Topics in Algebra and Number Theory

HU Yong 胡 勇
huy@sustech.edu.cn

January 28, 2022

Contents

This page is intentionally left blank.

1 Reciprocity Law, Gauss Sums and Beyond

1.1 The quadratic reciprocity revisited

(1.1.1) Let p be an odd prime number and a be an integer coprime to p. If the congruence equation $x^2 \equiv a \pmod{p}$ has integer solutions, we say that a is a ***quadratic residue*** modulo/of p; otherwise we say a is a ***quadratic non-residue***. The ***Legendre symbol*** $\left(\frac{a}{p}\right)$ is defined by

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{if } a \text{ is a quadratic residue mod } p\,, \\ -1 & \text{if } a \text{ is a quadratic non-residue mod } p\,. \end{cases}$$

Sometimes we also use the convention that $\left(\frac{a}{p}\right) = 0$ if $\gcd(a,\, p) > 1$.

Now let q be an odd prime different from p. Suppose that we know whether q is a quadratic residue of p. Do we also know whether p is a quadratic residue of q? Euler (1707–1783) found the answer to this question by examining numerical evidence but did not give a proof. The answer is now known as the famous ***law of quadratic reciprocity***. Its elegant modern form was first formulated by Legendre (1752–1833) in 1785, as follows:

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\,.$$

Legendre published several proposed proofs of this reciprocity law, but each of them contained a serious gap. The first complete proof is due to Gauss (1777–1855), who recorded the date of the proof in his diary on April 8, 1796. An elementary proof, due to Eisenstein (1823–1852), based on counting integral points in a suitably chosen triangle is adopted by many textbooks in elementary number theory (see e.g. [Ros11] or [Hu21]).

For an up-to-date chronology and bibliography of proofs of the quadratic reciprocity law, the interested reader may visit the website

`https://www.mathi.uni-heidelberg.de/~flemmermeyer/qrg_proofs.html`

Gauss liked very much the quadratic reciprocity law and continued searching for additional proofs. His goal in looking for more proofs was to find an approach that could be generalized to higher powers. During his lifetime Gauss published six different proofs of this remarkable law. With his sixth proof, Gauss finally succeeded in his goal.

In 1923, Hecke (1887–1947) wrote

"*Modern number theory dates from the discovery of the reciprocity law. [...] The development of algebraic number theory has now actually shown that the content of the quadratic reciprocity law only becomes understandable if one passes to general algebraic numbers and that a proof appropriate to the nature of the problem can be best carried out with these higher methods.*"

Naturally, along with these higher methods came generalizations of the reciprocity law itself. These generalizations changed our way of looking at the reciprocity law dramatically, and had profoundly effected the development of number theory in the 20th century. ■

Let us present Gauss' sixth proof (in his *Disquisitiones Arithmeticae*) of the quadratic reciprocity law.

Lemma 1.1.2. *Let p be a prime number and let C be a field of characteristic $\neq p$. Suppose that C contains a primitive p-th root of unity ζ (e.g. $C = \mathbb{C}$ and $\zeta = \exp(\frac{2\pi i}{p})$).*

For all $x, y \in \mathbb{Z}$, we have the following equality in C:

$$\frac{1}{p}\sum_{t=0}^{p-1} \zeta^{(x-y)t} = \delta(x, y) := \begin{cases} 1 & \text{if } x \equiv y \pmod{p}, \\ 0 & \text{otherwise}. \end{cases}$$

Proof. The sum in question is easily computed, as a partial sum of a geometric series. □

Proposition 1.1.3. *With notation and hypotheses as in Lemma 1.1.2, suppose p is odd. For each $a \in \mathbb{Z}$ define*

$$g_a := g_a(p) := \sum_{t=0}^{p-1} \left(\frac{t}{p}\right) \zeta^{at}. \tag{1.1.3.1}$$

(This is called a **quadratic Gauss sum** *mod p in C.)*

Then we have

$$\forall\, a \in \mathbb{Z}, \quad g_a = \left(\frac{a}{p}\right) g_1 \quad \text{and} \quad g_1^2 = (-1)^{\frac{p-1}{2}} p \tag{1.1.3.2}$$

in the field C.

