\mathcal{O}_F$. For any $x \in F$, define the **$\mathfrak{p}$-adic valuation** $v_\mathfrak{p}(x)$ be the maximal element of $\mathbb{Z} \cup \{\infty\}$ such that $a \in \mathfrak{p}^{v_\mathfrak{p}(x)}$. (Note this is a fractional ideal if the exponent is negative, and agrees with v_p on $\mathbb{Q}$ when $F = \mathbb{Q}$.) It is easy to check that $v_\mathfrak{p}$ is a nonarchimedean valuation on F. Using this, we define the **$\mathfrak{p}$-adic absolute value** on F by

$$|x|_\mathfrak{p} = q^{-v_\mathfrak{p}(x)}, \quad \text{where } q = \#\mathcal{O}_F/\mathfrak{p}.$$

We can determine q in terms of norms. Recall that the **(ideal) norm** $N(\mathcal{I}) = N_{F/\mathbb{Q}}(\mathcal{I})$ of a (fractional) ideal $\mathcal{I}$ of $\mathcal{O}_F$ is the (fractional) ideal of $\mathbb{Z}$ generated by the element norms $N(x)$ as x ranges over $\mathcal{I}$. Hence we have $N(\mathcal{I}) = \frac{a}{b}\mathbb{Z}$ for some $\frac{a}{b} \in \mathbb{Q}$. We denote by $|N(\mathcal{I})|$ the (usual) absolute value $|\frac{a}{b}|$ of a generator—$|N(\mathcal{I})|$ is called the **absolute norm** of $\mathcal{I}$. Thus if $\mathcal{I} = x\mathcal{O}_F$ is a principal ideal of F, then

$$|N(x\mathcal{O}_F)| = |N(x)|,$$

[16] I might occasionally get forgetful and breach our conventions by saying valuation to include the archimedean case as well—if I do, just interpret valuation to mean absolute value in the archimedean case, i.e., multiplicative valuation.

i.e., the absolute values of the ideal norm and element norms are the same.

Note if $\mathfrak{p}$ is a prime ideal in $\mathcal{O}_F$ above $p \in \mathbb{N}$, then $|N(\mathfrak{p})| = p^f$ for some f. A basic result is that $\#\mathcal{O}_F/\mathfrak{p} = \#\mathbb{Z}/N(\mathfrak{p})$ (but not isomorphic in general—the left hand quotient always defines a field whereas the righthand side is just a ring), i.e., $q = p^f$. In analogy with the local setting, we call f the **inertia degree** of $\mathfrak{p}$ (over p).

Below, when we see how to associate $\mathfrak{p}$-adic fields to number fields, we will see that the definitions of $\mathfrak{p}$-adic valuations and absolute values (as well as inertia degree) on number fields are compatible with the definitions we gave last section in $\mathfrak{p}$-adic fields.

Exercise 1.3.4. If $\mathfrak{p}$ and $\mathfrak{q}$ are distinct nonzero prime ideals in $\mathcal{O}_F$, check that the valuations $v_\mathfrak{p}$ and $v_\mathfrak{q}$ are not equivalent.

This partly justifies the use of the term prime for an equivalence class of absolute values—this says that each distinct prime ideal $\mathfrak{p}$ gives rise to an equivalence class v of absolute values. We will often abuse notation and write $v = \mathfrak{p}$ for the nonarchimedean prime/place of F obtained from the prime ideal $\mathfrak{p}$.

What about archimedean absolute values? In number theory, it's standard to define these in terms of the real and complex absolute values. On $\mathbb{R}$, the **real absolute value** $|a|_\mathbb{R}$ is just the usual absolute value, so $|a|_\mathbb{R} = \max\{a, -a\}$. On $\mathbb{C}$, the **complex absolute value** is $|z|_\mathbb{C} = |N_{\mathbb{C}/\mathbb{R}}(z)|_\mathbb{R} = x^2 + y^2$ if $z = x + iy$, $x, y \in \mathbb{R}$. We use the complex absolute value because we like working with absolute values along extensions which are compatible with the norm, in the sense that $|a|_K = |N_{K/F}(a)|_F$. Note that the complex absolute value is just the square of the usual absolute value on $\mathbb{C}$, and hence they are equivalent.

Example 1.3.3. Let σ be an embedding of F into $\mathbb{R}$ (resp. $\mathbb{C}$). Then $|a|_\sigma = |\sigma(a)|_\mathbb{R}$ (resp. $|\sigma(a)|_\mathbb{C}$) is an archimedean absolute value on F.

Exercise 1.3.5. (a) Check that if σ and σ' are different embeddings of F into $\mathbb{R}$ then $|\cdot|_\sigma$ and $|\cdot|_{\sigma'}$ are not equivalent.

(b) Check that if σ and σ' are embeddings of F into $\mathbb{C}$ then $|\cdot|_\sigma$ and $|\cdot|_{\sigma'}$ are equivalent if and only if $\sigma' = \sigma$ or $\sigma' = \overline{\sigma}$, where the bar denotes complex conjugation.

It turns out these are essentially the only absolute values on F. While it's not logically important for us that there are no other absolute values, this result is philsophically reassuring for what we will do:

Theorem 1.3.1 (Ostrowski)**.** *Any nontrivial absolute value on a number field F is equivalent to either a p-adic absolute value $v_\mathfrak{p}$ for some prime ideal $\mathfrak{p}$ of $\mathcal{O}_F$ or an archimedean absolute value $|\cdot|_\sigma$ where σ is a real or complex embedding of F.*

Proof. Combine [Neu99, Prop II.3.7] or [RV99, Thm 4-30] with [Neu99, Prop II.8.1] or [RV99, Prop 4-31]. □

Ostrowski's theorem is often just stated for $F = \mathbb{Q}$, and the version for general number fields is deduced by studying absolute values along extension fields K/F (e.g., this is how

it's done in [Neu99], where it's not even called Ostrowski's theorem, something else is). The nonarchimedean valuations on F are all discrete.

Combining Ostrowski's theorem with the above exercises, one has

Corollary 1.3.2. *The nonarchimedean places v of F are in 1-1 correspondence with the prime ideals of $\mathcal{O}_F$. The archimedean places v of F are in 1-1 correspondence with the set of real embeddings of F union the set of complex conjugacy classes of complex embeddings of F.*

In particular, if F has r real embedddings and $2s$ complex embeddings (so $[F : \mathbb{Q}] = r + 2s$), then F has $r + s$ distinct archimedean places. For instance, an imaginary quadratic field has 1 archimedean place, whereas a real quadratic field has 2.

The point of understanding absolute values/valuations on F is that the different absolute values yield the reasonable ways to measure size for doing geometry and arithmetic on F. It turns out that for many important questions in number theory, we can reduce our problems to understanding how the problems behave for each absolute value, and putting all of our results together. This idea (which fails for some problems) is called the **local-global principle** (or **Hasse principle**). For example, the Hasse–Minkowski theorem (Theorem 3.4.1) says that a quadratic form (e.g., $5x^2 - 3xy + 17y^2$) nontrivially represents 0 if and only if it does in each $\mathbb{Q}_p$ and in $\mathbb{R}$. The fields $\mathbb{Q}_p$ correspond to the p-adic absolute values and $\mathbb{R}$ corresponds to the unique (up to equivalence) archimedean absolute value on $\mathbb{Q}$.

We call the (equivalence classes of) p-adic valuations $v_\mathfrak{p}$ the **finite primes** (or **finite places**) of F and the (equivalence classes of) archimedean valuations v_σ the **infinite primes** (or **infinite places**) of F. It is common to abuse notation and call our prime ideals $\mathfrak{p}$ finite places and real or complex embeddings σ infinite places.

The letter v will be used for both finite and infinite places, but $\mathfrak{p}$ (or p) will only be used to denote finite primes. (Some authors use $\mathfrak{p}$ for finite and infinite primes.)

By $v < \infty$, we mean v is a finite prime, and by $v|\infty$, we mean v is an infinite prime. In the case of $F = \mathbb{Q}$, where there is only one infinite prime, we often denote it simply by $v = v_\infty = \infty$. We call an infinite prime **real** (resp. **complex**) if it is the equivalence class of a real (resp. complex) embedding σ).

Now we can try to complete our justification of why we call (classes) of absolute values primes. Local-global principles (say for $\mathbb{Q}$) suggest that one can (at least to some extent) treat the fields $\mathbb{Q}_p$ and $\mathbb{R}$ on an equal footing, and this is one thing we are trying to do by looking at classes of valuations/absolute values (and one of the goals of using adeles). If we think of $\mathbb{Q}_p$ as corresponding to the valuation v_p, and thus the prime number or ideal p or $p\mathbb{Z}$, then the analogous object attached to $\mathbb{R}$ would be the "valuation" v_∞, i.e., the embedding $\sigma : \mathbb{Q} \to \mathbb{R}$, which we want to think of on a similar footing as a prime.[17]

[17] If you're wondering about why we also say "place," this is motivated by geometric analogies. Namely, if an algebraic curve (or more generally a "scheme") X has a coordinate ring A, the (0-dimensional) points of X correspond to the maximal ideals of A. If $A = \mathbb{Z}$, the maximal ideals are just the nonzero prime ideals $p\mathbb{Z}$, and the points of X (called $\operatorname{Spec}\mathbb{Z}$ in this case) can be thought of as the nonzero primes p. (In this particular geometric analogy, one does not see the infinite primes.) One can think of number theory as doing geometry over these weird 0-dimensional "curves" like $X = \operatorname{Spec}\mathbb{Z}$, and taking an equation mod p (or

Now we make precise the connection between places of a number field like $\mathbb{Q}$ and the extensions $\mathbb{Q}_p$ and $\mathbb{R}$. From now on, we assume all valuations and absolute values are non-trivial.

Given an absolute value $|\cdot|$ on an arbitrary field F, we get a distance function on F by

$$d(a,b) = |a-b|,$$

which makes F into a metric space, and the open sets are generated by open balls $B_x(r) = \{a \in F : |x-a| < r\}$ for $r \in \mathbb{R}_{\geq 0}$. The actual distance depends upon a normalization of the absolute value, i.e., the actual absolute value used rather than just the equivalence class, but it is easy to see that the topology only depends on the equivalence class of $|\cdot|$.

If v is the place associated to $|\cdot|$, define the **completion** F_v to be the (metric) completion (in the sense of Cauchy sequences) of F with respect to v. Thus the various completions of $\mathbb{Q}$ are precisely the set of $\mathbb{Q}_p$ for p prime (Exercise 1.2.7) and $\mathbb{Q}_\infty = \mathbb{R}$. In particular, $\mathbb{Q}$ has one real place and no complex places. For any number field F, $F_v = \mathbb{R}$ for v a real place and $F_v = \mathbb{C}$ for v a complex place, whereas the nonarchimedean completions F_v are p-adic fields:

Proposition 1.3.3. *Let F be a number field, and $\mathfrak{p}$ be prime ideal of $\mathcal{O}_F$ lying above the rational prime p. Then $F_\mathfrak{p}$ is a p-adic field, i.e., a finite extension of $\mathbb{Q}_p$. In fact, $[F_\mathfrak{p} : \mathbb{Q}_p] \leq [F : \mathbb{Q}]$. Moreover, the $\mathfrak{p}$-adic valuation $v_\mathfrak{p}$ and $\mathfrak{p}$-adic absolute value $|\cdot|_\mathfrak{p}$ defined on F agrees with those defined on $F_\mathfrak{p}$.*

Proof. For the first part, $\mathbb{Q}_p$ is the p-adic completion of $\mathbb{Q}$ (Exercise 1.2.7), so $F_\mathfrak{p}$ must contain $\mathbb{Q}_p$, because the restriction of $|\cdot|_\mathfrak{p}$ to $\mathbb{Q}$ is equivalent to $|\cdot|_p$. On the other hand, $F = \mathbb{Q}(\alpha)$ for an algebraic number α. So F contains the $\mathfrak{p}$-adic field $\mathbb{Q}_p(\alpha)$. But $\mathbb{Q}_p(\alpha)$ is complete by Proposition 1.2.13, and therefore we have equality $F_\mathfrak{p} = \mathbb{Q}_p(\alpha)$.

The agreement of $v_\mathfrak{p}$ on F and $F_\mathfrak{p}$ is because $\mathfrak{p}\mathcal{O}_{F_\mathfrak{p}}$ is the unique prime ideal of $\mathcal{O}_{F_\mathfrak{p}}$, which yields a 1-1 correspondence between the ideals $\mathfrak{p}^m \subset \mathcal{O}_F$ and the non-zero ideals $\mathfrak{p}^m\mathcal{O}_{F_\mathfrak{p}}$ of $\mathcal{O}_{F_\mathfrak{p}}$. (Cf. [Neu99, Prop I.11.1], which proves the analogous correspondence between $\mathcal{O}_F$ and its localization $\mathcal{O}_{F,(\mathfrak{p})}$ (see below). As we will explain below, the ideal theories for $\mathcal{O}_{F_\mathfrak{p}}$ and $\mathcal{O}_{F,(\mathfrak{p})}$ are identical.) That the $\mathfrak{p}$-adic absolute values on F and $F_\mathfrak{p}$ agree will then follow from the compatibility of local and global inertia degrees (see Proposition 1.3.6 below). □

Thus the various completions of F are just a collection of p-adic fields parametrized by the prime ideals of F, together with the archimedean completions.

While $F_\mathfrak{p} = \mathbb{Q}_p(\alpha)$ in the proof, we cannot conclude the equality $[F_\mathfrak{p} : \mathbb{Q}_p] = [F : \mathbb{Q}]$ in general.

> **Example 1.3.4.** Let $F = \mathbb{Q}(\sqrt{7})$ and $\mathfrak{p}$ be a prime of F above 3. Then $F_\mathfrak{p} = \mathbb{Q}_3$ because $\sqrt{7} \in \mathbb{Q}_3$ (it suffices to note that 7 is a square mod 3 by Lemma 1.2.11—and technically by $\sqrt{7}$ here I mean an $x \in \mathbb{Q}_3$ such that $x^2 = 7$, rather than the real number $\sqrt{7}$). On the other hand if $K = \mathbb{Q}(\sqrt{5})$ and $\mathfrak{q}$ is a prime of K above 3, then $[K_\mathfrak{q} : \mathbb{Q}_3] = 2$ because 5 is

rather in $\mathbb{Q}_p$) is like examining the local behaviour of a function on X at the point p. Hence the local–global terminology, which also comes from geometric analogies. (Now I wonder if it's just coincidence that we use the letter p both for points and for primes...) But if all this sounds like crazy talk, don't worry, just erase this from your mind. And if it doesn't sound like crazy talk, you should definitely have your head checked.

not a square in $\mathbb{Q}_3$.

The difference in the behavior of $F_\mathfrak{p}$ and $K_\mathfrak{q}$ is reflected in the different ways the rational prime 3 splits in F and K. Specifically, $3\mathcal{O}_F$ is a product of two prime ideals of $\mathcal{O}_F$ where as $3\mathcal{O}_K$ is a prime ideal in $\mathcal{O}_K$, i.e., 3 splits in F but is inert in K. This relationship is explained by the global fundamental identity below (Corollary 1.3.9; cf. Example 1.3.5).

First we will explain how integrality behaves with respect to localization and completion. Understanding this is important to be able to use local methods ($\mathfrak{p}$-adic theory) to questions about integers of number fields.

Assume F is a number field. Recall that for a prime ideal $\mathfrak{p}$ of $\mathcal{O}_F$, the **localization** of $\mathcal{O}_F$ at $\mathfrak{p}$ is

$$\mathcal{O}_{F,(\mathfrak{p})} = \left\{ \frac{a}{b} : a \in \mathcal{O}_F,\, b \in \mathcal{O}_F - \mathfrak{p} \right\} \subset F. \tag{1.3.1}$$

(Here the parentheses around the $\mathfrak{p}$ do not mean the ideal generated by $\mathfrak{p}$ since $\mathfrak{p}$ is already an ideal, so when $F = \mathbb{Q}$ to be consistent you should write $\mathbb{Z}_{((p))}$ for the localization of $\mathbb{Z}$ at (p). In practice, however, one just writes $\mathbb{Z}_{(p)}$. The point of the parentheses is to distinguish the localization $\mathbb{Z}_{(p)}$ from the completion $\mathbb{Z}_p$.[18]) Note that

$$\mathcal{O}_{F,(\mathfrak{p})} = \{x \in F : v_\mathfrak{p}(x) \geq 0\}.$$

Proposition 1.3.4. *The completion of $\mathcal{O}_{F,(\mathfrak{p})}$ with respect to $v_\mathfrak{p}$ is the ring of $\mathfrak{p}$-adic integers $\mathcal{O}_{F_\mathfrak{p}}$[19] inside $F_\mathfrak{p}$, and $\mathcal{O}_{F_\mathfrak{p}} \cap F = \mathcal{O}_{F,(\mathfrak{p})}$.*

Proof. The completion of $\mathcal{O}_{F,(\mathfrak{p})}$ is the same as the closure of $\mathcal{O}_{F,(\mathfrak{p})}$ inside $F_\mathfrak{p}$. Note $\mathcal{O}_{F,(\mathfrak{p})} = \{x \in F : |x|_\mathfrak{p} \leq 1\}$ so the closure of $\mathcal{O}_F$ is contained in $\mathcal{O}_{F_\mathfrak{p}} = \{x \in F_\mathfrak{p} : |x|_\mathfrak{p} \leq 1\}$ by continuity of $|\cdot|_\mathfrak{p}$. Since $x \in F - \mathcal{O}_{F,(\mathfrak{p})}$ implies $|x|_\mathfrak{p} \geq q > 1$, the closure of $\mathcal{O}_{F,(\mathfrak{p})}$ must be all of $\mathcal{O}_{F_\mathfrak{p}}$ since F is dense in $F_\mathfrak{p}$.

The latter statement follows as $\mathcal{O}_{F_\mathfrak{p}} \cap F = \{x \in F : v_\mathfrak{p}(x) \geq 0\}$. □

In other words, to get from a global ring of integers $\mathcal{O}_F$ to a local ring of integers $\mathcal{O}_{F_\mathfrak{p}}$, one can take the localization at $\mathfrak{p}$ and then the completion with respect to the $\mathfrak{p}$-adic valuation. That is, the localization $\mathcal{O}_{F,(\mathfrak{p})}$ is dense in $O_{F_\mathfrak{p}}$, analogous to how F is dense in $F_\mathfrak{p}$. This is also true for $\mathcal{O}_F$ itself.

Exercise 1.3.6. Show $\mathcal{O}_F$ is dense in the $\mathfrak{p}$-adic topology on $\mathcal{O}_{F_\mathfrak{p}}$.

We can also consider localizations and completions for ideals. Say $\mathcal{I} = \mathfrak{p}^m\mathcal{J}$ is an integral ideal in $\mathcal{O}_F$ such that $\mathfrak{p} \nmid \mathcal{J}$. Then we can "localize" our ideal and pass to completion to get

$$\mathcal{I}\mathcal{O}_{F,(\mathfrak{p})} = \mathfrak{p}^m\mathcal{O}_{F,(\mathfrak{p})}, \quad \mathcal{I}_\mathfrak{p} := \mathcal{I}\mathcal{O}_{F_\mathfrak{p}} = \mathfrak{p}^m\mathcal{O}_{F_\mathfrak{p}}. \tag{1.3.2}$$

[18] This distinction between $\mathcal{O}_{F,\mathfrak{p}}$ and $\mathcal{O}_{F,(\mathfrak{p})}$ is important for number theorists but not a concern for most other mathematicians, so in algebra books it's common to see the notation $R_\mathfrak{p}$ for the localization of a ring R at an ideal $\mathfrak{p}$ (or worse, $R_{R\setminus\mathfrak{p}}$), just like many people use $\mathbb{Z}_p$ for $\mathbb{Z}/p\mathbb{Z}$. (I suppose such people would use $\mathbb{Z}_{(p)}$ to denote the localization of $\mathbb{Z}$ at $p\mathbb{Z}$.) If you're one of the people who do either of these things, stop immediately.

[19] To avoid double or higher subscripts, some people write $\mathcal{O}_{F,\mathfrak{p}}$ instead of $\mathcal{O}_{F_\mathfrak{p}}$. I might on occasion do this if I feel subscripts are getting out of hand.

This follows because the ideal theory of $\mathcal{O}_{F,(\mathfrak{p})}$ is the same as the ideal theory of $\mathcal{O}_{F_\mathfrak{p}}$. Namely $\mathcal{O}_{F,(\mathfrak{p})}$ is a DVR with prime ideal $\mathfrak{p}\mathcal{O}_{F,(\mathfrak{p})}$, and the nonzero fractional ideals are precisely

$$\cdots \supset \mathfrak{p}^{-1}\mathcal{O}_{F,(\mathfrak{p})} \supset \mathcal{O}_{F,(\mathfrak{p})} \supset \mathfrak{p}\mathcal{O}_{F,(\mathfrak{p})} \supset \mathfrak{p}^2\mathcal{O}_{F,(\mathfrak{p})} \supset \cdots,$$

and if $\mathfrak{P} = \mathfrak{p}\mathcal{O}_{F,(\mathfrak{p})}$ is the unique (nonzero) prime ideal in $\mathcal{O}_{F,(\mathfrak{p})}$ then $\mathfrak{P}\mathcal{O}_{F_\mathfrak{p}}$ is the unique (nonzero) prime ideal in $\mathcal{O}_{F_\mathfrak{p}}$ (in fact, the same argument for Proposition 1.3.4 shows the prime ideal of $\mathcal{O}_{F_\mathfrak{p}}$ is the $\mathfrak{p}$-adic completion of $\mathfrak{P}$). (See, e.g., [CR06, Sec 19] or [Neu99, Sec I.11] and [Neu99, Sec II.4].)