Proof. First assume $a \equiv 0 \pmod{p}$. Then $\zeta^a = 1$ and

$$g_a = \sum_{t=0}^{p-1} \left(\frac{t}{p}\right) = \sum_{t=1}^{p-1} \left(\frac{t}{p}\right) = 0,$$

because precisely half of the integers $1, 2, \cdots, p-1$ are quadratic residues mod p. (Recall that $\left(\frac{0}{p}\right) = 0$ by definition.)

Now suppose $a \not\equiv 0 \pmod{p}$, so that $\left(\frac{a}{p}\right) \neq 0$. Then

$$\left(\frac{a}{p}\right) g_a = \sum_{t=0}^{p-1} \left(\frac{at}{p}\right) \zeta^{at} = \sum_{s=0}^{p-1} \left(\frac{s}{p}\right) \zeta^{s} = g_1.$$

Here we have used the fact at runs over a complete residue system mod p when t does and that $\left(\frac{s}{p}\right)$ and ζ^s depend only on the residue class of $s \in \mathbb{Z}$ mod p. This proves the first equality in (1.1.3.2).

To see the other equality, we rewrite the quadratic Gauss sum g_1 as a sum over the finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$: $g_1 = \sum_{s \in \mathbb{F}_p} \left(\frac{s}{p}\right)\zeta^s$. Then

$$\begin{aligned} g_1^2 &= \sum_{x,\, y \in \mathbb{F}_p} \left(\frac{xy}{p}\right) \zeta^{x+y} = \sum_{u \in \mathbb{F}_p} \zeta^u \left(\sum_{x \in \mathbb{F}_p} \left(\frac{x(u-x)}{p} \right) \right) \\ &= \sum_{u \in \mathbb{F}_p} \zeta^u \left(\sum_{x \in \mathbb{F}_p^*} (-1)^{\frac{p-1}{2}} \left(\frac{1 - ux^{-1}}{p} \right) \right). \end{aligned}$$

Put $A_u = \sum_{x\in\mathbb{F}_p^*} \left(\frac{1-ux^{-1}}{p}\right)$ for each $u \in \mathbb{F}_p$. If $u = 0$, we get $A_0 = p - 1$. Otherwise $s := 1 - ux^{-1}$ runs over $\mathbb{F}_p \setminus \{1\}$ and we find

$$A_u = \sum_{s\in\mathbb{F}_p} \left(\frac{s}{p}\right) - \left(\frac{1}{p}\right) = 0 - 1 = -1\,.$$

Therefore,

$$g_1^2 = (-1)^{\frac{p-1}{2}} \sum_{u\in\mathbb{F}_p} \zeta^u A_u = (-1)^{\frac{p-1}{2}} \left((p-1) - \sum_{u\in\mathbb{F}_p^*} \zeta^u\right) = (-1)^{\frac{p-1}{2}} p$$

noticing that

$$\sum_{u\in\mathbb{F}_p^*} \zeta^u = \sum_{u\in\mathbb{F}_p} \zeta^u - 1 = -1$$

by Lemma 1.1.2. □

Remark 1.1.4. If we further assume $\mathrm{char}(C) \nmid (p-1)p$ in Prop. 1.1.3, another proof of the equality $g_1^2 = (-1)^{\frac{p-1}{2}} p$ can be given by evaluating the sum $\sum_{a=0}^{p-1} g_a g_{-a}$ in two ways.

Indeed, for $a \not\equiv 0 \pmod{p}$, we have

$$g_a g_{-a} = \left(\frac{a}{p}\right)\left(\frac{a}{p}\right) g_1^2 = \left(\frac{-1}{p}\right) g_1^2 = (-1)^{\frac{p-1}{2}} g_1^2$$

by the first equality in (1.1.3.2). Thus,

$$\sum_{a=0}^{p-1} g_a g_{-a} = (-1)^{\frac{p-1}{2}} (p-1) g_1^2\,.$$

On the other hand, computing directly from the definition we get

$$g_a g_{-a} = \sum_{x,\,y\in\mathbb{F}_p} \left(\frac{x}{p}\right)\left(\frac{y}{p}\right) \zeta^{(x-y)a}\,.$$