A consequence of the correspondence (1.3.2) is a description of our $\mathfrak{p}$-adic valuations restricted to F in terms of global ideal factorization:

Corollary 1.3.5. *Let $x \in F^\times$ and write $x\mathcal{O}_F = \prod \mathfrak{p}_i^{m_i}$ where $m_i \in \mathbb{Z}$. Then $v_{\mathfrak{p}_i}(x) = m_i$.*

We remark we can try something similar for archimedean absolute values, but there there is no corresponding prime ideal to localize at. Instead, one can just look at completions of $\mathcal{O}_F$ with respect to archimedean valuations. For instance, when $F = \mathbb{Q}$ the completion of $\mathbb{Z}$ in $\mathbb{Q}_\infty = \mathbb{R}$ is just $\mathbb{Z}$ and when $F = \mathbb{Q}(\sqrt{2})$, the completion of $\mathcal{O}_F = \mathbb{Z}[\sqrt{2}]$ in $\mathbb{R}$ is $\mathbb{R}$. In general, $\mathcal{O}_F$ will either be dense or discrete in $\mathbb{R}$ or $\mathbb{C}$. To get a uniform archimedean theory, we should view $\mathcal{O}_F \subset F \subset \prod_{v|\infty} F_v$, which will be a $[F:\mathbb{Q}]$-dimensional $\mathbb{R}$-vector space V. In this case $\mathcal{O}_F$ is always discrete in V, and we will briefly discuss this again in Section 1.4.

Extensions of number fields

A basic question in algebraic number theory is: how do primes behave along extensions of number fields? In the introduction, we pointed out the connection between this problem for $\mathbb{Q}(i)/\mathbb{Q}$ and the representation of numbers as a sum of two squares. Here we will just summarize the main points for extensions of $\mathbb{Q}$ for simplicity of exposition, but the theory extends analogously to arbitrary number field extensions K/F.

Fix the following notation for the next few results. Say $[F:\mathbb{Q}] = n$ and fix a rational prime p. Let $p\mathcal{O}_F = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$ be the prime ideal factorization in $\mathcal{O}_F$. We call e_i the **ramification index** of $\mathfrak{p}_i$ (over p).

Proposition 1.3.6 (Compatibility with localizations)**.** *Denote by $\mathfrak{P}_i$ the unique prime ideal in $\mathcal{O}_{F_{\mathfrak{p}_i}}$. Then*

(a) $\mathcal{O}_{F_{\mathfrak{p}_i}}/\mathfrak{P}_i \simeq \mathcal{O}_F/\mathfrak{p}_i$.

(b) [compatibility of ramification indices] $F_{\mathfrak{p}_i}/\mathbb{Q}_p$ is an extension of p-adic fields with ramification index e_i, i.e., $p\mathcal{O}_{F_{\mathfrak{p}_i}} = \mathfrak{P}_i^{e_i}$.

(c) [compatibility of inertia degrees] If f_i is the inertia degree of $F_{\mathfrak{p}_i}/\mathbb{Q}_p$, then also $\mathcal{O}_F/\mathfrak{p}_i$ is a finite field of size p^{f_i}.

Proof. For (a), see [Neu99, Prop II.4.3]. For (b), we use the correspondence between ideals of $\mathcal{O}_F$ and ideals of $\mathcal{O}_{F_\mathfrak{p}}$ from (1.3.2). Lastly, note (c) is an immediate consequence of (a). □

Corollary 1.3.7. *Let $x \in F$. Then $\prod_{v|p} |x|_v = |N_{F/\mathbb{Q}}(x)|_p$ for any prime p.*

This is a statement about compatibility of p-adic absolute values with norms. The product on the left means over all prime ideals of $\mathcal{O}_F$ above p.

Proof. Note if $x = 0$, then both sides are 0, so take $x \neq 0$. Say $x\mathcal{O}_F = \prod \mathfrak{p}_i^{m_i}$ where the $\mathfrak{p}_i$'s are distinct prime ideals of $\mathcal{O}_F$ and $m_i \in \mathbb{Z}$. Let p_i be the rational prime under $\mathfrak{p}_i$ (so the p_i's need not be distinct), and say $|N_{F/\mathbb{Q}}(\mathfrak{p}_i)| = \#\mathcal{O}_F/\mathfrak{p}_i = p_i^{f_i}$, where the f_i's are global inertial degrees. Then $|N_{F/\mathbb{Q}}(x)|_p = \prod_{p_i=p} p^{m_i f_i}$. On the other hand, we have $|x|_{\mathfrak{p}_i} = q_i^{m_i}$ where $q_i = p_i^{f_i}$ with the f_i's now being the local inertia degrees. Hence (c) of the above proposition (i.e., that the locally and globally defined f_i's are the same) yields the desired equality. □

Recall the local fundamental identity (1.2.6) tells us

$$n_i := [F_{\mathfrak{p}_i} : \mathbb{Q}_p] = e_i f_i.$$

There is an important global analogue. The all-powerful Chinese Remainder Theorem yields:

Proposition 1.3.8. *We have*

$$F_p := F \otimes_{\mathbb{Q}} \mathbb{Q}_p \simeq F_{\mathfrak{p}_1} \oplus \cdots \oplus F_{\mathfrak{p}_g}$$

and

$$\mathcal{O}_{F_p} := \mathcal{O}_F \otimes_{\mathbb{Z}} \mathbb{Z}_p \simeq \mathcal{O}_{F_{\mathfrak{p}_1}} \oplus \cdots \oplus \mathcal{O}_{F_{\mathfrak{p}_g}}.$$

Proof. See [Neu99, Prop II.8.3] for the first statement. The second is similar, and can be deduced from the first ([Neu99, Exer II.8.4].) □

Since $F \otimes_{\mathbb{Q}} \mathbb{Q}_p$ has dimension n as a $\mathbb{Q}_p$-vector space (Corollary 1.1.9), the above proposition immediately yields the (first part of the) desired

Corollary 1.3.9 (Global fundamental identity)**.** *We have $n = \sum_{i=1}^{g} e_i f_i$. Moreover, if $F/\mathbb{Q}$ is Galois, then $e_1 = \cdots = e_g = e$ and $f_1 = \cdots f_g = f$ for some e, f, and $n = efg$.*

The reason things are simpler in the Galois case is because then $\mathrm{Gal}(F/\mathbb{Q})$ acts transitively on the primes of F above p—see [Neu99, Sec II.9]. One can also prove this without resorting to local methods.

We say p **splits** in F if $g > 1$ and p is **totally split** if $g = n$. If $p\mathcal{O}_F = \mathfrak{p}$ is prime, we say p is **inert** in F. We remark that if p is split in F, we can never have $[F_{\mathfrak{p}} : \mathbb{Q}_p] = n$. In fact if p is totally split, then we see $F_{\mathfrak{p}_1} \simeq \cdots \simeq F_{\mathfrak{p}_n} \simeq \mathbb{Q}_p$. Note p being inert means $N(\mathfrak{p}) = p^n$, so is equivalent to $f = n$. This explains the terminology inertia degree for f.

If some $e_i > 1$, we say p is **ramified** in F, i.e., if and only if some $F_{\mathfrak{p}_i}/\mathbb{Q}_p$ is ramified; otherwise p is **unramified**. Note that any prime which is not split or inert must be ramified, though in general ramified primes can be split as well (but not totally split). However, we can at least say there are only finitely many ramified primes. In fact, they can be easily determined:

Proposition 1.3.10. *Let $p \in \mathbb{Z}$ be prime. Then p is ramified in F if and only if $p|\Delta_F$, where Δ_F denotes the discriminant of F.*

Proof. See [Neu99, Cor III.2.12]. □

For a quadratic field $F = \mathbb{Q}(\sqrt{d})$ of discriminant d, we can easily determine the splitting type of p with the quadratic residue symbol: p is inert if and only if $\left(\frac{d}{p}\right) = -1$ and p is split if and only if $\left(\frac{d}{p}\right) = 1$. The following example shows how to classify the primes of a quadratic field.

Example 1.3.5. Let $F = \mathbb{Q}(\sqrt{d})$ be a quadratic field of discriminant d. Then, by the fundamental identity, there are three distinct possibilities for the prime decomposition of $p\mathcal{O}_F$: (i) $p\mathcal{O}_F = \mathfrak{p}$ is prime, (ii) $p\mathcal{O}_F = \mathfrak{p}\mathfrak{q}$ where $\mathfrak{p}, \mathfrak{q}$ are distinct primes, and (iii) $p\mathcal{O}_F = \mathfrak{p}^2$. The latter case means p is ramified, and only happens when $p|d$; p is unramified in the first two cases.

Case (i) means p is inert so $\mathcal{O}_F/\mathfrak{p} \simeq \mathbb{F}_{p^2}$ and $[F_\mathfrak{p} : \mathbb{Q}_p] = 2$. In fact, $F_\mathfrak{p}$ must be the unramified quadratic extension of $\mathbb{Q}_p$. Case (ii) means p is *unramified* or *split*, and $\mathcal{O}_F/\mathfrak{p} \simeq \mathcal{O}_F/\mathfrak{q} \simeq \mathbb{F}_p$, so $F_\mathfrak{p} \simeq F_\mathfrak{q} \simeq \mathbb{Q}_p$. Lastly, in case (iii) $\mathcal{O}_F/\mathfrak{p} \simeq \mathbb{F}_p$ and $[F_\mathfrak{p} : \mathbb{Q}_p] = 2$. Here $F_\mathfrak{p}$ is one of the (2 if p is odd; 6 is $p = 2$) ramified quadratic extensions of $\mathbb{Q}_p$.

Since any prime $\mathfrak{p}$ of F lies above some prime $p\mathbb{Z}$ of $\mathbb{Z}$, this classifies the prime ideals of F, and consquently the finite places of F. If $d > 0$, then F is real quadratic and there are 2 infinite (real) places; if $d < 0$, then F is imaginary quadratic and there is 1 infinite (complex) place.

Exercise 1.3.7. Explicitly classify (using congruence conditions) the primes of $F = \mathbb{Q}(i)$. For each finite prime $\mathfrak{p}$ of $\mathbb{Q}(i)$, describe $F_\mathfrak{p}$, including its degree over the appropriate $\mathbb{Q}_p$ and the associated inertia degree and ramification index.

Exercise 1.3.8. Suppose $F/\mathbb{Q}$ is a Galois extension of degree 3. Determine the possible ways for $p\mathcal{O}_F$ to decompose and compute the size of the associated residue fields in each case.

1.4 Commutative orders and ideals

Let F be a number field, which we can regard as a finite-dimensional vector space over $\mathbb{Q}$.

A **($\mathbb{Z}$-)lattice** in F is a subset $\Lambda \subset F$ of the form

$$\Lambda = \{x_1\alpha_1 + \cdots + x_n\alpha_n : x_i \in \mathbb{Z}\}$$

for some finite subset $\{\alpha_1, \ldots, \alpha_n\} \subset F$. We call $\{\alpha_1, \ldots, \alpha_n\}$ a **generating set** for Λ, and further say it is a **$\mathbb{Z}$-basis** if $\alpha_1, \ldots, \alpha_n$ are linearly independent over $\mathbb{Z}$. Equivalently, a lattice in F is a finitely-generated additive subgroup of F. Equivalently, a lattice in F is a finitely-generated (free) $\mathbb{Z}$-submodule of F. (Note that any $\mathbb{Z}$-module inside F must be free as F has no torsion elements.) Then a $\mathbb{Z}$-basis for Λ is the same as a basis for Λ as a free $\mathbb{Z}$-module, whence bases exist and they all have the same dimension. We will use the description as a finitely-generated module to give a more general definition of lattices over more rings in Section 4.2.

Example 1.4.1. For any F, $\mathbb{Z}$ and $\mathbb{Z}[\frac{1}{2}]$ are lattices in F.

There is a fundamental difference between the lattice $\mathbb{Z}$ in $\mathbb{Q}$ and the lattice $\mathbb{Z}$ in another number field such as $\mathbb{Q}(i)$. Namely $\mathbb{Z}$ "fills out" $\mathbb{Q}$ but not $\mathbb{Q}(i)$ in the sense of dimension, i.e., $\mathbb{Q}\mathbb{Z} = \mathbb{Q}$ but $\mathbb{Q}\mathbb{Z} \neq \mathbb{Q}(i)$.

We say a lattice Λ in F is **complete** (or **full**) if $\mathbb{Q}\Lambda = F$, in other words, if a $\mathbb{Z}$-basis for Λ is a $\mathbb{Q}$-basis for F, i.e., if Λ is a free $\mathbb{Z}$-module of rank $[F : \mathbb{Q}]$. We remark some authors include the completeness condition in their definition of lattices.

Example 1.4.2. The ring of integers $\mathcal{O}_F$ is a complete lattice in F. So is $\lambda\mathcal{O}_F$ for any nonzero $\lambda \in F^\times$.

Note, if $F = \mathbb{Q}(\sqrt{-d})$ is an imaginary quadratic field, then we can draw $\mathcal{O}_F$ as a subset of $\mathbb{C} \simeq \mathbb{R}^2$, and we will get a lattice in the plane in the usual geometric sense (e.g., think about $\mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-3})$; cf. Fig. 1.4.1). More generally, let $\sigma_1, \dots, \sigma_m$ denote a set of representatives for the real and complex embeddings of F, so each represents an infinite place v_i of F. If we visualize $\mathcal{O}_F$ in $F \subset \prod_{i=1}^m F_{v_i} \simeq_{\mathbb{R}} \mathbb{R}^{[F:\mathbb{Q}]}$ via $x \mapsto (\sigma_1(x), \cdots, \sigma_m(x))$, then $\mathcal{O}_F$ is again a lattice in the usual geometric sense. This is the starting point for Minkowski's *geometry of numbers*, which leads to the usual classical proof of the finiteness of the class group.

An **order** in F is a complete lattice $\mathcal{O} \subset F$ which is also a subring of F. Clearly $\mathcal{O}_F$ is always an order in F. Here's another example.

Example 1.4.3. Let $d \neq 1$ be a squarefree integer. Then $F = \mathbb{Q}(\sqrt{d})$ is a quadratic field and $\mathbb{Z}[\sqrt{d}]$ is an order F. Recall that the discriminant Δ_F of F is d if $d \equiv 1 \bmod 4$ and $4d$ else, and the ring of integers $\mathcal{O}_F$ is $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ in the former case and $\mathbb{Z}[\sqrt{d}]$ in the latter. Hence we always have $\mathbb{Z}[\sqrt{d}] \subset \mathcal{O}_F$, but we do not have equality in general.

This sort of example provides one type of motivation for looking at general orders, rather than just rings of integers. For instance, if we want to solve $x^2 + 3y^2 = n$ over $\mathbb{Z}$, that means we want an element $\alpha = x + y\sqrt{-3} \in \mathbb{Z}[\sqrt{-3}]$ whose norm is n, rather than just an α in the whole ring of integers $\mathcal{O}_F = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$, where $F = \mathbb{Q}(\sqrt{-3})$, such that $N(\alpha) = n$.

However, our main motivation for studying orders is we want to extend the arithmetic theory to noncommutative algebras, where the notion of ring of integers breaks down. Though we will develop the theory of orders in our algebras from scratch, it seems like a good idea to at least briefly discuss orders are in the more familiar case of number fields first.

Proposition 1.4.1. *Let $\mathcal{O}$ be an order in F. Then $\mathcal{O}$ is a subring of $\mathcal{O}_F$.*

We will prove this in greater generality in Proposition 4.2.2, but if you want, you can do this case as an exercise.

Exercise 1.4.1. Prove the above proposition. (Hint: Think about the case $F = \mathbb{Q}$ first.)

Corollary 1.4.2. *Let $\mathcal{O}$ be an order in F. Then $[\mathcal{O}_F : \mathcal{O}] < \infty$.*

Proof. Note that $\mathcal{O}$ and $\mathcal{O}_F$ are free $\mathbb{Z}$-modules of the same rank $[F : \mathbb{Q}]$. Now apply Proposition 1.1.6. □

Consequently, $\mathcal{O}_F$ is the (unique) maximal order in F. When we discuss orders in algebras later, we will see that there may be many different maximal orders (given two orders, there need not be an order containing both of them).

What do the orders look like in general? By the above results, we can characterize the orders in F as the collections of subrings $\mathcal{O}$ of $\mathcal{O}_F$ such that $\mathbb{Q}\mathcal{O} = F$, i.e., the subrings $\mathcal{O}$ of $\mathcal{O}_F$ of full rank (= rank of $\mathcal{O}_F$) as a $\mathbb{Z}$-module, i.e., the subrings $\mathcal{O}$ of $\mathcal{O}_F$ that are of finite index as abelian groups (again, by Proposition 1.1.6).

If $F = \mathbb{Q}$, then $\mathcal{O}_F = \mathbb{Z}$ is the only order by the above proposition, as any order must contain $\mathbb{Z}$.

Proposition 1.4.3. *Let F be a quadratic field. Then the orders in F are exactly those of the form*

$$\mathcal{O} = \mathbb{Z} + f\mathcal{O}_F,$$

for $f \in \mathbb{N}$.

Proof. It is easy to check that a subset form $\mathbb{Z} + f\mathcal{O}_F$ is an order. Now, if $\mathcal{O}$ is any order, put $f = [\mathcal{O}_F : \mathcal{O}]$. Note that $f\mathcal{O}_F \subset \mathcal{O}$, thus $\mathcal{O} \supset \mathbb{Z} + f\mathcal{O}_F$. Now just check $\mathbb{Z} + f\mathcal{O}_F$ has index f in $\mathcal{O}_F$, so this must equal $\mathcal{O}$. □

Ideal theory is quite nice for rings of integers $\mathcal{O}_F$, e.g., integral ideals have unique factorization into prime ideals, and the nonzero fractional ideals form a group which measures the failure of unique factorization in $\mathcal{O}_F$. Here we want to see what happens if we consider *non-maximal* orders $\mathcal{O}$ such as $\mathbb{Z}[\sqrt{-3}] \subset \mathbb{Q}(\sqrt{-3})$. Some references are [Cox13] for quadratic fields and [Neu99] in general.

Let $\mathcal{O}$ be an order in F. Then an **(integral) ideal** *in* $\mathcal{O}$ is an additive subgroup $\mathcal{I}$ of $\mathcal{O}$ such that $\mathcal{O}\mathcal{I} = \mathcal{O}$, i.e., $\mathcal{I}$ is a $\mathcal{O}$-submodule of $\mathcal{O}$ (viewing $\mathcal{O}$ as a module over itself). We note that, like $\mathcal{O}_F$, the (integral) prime ideals are precisely the maximal ideals.

Proposition 1.4.4. *Let $\mathcal{O}$ be an order in F. Then every (nonzero) prime ideal in $\mathcal{O}$ is maximal (aka, $\mathcal{O}$ has* Krull dimension one*).*

Proof. Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}$. Then, as a $\mathbb{Z}$-lattice (or free $\mathbb{Z}$-module), $\mathfrak{p}$ has the same rank as $\mathcal{O}$ (if $\alpha_1, \dots, \alpha_n$ is a $\mathbb{Z}$-basis for $\mathcal{O}$ and $x \in \mathfrak{p}$ is nonzero, then $x\alpha_1, \dots, x\alpha_n$ are linearly independent elements of $\mathfrak{p}$). Hence $\mathcal{O}/\mathfrak{p}$ is finite by Proposition 1.1.6. Recall $\mathfrak{p}$ being prime means $\mathcal{O}/\mathfrak{p}$ is an integral domain. Since all finite integral domains are fields, we conclude $\mathfrak{p}$ is maximal. □

A **(fractional) ideal** *of* $\mathcal{O}$ is a subset of F of the form $\lambda\mathcal{I}$ where $\mathcal{I}$ is an integral ideal in $\mathcal{O}$ and $\lambda \in F$. So every integral ideal is a fractional ideal. If we just say "ideal" without specifying fractional or integral, then by default we mean the more general fractional ideal, unless it is clear we are working with only integral ideals, or we say something like "ideal *in* $\mathcal{O}$," which implies integral ideal. We sometimes say $\mathcal{O}$-ideal for a (fractional or integral) ideal of $\mathcal{O}$ to specify the order $\mathcal{O}$.

Exercise 1.4.2. Check that the fractional ideals of $\mathcal{O}$ are precisely the finitely generated $\mathcal{O}$-submodules of F.

Of course the reason for introducing fractional ideals is to get a group structure on ideals. Recall the product $\mathcal{I}\mathcal{J}$ of two ideals $\mathcal{I}$ and $\mathcal{J}$ is the ideal generated by elements of the form $\alpha\beta$ where $\alpha \in \mathcal{I}$ and $\beta \in \mathcal{J}$. Explicitly, $\mathcal{I}\mathcal{J}$ is the collection of finite sums of such elements. We say an $\mathcal{O}$-ideal $\mathcal{I}$ is **invertible** (over $\mathcal{O}$) if there exists an $\mathcal{O}$-ideal $\mathcal{I}^{-1}$ such that $\mathcal{I}\mathcal{I}^{-1} = \mathcal{O}$. For instance, $\lambda\mathcal{O}$ is invertible with inverse $\lambda^{-1}\mathcal{O}$ for any $\lambda \in F^\times$.

Let $J(\mathcal{O})$ be the collection of all invertible ideals in $\mathcal{O}$.