summing both sides over a and using Lemma 1.1.2 we obtain

$$\begin{aligned}\sum_{a=0}^{p-1} g_a g_{-a} &= \sum_{x,\,y\in\mathbb{F}_p} \left(\frac{x}{p}\right)\left(\frac{y}{p}\right) p\delta(x,\,y) = \sum_x p\left(\frac{x}{p}\right)\left(\sum_y \left(\frac{y}{p}\right)\delta(x,\,y)\right) \\ &= \sum_x p\left(\frac{x}{p}\right)^2 = (p-1)p\,.\end{aligned}$$

It follows that $(p-1)p = (-1)^{\frac{p-1}{2}}(p-1)g_1^2$. Since $p - 1 \neq 0$ in C, we get $g_1^2 = (-1)^{\frac{p-1}{2}} p$ as desired. ■

(1.1.5) We now proceed to prove the quadratic reciprocity law. Let p, q be distinct odd primes. Let C be an algebraic closure of the prime field $\mathbb{F}_q$. The quadratic Gauss sum $g_1 = \sum_{t\in\mathbb{F}_p} \left(\frac{t}{p}\right)\zeta^t$ in F satisfies

$$g_1^q = \sum_{t\in\mathbb{F}_p} \left(\frac{t}{p}\right)^q \zeta^{tq} = \sum_{t\in\mathbb{F}_p} \left(\frac{t}{p}\right) \zeta^{tq} = \sum_{s\in\mathbb{F}_p} \left(\frac{sq^{-1}}{p}\right) \zeta^{s} = \left(\frac{q}{p}\right) g_1 = \left(\frac{q}{p}\right)^{-1} g_1 \,.$$

(Here we use the formula $(x+y)^q = x^q + y^q$ in any field of characteristic q. Notice also that $(-1)^q = -1$ since q is odd.) Note that $g_1 \neq 0$ in C since $g_1^2 = \pm p \neq 0$ in C by the second equality in (1.1.3.2). It follows that $g_1^{q-1} = \left(\frac{q}{p}\right)$. But (1.1.3.2) also yields

$$g_1^{q-1} = \left(g_1^2\right)^{\frac{q-1}{2}} = \left((-1)^{\frac{p-1}{2}} p\right)^{\frac{q-1}{2}} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} p^{\frac{q-1}{2}} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \left(\frac{p}{q}\right) \,.$$

So we find $\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \left(\frac{p}{q}\right)$, proving the quadratic reciprocity law. ■

Remark 1.1.6. In (1.1.5) we have worked with $C = \overline{\mathbb{F}}_q$, the algebraic closure of the finite field $\mathbb{F}_q = \mathbb{Z}/q\mathbb{Z}$, whose characteristic may divide $p-1$. It is also possible to work over $C = \mathbb{C}$ by using congruences mod q in a certain ring of algebraic integers, as in [IR90, § 6.3]. But to make the second approach precise we need to define "the ring of algebraic integers". This will be done in the next chapter. ■

1.2 Trace and norm

For later use, we recall some basic facts about the trace and norm maps associated to a finite extension of fields. We omit most of the proofs since they can be easily found in standard textbooks on field and Galois theory (see e.g. [Mor96, § II.8]).

Throughout this section, let K/F be a finite extension of fields.

(1.2.1) For any $\alpha \in K$, the map $m_\alpha : K \to K$, $x \mapsto \alpha x$ is a linear endomorphism when we view K as a vector space over F. We can thus define the ***trace*** and the ***norm*** of α relative to K/F by

$$\mathrm{Tr}_{K/F}(\alpha) := \mathrm{Tr}(m_\alpha) \quad \text{and} \quad N_{K/F}(\alpha) := \det(m_\alpha)$$

respectively. From the definition we get easily the following elementary properties:

1. The trace map $\mathrm{Tr}_{K/F} : K \to F$ is F-linear.
2. The norm map $N_{K/F} : K \to F$ is multiplicative, i.e.,
$$N_{K/F}(\alpha\beta) = N_{K/F}(\alpha) N_{K/F}(\beta) \quad \text{for all } \alpha,\, \beta \in K \,.$$
3. If $\alpha \in F \subseteq K$, then we have
$$\mathrm{Tr}_{K/F}(\alpha) = n\alpha \quad \text{and} \quad N_{K/F}(\alpha) = \alpha^n \,,$$
where $n = [K : F]$. ■

Example 1.2.2. In general it is not always easy to compute traces and norms directly from the definitions. But we can do so in the following two special cases.