Exercise 1.4.3. Check that, if $\mathcal{I}$ is invertible,

$$\mathcal{I}^{-1} = \{\alpha \in F : \alpha\mathcal{I} \subseteq \mathcal{O}\},$$

and show that $J(\mathcal{O})$ is an abelian group.

If $\mathcal{O} = \mathcal{O}_F$, then any nonzero ideal is invertible. However, this is not true for non-maximal orders.

Example 1.4.4. Let $F = \mathbb{Q}(\sqrt{-3})$ and $\mathcal{O} = \mathbb{Z}[\sqrt{-3}]$. Recall $\mathcal{O}_F = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$. Consider the ideal $\mathcal{I} = (1+\sqrt{-3}, 2)$ in $\mathcal{O}$ (see Fig. 1.4.1). Let $\alpha = a + b\sqrt{-3} \in F$. Then $\alpha\mathcal{I} \subset \mathcal{O}$ if and only if $2\alpha \in \mathcal{O}$ and $(1+\sqrt{-3})\alpha \in \mathcal{O}$, which happens if and only if $a, b \in \frac{1}{2}\mathbb{Z}$ with $2a \equiv 2b \bmod 2$, i.e., if and only if $\alpha \in \mathcal{O}_F$. So if $\mathcal{I}$ has an inverse $\mathcal{I}^{-1}$ then we need $\mathcal{I}^{-1} \subset \mathcal{O}_F$ (in fact, the above exercise says that we would have $\mathcal{I}^{-1} = \mathcal{O}_F$). However, since $\mathcal{I} = 2\mathcal{O}_F$, we see $\mathcal{I}\mathcal{I}^{-1} \subset 2\mathcal{O}_F\mathcal{O}_F = 2\mathcal{O}_F = \mathcal{I} \neq \mathcal{O}$, whence $\mathcal{I}$ is not invertible.

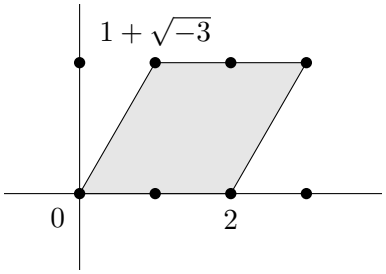
Still, one can give a local characterization of invertibility. To do this, we need to understand how to localize orders.

Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}$. Then, as in the case of rings of integers in (1.3.1), we can consider the **localization** of $\mathcal{O}$ at $\mathfrak{p}$ given by

$$\mathcal{O}_{(\mathfrak{p})} = \left\{\frac{a}{b} \in F : a \in \mathcal{O},\, b \in \mathcal{O} - \mathfrak{p}\right\}. \tag{1.4.1}$$

In general for localizations of integral domains, the ideals of the localization $\mathcal{O}_{(\mathfrak{p})}$ correspond (one-to-one) to the ideals $\mathcal{I}$ of $\mathcal{O}$ divisible by $\mathfrak{p}$ via $\mapsto \mathcal{I}\mathcal{O}_{(\mathfrak{p})}$ ([Neu99, Prop I.11.1]).

Figure 1.4.1: (A fundamental domain for) the ideal $(1+\sqrt{-3}, 2)$ in $\mathbb{Z}[\sqrt{-3}]$



One issue when we don't work with full rings of integers in that the localizations $\mathcal{O}_{(\mathfrak{p})}$ may not be DVRs, because ideals do not always become principal (recall a DVR is not just a ring with a discrete valuation, it is a PID with a unique maximal ideal). In fact, both $\mathcal{O}$ and $\mathcal{O}_{(\mathfrak{p})}$ may not even possess prime factorization of ideals!

Example 1.4.5. We continue with Example 1.4.4. It is easy to algebraically check that $\mathfrak{p} := \mathcal{I} = (1+\sqrt{-3}, 2)$ is a maximal ideal in $\mathcal{O} = \mathbb{Z}[\sqrt{-3}]$ from the description

$$\mathfrak{p} = \left\{a + b\sqrt{-3} \in \mathbb{Z}[\sqrt{-3}] : a \equiv b \bmod 2\right\},$$

and therefore $\mathfrak{p}$ is a prime ideal. One can also visually see this $\mathfrak{p}$ is prime—by looking at the lattice $\mathfrak{p} = \mathcal{I}$, one sees from Fig. 1.4.1 that $\mathcal{O}/\mathfrak{p} = \{0, 1\} \simeq \mathbb{F}_2$. By the exercise below, $\mathfrak{p}$ is the only prime ideal dividing the ideal (2) in $\mathcal{O}$. If we had prime ideal factorization, then $(2) = \mathfrak{p}^e$ for some e. But one readily checks that $\mathfrak{p}^2 = (2+2\sqrt{-3}, 4)$ does not contain 2. Hence $\mathcal{O}$ does not have prime ideal factorization. (This issue does not arise when we pass to the ring of integers $\mathcal{O}_F$ because then $(2) = (1+\sqrt{-3}, 2)$ is already prime—i.e, because $\frac{1+\sqrt{-3}}{2}$ is a unit in $\mathcal{O}_F$.)

Consider the localization $\mathcal{O}_{(\mathfrak{p})}$. From the definition, it is clear that $\mathfrak{p}\mathcal{O}_{(\mathfrak{p})}$ is the unique maximal ideal in $\mathcal{O}_{(\mathfrak{p})}$. Via the correspondence of ideals of $\mathcal{O}_{(\mathfrak{p})}$ with the ideals of $\mathcal{O}$ containing $\mathfrak{p}$ mentioned after (1.4.1), we see $\mathfrak{p}\mathcal{O}_{(\mathfrak{p})} \supsetneq 2\mathcal{O}_{(\mathfrak{p})} \supsetneq (\mathfrak{p}\mathcal{O}_{(\mathfrak{p})})^2$. I.e., also in the localization $\mathcal{O}_{(\mathfrak{p})}$, $2\mathcal{O}_{(\mathfrak{p})}$ does not factor into prime ideals. Therefore $\mathcal{O}_{(\mathfrak{p})}$ is not a PID, and also not a DVR.

Exercise 1.4.4. Show that the only maximal ideal of $\mathbb{Z}[\sqrt{-3}]$ containing the ideal (2) is $(1+\sqrt{-3}, 2)$. (*Unnecessary suggestion:* draw a picture of the lattice $2\mathbb{Z}[\sqrt{-3}]$ and see what a maximal ideal must look like.)

Exercise 1.4.5. Show $\mathfrak{p} = (1+\sqrt{-5}, 2)$ is a prime ideal in $\mathcal{O} = \mathbb{Z}[\sqrt{-5}]$. Show $\mathfrak{p}$ is not principal in $\mathcal{O}$ but becomes principal when we localize, i.e., $\mathfrak{p}\mathcal{O}_{(\mathfrak{p})}$ is principal in $\mathcal{O}_{(\mathfrak{p})}$. What is the difference between this case and Example 1.4.5?

The obstruction to $\mathcal{I}$ being invertible in Example 1.4.4 in $\mathcal{O}$ can be viewed as a local obstruction.

We say an ideal $\mathcal{I}$ of $\mathcal{O}$ is **locally principal** if $\mathcal{I}\mathcal{O}_{(\mathfrak{p})}$ is principal in the localization $\mathcal{O}_{(\mathfrak{p})}$ for every prime ideal $\mathfrak{p}$ of $\mathcal{O}$.

Proposition 1.4.5. *An ideal of $\mathcal{O}$ is invertible if and only if it is locally principal.*

Proof. Suppose $\mathcal{I}$ is an invertible ideal of $\mathcal{O}$. Then we can write $1 = \sum a_i b_i$ where $a_i \in \mathcal{I}$ and $b_i \in \mathcal{I}^{-1}$. For any prime ideal $\mathfrak{p}$, one of the $a_i b_i$'s, say $a_1 b_1$, must not lie in $\mathfrak{p}\mathcal{O}_{(\mathfrak{p})}$, so $a_1 b_1 \in \mathcal{O}_{(\mathfrak{p})}^\times$. Then $\mathcal{I}\mathcal{O}_{(\mathfrak{p})} = a_1\mathcal{O}_{(\mathfrak{p})}$ because, for any $x \in \mathcal{I}$, we have $b_1 x \in \mathcal{I}^{-1}\mathcal{I} = \mathcal{O}$ and therefore

$$x\mathcal{O}_{(\mathfrak{p})} = (a_1 b_1)x\mathcal{O}_{(\mathfrak{p})} = a_1(b_1 x)\mathcal{O}_{(\mathfrak{p})} \subset a_1\mathcal{O}_{(\mathfrak{p})}.$$

Conversely, suppose $\mathcal{I}$ is not invertible. Then $\mathcal{J} = \{x \in F : x\mathcal{I} \subset \mathcal{O}\}$ satisfies $\mathcal{I}\mathcal{J} \subsetneq \mathcal{O}$. Hence there exists a prime ideal $\mathfrak{p}$ of $\mathcal{O}$ such that $\mathfrak{p} \supset \mathcal{I}\mathcal{J}$. Write $\mathcal{I} = \mathbb{Z}\langle a_1, \dots, a_n\rangle$. Suppose $\mathcal{I}$ is locally principal, i.e., there exists $a \in \mathcal{I}$ such that $\mathcal{I}\mathcal{O}_{(\mathfrak{p})} = a\mathcal{O}_{(\mathfrak{p})}$. Then $a_i = a\frac{b_i}{c_i}$ where $b_i \in \mathcal{O}$ and $c_i \in \mathcal{O} - \mathfrak{p}$. We see $c = \prod c_i \in \mathcal{O} - \mathfrak{p}$ satisfies $\frac{c}{a}a_i \in \mathcal{O}$ for each i, and thus $\frac{c}{a} \in \mathcal{J}$. But then $c = a\frac{c}{a} \in \mathcal{I}\mathcal{J} \subset \mathfrak{p}$, a contradiction. □

Given ideals $\mathcal{I}$, $\mathcal{J}$ of $\mathcal{O}$, we say $\mathcal{I}$ and $\mathcal{J}$ are **equivalent** if $\mathcal{J} = \lambda\mathcal{I}$ for some $\lambda \in F^\times$. Geometrically, this means that the lattices $\mathcal{I}$ and $\mathcal{J}$ have the same "shape" and only differ by a scaling factor. Let $J(\mathcal{O})$ denote the set of equivalence classes. The **principal** ideals $P(\mathcal{O})$ are the ideals equivalent to $\mathcal{O}$. Then we define the **(Picard** or **ideal) class group** of $\mathcal{O}$ to be $\mathrm{Cl}(\mathcal{O}) = \mathrm{Pic}(\mathcal{O}) = J(\mathcal{O})/P(\mathcal{O})$, which is the group of invertible ideals modulo equivalence. Of course when $\mathcal{O} = \mathcal{O}_F$, this is the class group of F.