(1) Suppose $K = F(\sqrt{d})$, where $d \in F$ is a non-square in F. Then we have

$$\mathrm{Tr}_{K/F}(a + b\sqrt{d}) = 2a \quad \text{and} \quad N_{K/F}(a + b\sqrt{d}) = a^2 - b^2 d$$

for all a, $b \in F$.

(2) Suppose $\mathrm{char}(F) = p > 0$ and $K = F(\sqrt[p]{a})$, where $a \in F$ is not a p-th power in F. Then

$$\mathrm{Tr}_{K/F}(\alpha) = 0 \quad \text{and } N_{K/F}(\alpha) = (-1)^{p+1}\alpha^p = \alpha^p \quad \text{for all } \alpha \in K\,.$$

(Note that $-1 = 1$ in F if $p = 2$.) ■

(1.2.3) Let L be another field extension of F. An F-***embedding*** of K into L is an F-algebra homomorphism $\sigma : K \to L$, i.e., a map $\sigma : K \to L$ such that

$$\sigma(a + b) = \sigma(a) + \sigma(b)\,,\ \sigma(ab) = \sigma(a)\sigma(b) \quad \text{and} \quad \sigma(x) = x \text{ for all } x \in F\,.$$

Such a homomorphism is necessarily injective. We denote by $\mathrm{Hom}_{F\text{-alg}}(K, L)$ the set of F-embeddings of K into L.

Recall that the ***inseparable degree*** of K/F is defined as the number $[K : F]_i := [K : S]$, where S is the separable closure of F in K. A well known fact in field theory is that for any algebraically closed field Ω containing F, we have

$$|\,\mathrm{Hom}_{F\text{-alg}}(K, \Omega)| = [S : F] = \frac{[K : F]}{[K : F]_i} \le [K : F]\,.$$

In particular, if K/F is purely inseparable, there is one and only one F-embedding of K into Ω; and if K/F is separable, then $|\,\mathrm{Hom}_{F\text{-alg}}(K, \Omega)| = [K : F]$.

When K/F is a Galois extension, choosing any $\tau_0 \in \mathrm{Hom}_{F\text{-alg}}(K, \Omega)$, the map

$$\mathrm{Gal}(K/F) \longrightarrow \mathrm{Hom}_{F\text{-alg}}(K, \Omega)\ ; \quad \sigma \longmapsto \tau_0 \circ \sigma$$

is bijective. So in this case, we may identify $\mathrm{Hom}_{F\text{-alg}}(K, \Omega)$ with the Galois group $\mathrm{Gal}(K/F)$. ■

Theorem 1.2.4. *Let $\alpha \in K$, $n = [K : F]$ and $m = [F(\alpha) : F]$.*

1. *Let $f(X) = X^m + a_{m-1}X^{m-1} + \cdots + a_1X + a_0 \in F[X]$ be the minimal polynomial of α over F. Then*

$$\mathrm{Tr}_{K/F}(\alpha) = -\frac{n}{m}a_{m-1} \quad \textit{and} \quad N_{K/F}(\alpha) = (-1)^n a_0^{n/m}\,.$$

In particular, if $K = F(\alpha)$, then $\mathrm{Tr}_{K/F}(\alpha) = -a_{m-1}$ and $N_{K/F}(\alpha) = (-1)^n a_0$.

2. *Let Ω be an algebraically closed field containing F. Then*

$$\mathrm{Tr}_{K/F}(\alpha) = [K:F]_i \sum_{\sigma} \sigma(\alpha) \quad \text{and} \quad N_{K/F}(\alpha) = \left(\prod_{\sigma} \sigma(\alpha) \right)^{[K:F]_i}$$

where σ runs over the set $\mathrm{Hom}_{F\text{-}alg}(K, \Omega)$.

In particular, if K/F is a Galois extension, then

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

Theorem 1.2.5. *If $F \subseteq E \subseteq K$ are fields and $[K:F] < +\infty$, then*

$$\mathrm{Tr}_{K/F} = \mathrm{Tr}_{E/F} \circ \mathrm{Tr}_{K/E} \quad \text{and} \quad N_{K/F} = N_{E/F} \circ N_{K/E}\,.$$

Corollary 1.2.6. *The following assertions are equivalent for a finite extension K/F:*

(i) *The trace map $\mathrm{Tr}_{K/F} : K \to F$ is not identically zero.*

(ii) *The trace map $\mathrm{Tr}_{K/F} : K \to F$ is surjective.*

(iii) *The extension K/F is separable.*

Proof. Since $\mathrm{Tr}_{K/F}$ is F-linear and F is 1-dimensional as a vector space over itself, we have (i)⇒(ii).

If K/F is not separable, then it has an subextension E/F such that K/E is purely inseparable of prime degree*. By Example 1.2.2 (2), $\mathrm{Tr}_{K/E} = 0$. Hence by Thm. 1.2.5, $\mathrm{Tr}_{K/F} = 0$.

Now suppose K/F is separable. Let L/F be a finite Galois extension with $K \subseteq L$. Then $\mathrm{Tr}_{K/F} = 0$ would imply $\mathrm{Tr}_{L/F} = 0$ by Thm. 1.2.5. Therefore, it suffices to show $\mathrm{Tr}_{L/F}$ is a nonzero map. In other words, we may assume K/F is a Galois extension.

Notice that restriction yields a natural injection

$$\mathrm{Gal}(K/F) \hookrightarrow \mathrm{Hom}_{\mathrm{group}}(K^*, K^*) := \{\text{group homomorphisms } K^* \to K^*\}$$

and $\mathrm{Hom}_{\mathrm{group}}(K^*, K^*)$ can be further regarded as a subset of

$$\mathrm{Map}(K^*, K) := \{\text{set-theoretic maps } K^* \to K\}\,.$$

By Dedekind's lemma on the linear independence of characters of groups (see e.g. [Mor96, Lemma I.2.12]), $\mathrm{Gal}(K/F)$ is a linearly independent subset of the K-vector space $\mathrm{Map}(K^*, K)$. In particular, $\mathrm{Tr}_{K/F} = \sum_{\sigma \in \mathrm{Gal}(K/F)} \sigma$ is not identically zero. We have thus proved (i)⇔(iii). □

*In general, there may not exist a nontrivial inseparable subextension in K/F. See [Mor96, Example I.4.24] for such an example. Thanks to ZHAO Hongxiang (赵泓翔) for saving me from a mistake about this subtlety.

(1.2.7) Now suppose F is a finite field with q elements and $n = [K : F]$. Then K/F is a Galois extension and the Galois group $\mathrm{Gal}(K/F)$ is a cyclic group generated by the F-automorphism

$$\sigma \,:\, K \longrightarrow K\,; \quad x \longmapsto x^q\,,$$

which is often called the (***arithmetic***) ***Frobenius map*** of K/F.

Hence

$$\mathrm{Tr}_{K/F}(\alpha) = \sum_{i=0}^{n-1} \sigma^i(\alpha) = \sum_{i=0}^{n-1} \alpha^{q^i} \tag{1.2.7.1}$$

and

$$N_{K/F}(\alpha) = \prod_{i=0}^{n-1} \sigma^i(\alpha) = \prod_{i=0}^{n-1} \alpha^{q^i} = \alpha^{\frac{q^n-1}{q-1}} \tag{1.2.7.2}$$

for all $\alpha \in K$. ■

Proposition 1.2.8. *If K/F is a finite extension of finite fields, then the trace $\mathrm{Tr}_{K/F} : K \to F$ and the norm map $N_{K/F} : K \to F$ are both surjective.*

Proof. The statement for the trace map is a special case of Cor. 1.2.6 since K/F is separable. But it also follows directly from the formula (1.2.7.1). Indeed, The polynomial $\sum_{i=0}^{n-1} X^{q^i}$ has at most q^{n-1} roots in K. But $|K| = q^n$. So there exists $\alpha \in K$ such that $\sum_{i=0}^{n-1} \alpha^{q^i} \neq 0$. This shows that $\mathrm{Tr}_{K/F} : K \to F$ is not identically zero by (1.2.7.1). As it is an F-linear map with values in a 1-dimensional space, $\mathrm{Tr}_{K/F}$ is surjective.