In general, to relate this to the class group of F, we will consider the map

$$\begin{aligned} J(\mathcal{O}) &\to J(\mathcal{O}_F) \\ \mathcal{I} &\mapsto \mathcal{I}\mathcal{O}_F. \end{aligned}$$

Indeed, $\mathcal{I} \mapsto \mathcal{I}\mathcal{O}_F$ defines a map of ideals of $\mathcal{O}$ to ideals of $\mathcal{O}_F$, and since $\mathcal{I}\mathcal{J} = \mathcal{O}$ implies $(\mathcal{I}\mathcal{O}_F)(\mathcal{J}\mathcal{O}_F) = \mathcal{O}_F$, this map invertible ideals to invertible ideals. It is also a group homomorphism, and because principal ideals get sent to principal ideals, this induces a map of class groups:

$$\mathrm{Cl}(\mathcal{O}) \to \mathrm{Cl}(\mathcal{O}_F).$$

Define the **conductor** of $\mathcal{O}$ to be

$$\mathfrak{f} = \mathfrak{f}(\mathcal{O}) = \{\alpha \in \mathcal{O}_F : \alpha\mathcal{O}_F \subseteq \mathcal{O}\}.$$

One easily checks that conductor is the largest $\mathcal{O}_F$-ideal contained in $\mathcal{O}$.

Proposition 1.4.6. *If $\mathfrak{p}$ is a prime ideal of $\mathcal{O}$, then $\mathfrak{p}$ is invertible if and only if $\mathfrak{p} \nmid \mathfrak{f}(\mathcal{O})$. In this case, $\mathfrak{P} = \mathfrak{p}\mathcal{O}_F$ is a prime ideal of $\mathcal{O}_F$ and $\mathcal{O}_{(\mathfrak{p})} = \mathcal{O}_{F,(\mathfrak{P})}$.*

Proof. See [Neu99, Prop I.12.10]. □

We remark that $\mathfrak{p} \nmid \mathfrak{f}(\mathcal{O})$, $\mathcal{O}_{(\mathfrak{p})}$ is a DVR, and we can take the completion to get a local ring, which we denote $\mathcal{O}_{\mathfrak{p}}$ (which is just $\mathcal{O}_{F_{\mathfrak{P}}}$) as in the case of full rings of integers.

When $\mathfrak{p}$ is not invertible, one can still try to take the completion of $\mathcal{O}_{(\mathfrak{p})}$ (or just $\mathcal{O}$) in $F_{\mathfrak{P}}$, but things are not as nice—one issue is that $\mathcal{O}$ need not contain all the units in $\mathcal{O}_F$.

We have the following class number formula for class number of non-maximal orders in terms of maximal ones.

Theorem 1.4.7. *Let $\mathcal{O}$ be an order in F. The class group $\mathrm{Cl}(\mathcal{O})$ is a finite abelian group. Moreover, the* **class number** *$h(\mathcal{O}) = |\mathrm{Cl}(\mathcal{O})|$ of $\mathcal{O}$ is*

$$h(\mathcal{O}) = \frac{1}{[\mathcal{O}_F^\times : \mathcal{O}^\times]} \frac{|(\mathcal{O}_F/\mathfrak{f}(\mathcal{O}))^\times|}{|(\mathcal{O}/\mathfrak{f}(\mathcal{O}))^\times|} h_F,$$

where $h_F = \mathrm{Cl}(\mathcal{O}_F)$ is the class number of F.

Proof. See [Neu99, Thm I.12.12]. □

Of course, a simple description of h_F itself is hard, even for quadratic fields. There is a class number formula for h_F in terms of the residue of the Dedekind zeta function at 1 (which can be expressed in terms of Dirichlet L-values at 1 if F is quadratic, or more generally abelian over $\mathbb{Q}$), a regulator, and some simple quantities. But these quantities are not so easy to understand. For instance, it is an outstanding conjecture if there are infinitely many real quadratic fields of class number 1.

One of our main goals will be to understand analogues of these class number formulas for quaternion algebras (principally, the *Eichler mass formula*). This analogue has deep consequences in the arithmetic of quadratic and modular forms. In some sense, class number for quaternion algebras turn out to be simpler than for number fields.

Exercise 1.4.6. Compute the class number of $\mathbb{Z}[\sqrt{-3}]$.

Exercise 1.4.7. Let $F = \mathbb{Q}(\sqrt{-15})$, so $h_F = 2$. Compute the class number of $\mathcal{O} = \mathbb{Z}[\sqrt{-15}]$. Can you describe the homomorphism $\mathrm{Cl}(\mathcal{O}) \to \mathrm{Cl}(\mathcal{O}_F)$? Is it injective or surjective?

We remark that being invertible is a local property of ideals, but being principal is a strictly global property. That is, we saw we could detect invertibility of ideals in a global order $\mathcal{O}$ by local criteria, however an ideal may be locally principal without being globally principal. Indeed, if not, that would mean $h(\mathcal{O}) = 1$.

1.5 Adeles

We have seen a few aspects in the previous sections of local-global methods in number theory (e.g., Proposition 1.3.6, Corollary 1.3.9, Proposition 1.4.5). Adeles will provide a convenient way to study local-global issues. One application will be to prove finiteness of ideal class groups, though there will be many other applications for us. Note the ideal class group

measures the failure of a local-global principal: every (invertible) ideal is locally principal, and the ideal class group measures how far the ideal classes are from all being (globally) principal.

The idea with adeles is to put the information of all the completions F_v of F together in one object $\mathbb{A}$. The naive thing would just be to consider the infinite direct product $\prod_v F_v$ over all places, but this is too big to be very useful. One smaller object is the infinite direct sum $\bigoplus_v F_v$, which can be viewed as a subset of $\prod_v F_v$ (namely, the subset of elements which are only nonzero at a finite number of coordinates). However, this is too small. For instance, we will want to F to embed in $\mathbb{A}$ in a natural way. Well, F does embed naturally in $\prod_v F_v$, simply via the diagonal embedding

$$x \mapsto (x, x, x, \ldots) \in \prod_v F_v.$$

However this is only contained in the infinite direct sum if $x = 0$. So we want something in between an infinite direct product and an infinite direct sum. This is provided by a construction called the restricted direct product (which was, as far as I know, designed with the adeles in mind), and will give us the adele ring $\mathbb{A}_F$ which lies between $\bigoplus_v F_v$ and $\prod_v F_v$.

We first define it algebraically. Let G_v be a collection of groups for v in some index set V and $H_v \subset G_v$ a collection of subgroups. The **restricted direct product** of G_v's with respect to H_v's is

$$\prod_v{}' G_v = \{(g_v) | g_v \in G_v \text{ for all } v \text{ with } g_v \in H_v \text{ for a.a. } v\} \subset \prod_v G_v.$$

(The H_v is suppressed in the notation in the left, but this should not cause any confusion because for each choice of G_v we make, there will be a standard choice of H_v.) Here "a.a." stands for "almost all," by which we mean for all but finitely many v. So if V is a finite set, the "for almost all" condition is vacuously satisfied and $\prod_v' G_v$ is just the direct product. Note that if (g_v), $(g_v') \in \prod_v' G_v$, then their product $(g_v g_v') \in \prod_v' G_v$ since both $g_v, g_v' \in H_v$ for almost all v. Hence the restricted direct product is a subgroup of the direct product.

Note that if $G_v = F_v$ and $H_v = \{0\}$ for all places v of a number field F, this gives the direct sum we mentioned earlier:

$$\prod_v{}' G_v = \{(x_v) | x_v \in F_v,\ x_v = 0 \text{ for a.a. } v\} = \bigoplus_v F_v.$$

On the other hand, taking $H_v = G_v$ for all v gives the full direct product $\prod_v' G_v = \prod_v G_v$. Thus, varying the H_v's will allow us to interpolate between $\bigoplus F_v$ and $\prod F_v$.

We also remark that, because of the almost all condition, changing H_v at finitely many places does not affect the restricted direct product.

Now we can define adeles and ideles. Let F be a number field and v be a place of F. Note that $\mathcal{O}_{F,v}$ is the (topological) closure of $\mathcal{O}_F$ inside F_v for a finite prime $v < \infty$. For uniformity, we can define $\mathcal{O}_{F,v}$ to be the closure of $\mathcal{O}_F$ in F_v for an infinite prime $v|\infty$ also, though most authors do not define $\mathcal{O}_{F,v}$ for $v|\infty$. For instance, if $F = \mathbb{Q}$, then $\mathcal{O}_{F,\infty} = \mathbb{Z}_\infty = \mathbb{Z}$, since $Z = \mathcal{O}_F$ is already closed in $\mathbb{Q}_\infty = \mathbb{R}$. In general, for any number field, $\mathcal{O}_F$ is closed (in fact discrete) in F_v for $v|\infty$, so $\mathcal{O}_{F,v} = \mathcal{O}_F$ for $v|\infty$.

Definition 1.5.1. *The* **adeles** *of a number field F are the restricted direct product $\mathbb{A}_F = \prod_v' F_v$ with respect to the additive subgroups $\mathcal{O}_{F,v}$. The* **ideles** *of F are the restricted direct product $\mathbb{A}_F^\times = \prod_v' F_v$ with respect to the multiplicative subgroups $\mathcal{O}_{F,v}^\times$. In both of these products, v runs over all primes of F.*

If you want to be fancy, you can stick *un accent grave* on the first e: adèle and idèle. I sort like it with the accent (at least for idèle), but I get lazy about typing \` in tex. The word idèle is a Frenchy variant on the the abbreviation "id. el." for "ideal element," and adèle is a *portmanteau* of "additive idèle." Idèles were first introduced by Chevalley as a way to study ideals, and then adèles were introduced later. Some authors use $\mathbb{I}$ or $\mathbb{J}$ to denote idèles.

Exercise 1.5.1. Check that $\mathbb{A}_F$ is a commutative ring and $\mathbb{A}_F^\times$ is the unit group of $\mathbb{A}_F$.

Despite the fact that one point of working with adeles is to treat the nonarchimedean and archimedean places of F uniformly, one will often want to work with them separately. Therefore, we introduce the following notation: the ring of **finite adeles** $\hat{F} = \mathbb{A}_{F,f}$ is the restricted direct product $\prod_{v<\infty}' F_v$ over all finite places. Then if we put $F_\infty = \prod_{v|\infty} F_v$, we have the decomposition of adeles into finite and archimedean parts:

$$\mathbb{A}_F = \mathbb{A}_{F,f} \times F_\infty = \hat{F} \times F_\infty.$$

Similarly, we define the group of **finite ideles** $\hat{F}^\times = \mathbb{A}_{F,f}^\times$ is the restricted direct product $\prod_{v<\infty}' F_v^\times$, and as in the previous exercise, this is the unit group of $\hat{F}$. We extend our "hat notation" to rings of integers: $\hat{\mathcal{O}}_F = \prod_{v<\infty} \mathcal{O}_{F_v}$ and $\hat{\mathcal{O}}_F^\times = \prod_{v<\infty} \mathcal{O}_{F_v}^\times$. We can think of $\hat{\mathcal{O}}_F$ and $\hat{\mathcal{O}}_F^\times$ as adelic and idelic integers. (Note we could also define these as restricted direct products with respect to $H_v = \mathcal{O}_{F_v}$ or $\mathcal{O}_{F_v}^\times$, but this is the same as the full direct product since $H_v = G_v$ in this case.)