To show the surjectivity of the norm map, note that K^* is a cyclic group of order $q^n - 1$ (if $q = |F|$ and $n = [K : F]$). Let ξ be a generator of K^*. Then $\theta := N_{K/F}(\xi)$ is a primitive $(q-1)$-th root of unity by (1.2.7.2). Hence θ is a generator of the cyclic group. This implies that the group homomorphism $N_{K/F} : K^* \to F^*$ is surjective. □

1.3 Characters and Gauss sums over finite fields

From now until the end of this chapter, we fix a prime number p and let F be a finite extension of $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, with $|F| = q$. We also fix an algebraically closed field C of characteristic $\mathrm{char}(C) \nmid (q-1)q$ and a primitive p-th root of unit $\zeta \in C$.

(1.3.1) A ***character*** or ***multiplicative character*** of F (with values in C) is a group homomorphism $\chi : F^* \to C^*$. The constant function $a \in F^* \mapsto 1 \in C^*$ is clearly a character. It is called the ***trivial character*** and denoted by ε.

Clearly, if χ is a character of F, then

$$\chi(F^*) \subseteq \mu_{q-1}(C) := \{z \in C \,|\, z^{q-1} = 1\}\,.$$

The set of all characters of F form a multiplicative group $\mathbf{X}(F)$ under the pointwise multiplication. That is, for any two characters χ, λ of F, the product $\chi\lambda$ sends each $a \in F^*$ to $\chi(a)\lambda(a)$. The identity element of this group is the trivial character ε. The inverse χ^{-1} of a character χ is the map sending each $a \in F^*$ to $\chi(a)^{-1}$. It is often convenient to write $\overline{\chi}$ instead of χ^{-1} and call it the ***conjugate*** of χ. ■

Example 1.3.2. If p is odd and $F = \mathbb{F}_p$, the Legendre symbol $\left(\frac{\cdot}{p}\right)$ can be viewed as a nontrivial character. ■

(1.3.3) Characters can be useful in the study of equations over finite fields. To illustrate this, we introduce the following notation: Let f be an n-variable polynomial in $F[X_1, \cdots, X_n]$ and $a \in F$. Let $N(f = a)$ denote the number of solutions of the equation $f = a$, i.e.,

$$N(f = a) := \#\{x = (x_1, \cdots, x_n) \in F^{\oplus n} \mid f(x) = a\}\,.$$

It will be useful to extend the domain of definition of a character χ to all of F by setting

$$\chi(0) = \begin{cases} 0 & \text{if } \chi \neq \varepsilon\,, \\ 1 & \text{if } \chi = \varepsilon\,. \end{cases}$$

The extended function $\chi : F \to C$ is still multiplicative: $\chi(ab) = \chi(a)\chi(b)$ for all $a, b \in F$. ■

Proposition 1.3.4. *Let m be a positive integer such that $q \equiv 1 \pmod{m}$.*

Then for all $a \in F$, we have

$$N(X^m = a) = \sum_{\chi^m = \varepsilon} \chi(a)\,,$$

where the sum is over all characters $\chi \in \mathbf{X}(F)$ of order dividing n.

Proof. Exercise. (Hint: if $a \in F$ is not an m-th power, there exists $\rho \in \mathbf{X}(F)$ such that $\rho^m = \varepsilon$ and $\rho(a) \neq 1$.) □

The following theorem is a special case of a more general result for characters of finite abelian groups. We refer the reader to [Was97, Chap. 3] or [IR90, § 8.1] for more details.