When working with multiplicative groups or subgroups of ideles, we will often drop the direct product sign and just write $\mathbb{A}_F^\times = \hat{F}^\times F_\infty^\times$. This coincides with usual group theory notation if you think of embedding $\hat{F}^\times$ and $F_\infty^\times$ into $\mathbb{A}_F^\times$ by putting 1's at all other components, and then $\hat{F}^\times F_\infty^\times$ just means an internal direct product of subgroups of the ideles. For adeles, the analogous thing is to embed $\hat{F}$ and F_∞ as subrings of $\mathbb{A}_F$ by putting 0's at all other components, so then we get $\mathbb{A}_F = \hat{F} + F_\infty$. Warning: this gives the notational conundrum $\hat{F} F_\infty = \{0\}$ even though $\hat{F}^\times F_\infty^\times = \mathbb{A}_F^\times$!

We consider F as a subring of $\mathbb{A}_F$ and $\hat{F}$ via diagonal embeddings, and similarly $F^\times$ as a subgroup of $\mathbb{A}_F^\times$ and $\hat{F}^\times$. We sometimes call the elements of F or $F^\times$ the **(F-)rational** elements (or points) of the finite or complete adeles or ideles. (Note this is very different from $(x_v) \in \mathbb{A}_F$ being rational component-wise—e.g., every element of $\hat{\mathbb{Q}} \times \mathbb{Q} \subset \mathbb{A}_\mathbb{Q}$ has rational components, but they won't be rational elements of $\mathbb{A}_\mathbb{Q}$ unless all components are identical.)

The following exercise indicates one reason why adeles are nicer that the full direct product: namely it essentially says that any finite adele $\alpha \in \mathbb{A}_{F,f} = \hat{F}$ is an "adelic integer" $u \in \hat{\mathcal{O}}_F$ times a nonzero F-rational number $x \in F^\times$.

Exercise 1.5.2. Check that $\mathbb{A}_F = F(\hat{\mathcal{O}}_F \times F_\infty)$, i.e., $\hat{F} = F\hat{\mathcal{O}}_F$. That is, show that for any finite adele $\alpha \in \hat{F}$, there exists $x \in F^\times$ such that $x\alpha \in \hat{\mathcal{O}}_F$. Show this is not possible for an arbitrary $\alpha \in \prod F_v$ (the full direct product).

Note the analogous statement of this exercise for ideles is not true (for general F, though it is true for $F = \mathbb{Q}$ as we will see below). Think about what goes wrong with your argument.

For an adele $\alpha = (\alpha_v) \in \mathbb{A}_F$, we can define the adelic (semi)norm

$$\|\alpha\| = \|\alpha\|_{\mathbb{A}} = \prod_v |\alpha_v|_v \in \mathbb{R}_{\geq 0}.$$

Note that this converges, because $\alpha_v \in \mathcal{O}_{F_v}$ at almost all places, i.e., $|\alpha_v|_v \leq 1$ at almost all places. (This is another reason adeles are nicer than the full direct product.) It is not an absolute value or a norm in the strict sense because $\|\alpha\| = 0$ for many α (both which are 0 at some components and which are nonzero at all components—e.g., if $F = \mathbb{Q}$ take $\alpha_p = p$ at all p). On the other hand, if $\alpha \in \mathbb{A}_F^\times$, then we always have $\|\alpha\| \neq 0$ since α_v must be nonzero at all components and, for almost all v, $\alpha_v \in \mathcal{O}_{F_v}^\times$, i.e., $|\alpha_v|_v = 1$.

Proposition 1.5.2 (Product formula)**.** *For $x \in F^\times$, $\|x\|_{\mathbb{A}} = 1$.*

Proof. First we check this first for $F = \mathbb{Q}$. Write $x = \prod p_i^{e_i}$. Then

$$\|x\| = \prod_v |x|_v = \prod_i p_i^{-e_i} |x|_\infty = 1.$$

For arbitrary F, recall from Corollary 1.3.7 that $\prod_{v|p} |x|_v = |N_{F/\mathbb{Q}}(x)|_p$. We similarly similarly have $\prod_{v|\infty} |x|_v = |N_{F/\mathbb{Q}}(x)|_\infty$. (This is one reason we introduced the complex absolute value as the square of the usual one.) Now apply the result for $F = \mathbb{Q}$. □

Adelic topology

We can put a topology on the adeles by defining a basis for the open sets to be those of the form $\prod U_v$ where each U_v is an open subset of F_v and $U_v = \mathcal{O}_{F_v}$ for almost all v.

Exercise 1.5.3. The operations of addition, negation and multiplication are continuous on $\mathbb{A}_F$, i.e., $\mathbb{A}_F$ is a *topological ring*.

Recall that a subset S of a topological space X is **discrete** if, for any $p \in S$, there exists an open set $U \subset X$ such that $U \cap S = \{p\}$. Equivalently, $S \subset X$ is discrete if the subspace topology on S is the discrete topology.

Proposition 1.5.3. *F is a discrete subgroup of $\mathbb{A}_F$.*

This is the opposite of what happens locally—recall for any nonarchimedean place v, F is dense in F_v.

Proof. Let $x \in F$. We want to show there is an open set $U \subset \mathbb{A}_F$ such that $U \cap F = \{x\}$. Take U of the form $U = x + \hat{\mathcal{O}}_F \times \prod_{v|\infty} U_v$. Then $y \in F \cap U$ implies $y \in x + \mathcal{O}_{F_\mathfrak{p}}$ for all prime ideals $\mathfrak{p}$, i.e., $y - x \in \mathcal{O}_{F_\mathfrak{p}}$ for all $\mathfrak{p}$, i.e., $y - x \in \mathcal{O}_F$. Now we use the fact from Minkowski's geometry of numbers that $\mathcal{O}_F$ is a discrete lattice in F_∞ via the embedding $x \mapsto (\sigma_1(x), \dots, \sigma_m(x))$ described after Example 1.4.2. (This is obvious if, say, $F = \mathbb{Q}$ or $F = \mathbb{Q}(i)$, as this is tantamount to the statements that $\mathbb{Z}$ is discrete in $\mathbb{R}$ and $\mathbb{Z}[i]$ is discrete in $\mathbb{C}$.) Thus $U \cap F$ restricted to the F_∞ component is discrete, so we can choose our U_v's for $v|\infty$ such that $U \cap F = \{x\}$. □

Proposition 1.5.4. *$\mathbb{A}_F/F$ is compact.*

Proof. See [RV99, Thm 5-11]. □

The above two propositions are the adelic version of the statement that the embedding $F \subset \prod_{v|\infty} F_\infty$ described earlier is discrete and has compact quotient. (Indeed, we used this discreteness fact in the proof above.)

We also remark a topological generalization of Exercise 1.5.2.

Proposition 1.5.5 (Strong approximation)**.** *F is dense in $\mathbb{A}_f = \hat{F}$. In particular,*

$$F(\hat{\mathcal{O}}_F \times F_\infty) = \mathbb{A}_F.$$

Proof. See [cas67, Sec II.15]. □

Similar to the case of adeles, we put a topology on the ideles by defining a basis for the open sets to be those of the form $\prod U_v$ where each U_v is an open subset of $F_v^\times$ and $U_v = \mathcal{O}_{F_v}^\times$ for almost all v. This is different from the subspace topology of $\mathbb{A}_F^\times \subset \mathbb{A}_F$, but we can relate the topologies as follows. Consider the map $\mathbb{A}_F^\times \to \mathbb{A}_F \times \mathbb{A}_F$ given by $\alpha \mapsto (\alpha, \alpha^{-1})$. Then one takes the subspace topology of the product topology on the image of this map, and transports it to a topology on $\mathbb{A}_F^\times$.

Exercise 1.5.4. Show these two ways of defining a topology on $\mathbb{A}_F^\times$ are equivalent.

Exercise 1.5.5. Show that multiplication and inversion are continuous on $\mathbb{A}_F^\times$, i.e., $\mathbb{A}_F^\times$ is a topological group.

Proposition 1.5.6. *$F^\times$ is a discrete subgroup of $\mathbb{A}_F^\times$.*

Proof. By Exercise 1.5.4, this is equivalent to saying $\left\{(x, x^{-1}) : x \in F^\times\right\}$ is discrete in $\mathbb{A}_F \times \mathbb{A}_F$. This follows from Proposition 1.5.3. □

The naive multiplicative analogue of Proposition 1.5.4 is not true, i.e., $\mathbb{A}_F^\times/F^\times$ is not compact simply because the adelic norm map is a multiplicative map with $F^\times$ in its kernel. Thus $\|\cdot\| : \mathbb{A}_F^\times/F^\times \to \mathbb{R}_{>0}$ is a (continuous) map with unbounded image and we can construct a sequence of α's in $\mathbb{A}_F^\times/F^\times$ with unbounded norm.

However, this is the only obstruction to compactness. Define the **norm one ideles** to be the subgroup of $\mathbb{A}_F^\times$ given by

$$\mathbb{A}_F^1 = \{x \in \mathbb{A}_F : \|x\| = 1\}.$$

Theorem 1.5.7. *$\mathbb{A}_F^1/F^\times$ is compact.*

Proof. See [cas67, Sec II.16] or [RV99, Thm 5-15]. □

Connection with ideals

Now we explain how ideles are connected to ideals and how Theorem 1.5.7 implies finiteness of the ideal class group.

Fix a fractional ideal $\mathcal{I}$ of $\mathcal{O}_F$. For any $v < \infty$, we let $\mathcal{I}_v = \mathcal{I}\mathcal{O}_{F,v} \subset F_v$ as in (1.3.2). To treat the archimedean places and nonarchimedean places with uniform notation, we can define $\mathcal{O}_{F_v} = F_v$ ($= \mathbb{R}$ or $\mathbb{C}$) for $v|\infty$ and define $\mathcal{I}_v$ the same way, so for $v|\infty$, $\mathcal{I}_v$ is just $\mathbb{R}$ or $\mathbb{C}$ provided $\mathcal{I}$ is nonzero. (Though most authors do not do this.)

Suppose $\mathcal{I}$ is locally principal, i.e., $\mathcal{I}$ is an invertible ideal of $\mathcal{O}_F$ (cf. Proposition 1.4.5). Then we know that for any v, there exists $x_v \in F_v$ such that $\mathcal{I}_v = x_v\mathcal{O}_{F_v}$ (for $v|\infty$, we may take $x_v = 1$). If $v|p$ (i.e., v corresponds to a prime ideal $\mathfrak{p}$ of $\mathcal{O}_F$ which lies above p), then $p \nmid |N(\mathcal{I})|$ implies $\mathcal{I}_v = \mathcal{O}_{F_v}$, so $x_v \in \mathcal{O}_{F_v}^\times$. Thus $x_v \in \mathcal{O}_{F_v}^\times$ for almost all v. Hence we get a map from the invertible ideals to ideles by

$$\mathcal{I} \mapsto (x_v)_v \in \mathbb{A}_F^\times. \tag{1.5.1}$$

Of course this map is not unique, because at any place v, we may replace x_v by $u_v x_v$ for any unit $u_v \in \mathcal{O}_{F_v}^\times$.

Proposition 1.5.8. *The above map defines an isomorphism of the group of invertible fractional ideals*

$$\mathrm{Frac}(\mathcal{O}_F) \simeq \hat{\mathcal{O}}_F^\times F_\infty^\times \backslash \mathbb{A}_F^\times \simeq \hat{\mathcal{O}}_F^\times \backslash \hat{F}^\times.$$

Further, this map induces a natural isomorphism

$$\mathrm{Cl}(F) = \mathrm{Cl}(\mathcal{O}_F) \simeq \hat{\mathcal{O}}_F^\times F_\infty^\times \backslash \mathbb{A}_F^\times / F^\times \simeq \hat{\mathcal{O}}_F^\times \backslash \hat{F}^\times / F^\times. \tag{1.5.2}$$

If you prefer, you can write the entire quotient on one side (since everything is commutative): $\mathrm{Cl}(F) = \hat{F}^\times / F^\times \hat{\mathcal{O}}_F^\times$, but I like to visually separate the quotients so you see you're quotienting out by two things: first, by $\hat{\mathcal{O}}_F^\times$ on the left to get a correspondence with *left* $\mathcal{O}_F$-ideals; second, by $F^\times$ on the right to mod out by principal ideals. Indeed, when we pass to the noncommutative case, we really have to do one quotient on the left and one on the right as in (1.5.2).

This proposition says the map (1.5.1), viewed as a map $\mathrm{Frac}(\mathcal{O}_F) \to \hat{\mathcal{O}}_F^\times \backslash \hat{F}^\times$, is invertible. It is not hard to say what the inverse should be, can you can check this as part of the next exercise. Here is one way to describe the inverse map. Given $x = (x_v) \in \hat{F}^\times$, we can associate the local ideal $\mathcal{I}_v = x_v\mathcal{O}_{F_v}$, for each $v < \infty$. To the finite idele x, we associate the ideal

$$\mathcal{I} = \bigcap_{v<\infty} \mathcal{I}_v = x\hat{\mathcal{O}}_F \cap F.$$

We can also describe it explicitly in terms of prime ideals as follows. For each v, we can write $\mathcal{I}_v = \mathfrak{p}_v^{r_v}\mathcal{O}_{F_v}$, where $\mathfrak{p}_v$ is the global prime ideal of $\mathcal{O}_F$ associated to v. Then, it is easy to see the previous description of $\mathcal{I}$ is equivalent to:

$$\mathcal{I} = \prod \mathfrak{p}_v^{r_v}.$$

Exercise 1.5.6. Prove the above proposition.

In fact one can define a correspondence of ideals with norm one ideles because we are free to choose x_v at $v|\infty$ to be any element of $\mathbb{R}^\times$ or $\mathbb{C}^\times$. Thus we can always modify x_v at one archimedean place to make $\|x\| = 1$ because the archimedean norm maps are surjective. Alternatively,

$$F_\infty^\times \backslash \mathbb{A}_F^\times \simeq F_\infty^1 \backslash \mathbb{A}_F^1, \tag{1.5.3}$$

where $F_\infty = \left\{x \in F_\infty : \prod_{v|\infty} |x_v|_v = 1\right\}$. Hence one can rewrite (1.5.2) as

$$\mathrm{Cl}(F) \simeq \hat{\mathcal{O}}_F^\times F_\infty^1 \backslash \mathbb{A}_F^1 / F^\times. \tag{1.5.4}$$

Corollary 1.5.9. *The class group* $\mathrm{Cl}(\mathcal{O}_F)$ *is finite.*

Proof. Combining (1.5.3) with Theorem 1.5.7 shows $F_\infty^1 \backslash \mathbb{A}_F^1 / F^\times$ is compact. Because $\mathcal{O}_F^\times \times F_\infty^\times$ is an open subgroup of $\mathbb{A}_F^\times$, (the image of) $\mathcal{O}_F^1$ (in the quotient) is an open subgroup of $F_\infty^1 \backslash \mathbb{A}_F^1 / F^\times$, so $\mathrm{Cl}(\mathcal{O}_F)$ is a compact group modulo an open subgroup, and thus finite (Exercise 1.2.15). □

Note that if the idelic analogue of Exercise 1.5.2 were true (i.e., $\hat{F}^\times = F^\times \hat{\mathcal{O}}_F^\times$), that would mean that $\mathrm{Cl}(\mathcal{O}_F)$ is always trivial! Instead, this analogue is only true when $h_F = 1$.

Variants of the ideal class group are also important in number theory, such as ray class groups and the narrow class group. We can put these other notations of class groups in a similar framework as (1.5.2). Define the **idèle class group** C_F by

$$C_F := \mathbb{A}_F^\times / F^\times.$$

This is compact and we can rewrite (1.5.2) as

$$\mathrm{Cl}(F) \simeq \hat{\mathcal{O}}_F^\times F_\infty^\times \backslash C_F.$$

Ray class groups, as defined in [Neu99, Sec VI.1], are quotients of the form

$$\mathrm{Cl}^{\mathfrak{m}}(F) := \hat{\mathfrak{m}}^\times F_\infty^\times \backslash C_F,$$

where $\mathfrak{m} = \prod \mathfrak{p}^{e_\mathfrak{p}}$ is an integral ideal in $\mathcal{O}_F$ and $\hat{\mathfrak{m}}^\times = \prod_\mathfrak{p} \mathcal{O}_{F_\mathfrak{p}}^{(e_\mathfrak{p})}$.

We won't explain the ideal theoretic intepretation, or use ray class groups—however, the narrow class group will come up in our study of quaternion algebras, so we briefly introduce it now.

Classically, the narrow class group is defined to be the nonzero fractional ideals modulo the *totally positive* principal ideals, i.e., principal ideals of the form $a\mathfrak{o}_F$ where a is totally positive, i.e., for any embedding σ of F into $\mathbb{C}$, $\sigma(a) > 0$. Adelically, we define the **narrow class group** as

$$\mathrm{Cl}^+(F) = \mathrm{Cl}^+(\mathcal{O}_F) := \hat{\mathcal{O}}_F^\times F_\infty^{\times,0} \backslash C_F = \hat{\mathcal{O}}_F^\times F_\infty^{\times,0} \backslash \mathbb{A}_F^\times / F^\times,$$

where

$$F_\infty^{\times,0} = \prod_{F_v = \mathbb{R}} \mathbb{R}_{>0} \times \prod_{F_v = \mathbb{C}} \mathbb{C}^\times$$

is the connected component of 1 in $F_\infty^\times$. Since $F_\infty^\times \backslash \mathrm{Cl}^+(\mathcal{O}_F) = \mathrm{Cl}(\mathcal{O}_F)$, the usual class group is a quotient of the narrow class group. The narrow class group is also a finite abelian group (being the quotient of a compact group by an open subgroup), and we denote the size by h_F^+, which is called the **narrow class number**.

Exercise 1.5.7. Let r be the number of real embeddings of F into $\mathbb{R}$. Then $h_F^+ = 2^m h_F$ for some $0 \le m \le r-1$.

One can use adeles to prove important results like the class number formula and the Chebotarev density theorem, as well as the original goal of developing class field theory. See, e.g., [RV99] or [cas67].

Generalizations to non-maximal orders?

Now you might wonder, if $\mathcal{O}$ is a non-maximal order in $\mathcal{O}_F$, can we get an idelic description of the class group $\mathrm{Cl}(\mathcal{O})$. The first issue is: what should the adeles be? Before, we defined $\mathbb{A}_F^\times$ with respect to the integral structure $\mathcal{O}_F$ and its local completions $\mathcal{O}_{F_v}$. Here the v's range over prime ideals of $\mathcal{O}_F$, together with the infinite primes. But, for a non-maximal order, the prime ideals of $\mathcal{O}$ do not precisely correspond to the nonarchimedean valuations on F (which is still the field of fractions of $\mathcal{O}$).

For instance, in Example 1.4.5, we see that there is a unique prime ideal $\mathfrak{p}$ above 2 in $\mathcal{O} = \mathbb{Z}[\sqrt{-3}]$, but there are 2 nonarchimedean places above 2, corresponding to the 2 prime ideals $\mathfrak{p}_1$ and $\mathfrak{p}_2$ above 2 in $\mathcal{O}_F = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$. In particular, $\mathfrak{p}$ does not give rise to an absolute value on F in a unique (even up to equivalence), well-defined way. Hence it is not clear how to make sense of a local completion $F_\mathfrak{p}$ (though one can still define the localization $\mathcal{O}_{(\mathfrak{p})} \subset F$).

Instead, one thing we could do is think in terms of the extension $F/\mathbb{Q}$, i.e., think of F as a structure (a field or algebra) over $\mathbb{Q}$. Then our order $\mathcal{O}$ is a sort of extension of $\mathbb{Z}$—to be precise, it is a $\mathbb{Z}$-module. We can consider the adeles $\mathbb{A}_\mathbb{Q}$ of $\mathbb{Q}$ and extend them to F by $\mathbb{A}_\mathbb{Q} \otimes F$. This $\mathbb{Q}$-adelic structure on F will be a restricted product of rings of the form $F_p = F \otimes_\mathbb{Q} \mathbb{Q}_p$ with corresponding orders $\mathcal{O}_p = \mathcal{O} \otimes_\mathbb{Q} \mathbb{Z}_p$ (Proposition 1.3.8 describes these tensor products in the case of maximal orders). Thus one can try to study general orders $\mathcal{O}$ by working over the adeles $\mathbb{A}_\mathbb{Q}$ of our base field $\mathbb{Q}$.

Indeed, this will be our approach when looking at algebras A over a field F. We will look at some order $\mathcal{O}$ of A, which will be an $\mathfrak{o}_F$-module (at this point I will denote $\mathcal{O}_F$ by

$\mathfrak{o}_F$, to help make it more notationally obvious that $\mathcal{O}$ is an order "upstairs" whereas $\mathfrak{o}_F$ is an order "downstairs".) Then our local-global approach to studying A will be to consider the "local completions" $A_v = A \otimes F_v$ and $A(\mathbb{A}_F) = A \otimes \mathbb{A}_F$. Similar to the case of $\mathrm{Cl}(\mathfrak{o}_F)$, will be able to describe the space of ideal classes of $\mathcal{O}$ (not a group in general) adelically using $A(\mathbb{A}_F)$.

For an adelic approach the class number formula for non-maximal orders (Theorem 1.4.7) in the case of imaginary quadratic fields, see [Piz76, Lem 44].