Theorem 1.3.5. *With notation as above, we have:*

1. *There is a (non-canonical) isomorphism of groups $\mathbf{X}(F) \cong F^*$. Therefore, $\mathbf{X}(F)$ is a cyclic group of order $q - 1$.*
2. *(Duality) The pairing*

$$\mathbf{X}(F) \times F^* \longrightarrow C^*\,; \quad (\chi\,,\, a) \longmapsto \chi(a)$$

induces a canonical isomorphism $F^* \xrightarrow{\sim} \mathrm{Hom}_{group}\left(\mathbf{X}(F)\,,\, C^*\right)$.

3. *(Orthogonality relations) For all $\chi \in \mathbf{X}(F)$,*

$$\sum_{a \in F^*} \chi(a) = \begin{cases} |F^*| = q - 1 & \text{if } \chi = \varepsilon\,, \\ 0 & \text{if } \chi \neq \varepsilon \end{cases}$$

and for all $a \in F^*$,

$$\sum_{\chi \in \mathbf{X}(F)} \chi(a) = \begin{cases} |\mathbf{X}(F)| = q - 1 & \text{if } a = 1\,, \\ 0 & \text{if } a \neq 1\,. \end{cases}$$

Proposition 1.3.6. *The function*

$$\psi : F \longrightarrow C^* ; \quad \alpha \longmapsto \zeta^{\mathrm{Tr}_{F/\mathbb{F}_p}(\alpha)}$$

has the following properties:

1. *ψ is a homomorphism from the additive group F to the multiplicative group C^*. Sometimes we say that ψ is an* **additive character** *of F.*
2. *There is an $\alpha \in F$ such that $\psi(\alpha) \neq 1$.*
3. *$\sum_{\alpha \in F} \psi(\alpha) = 0$.*

Proof. Since the trace map is surjective (Prop. 1.2.8), choosing $\alpha \in F$ with $\mathrm{Tr}_{F/\mathbb{F}_p}(\alpha) = 1$ we get $\psi(\alpha) = \zeta \neq 1$. This proves (2). We leave it to the reader to prove the other two assertions. □

The following is a natural generalization of Lemma 1.1.2.

Corollary 1.3.7. *Let α, x, $y \in F$. Let $\psi : \alpha \mapsto \zeta^{\mathrm{Tr}_{F/\mathbb{F}_p}(\alpha)}$ be the function defined in Prop. 1.3.6.*

Then

$$\frac{1}{q} \sum_{\alpha \in F} \psi(\alpha(x-y)) = \delta(x,\, y) := \begin{cases} 1 & \text{if } x \equiv y \pmod{p}\,, \\ 0 & \text{otherwise}\,. \end{cases}$$

Proof. Exercise. □

Definition 1.3.8. Let χ be a character of F and $a \in F$. Let ψ be the function defined in Prop. 1.3.6. The sum

$$g_a(\chi) := \sum_{t \in F} \chi(t)\psi(at) = \sum_{t \in F} \chi(t)\zeta^{\mathrm{Tr}_{F/\mathbb{F}_p}(at)}$$

is called a ***Gauss sum*** belonging to the character χ. Its ***conjugate*** $\overline{g}_a(\chi)$ is defined as

$$\overline{g}_a(\chi) := g_{-a}(\overline{\chi}) = \sum_{t \in F} \overline{\chi}(t)\psi(-at) = \sum_{t \in F} \overline{\chi}(t)\zeta^{-\mathrm{Tr}_{F/\mathbb{F}_p}(at)}\,.$$

(Recall that by definition the conjugate $\overline{\chi}$ is the same as the inverse character χ^{-1} of χ.) If $C = \mathbb{C}$, $\overline{g}_a(\chi)$ is the usual conjugate of $g_a(\chi)$ as a complex number.

For $a = 1$, we will write $g(\chi) = g_1(\chi)$ and $\overline{g}(\chi) = \overline{g}_1(\chi)$. ■

Proposition 1.3.9. *Let $a \in F$ and $\chi \in \mathbf{X}(F)$. Then*

$$g_a(\chi) = \begin{cases} \chi(a^{-1})g(\chi) & \text{if } a \neq 0 \text{ and } \chi \neq \varepsilon\,, \\ 0 & \text{if } a \neq 0 \text{ and } \chi = \varepsilon\,, \\ 0 & \text{if } a = 0 \text{ and } \chi \neq \varepsilon\,, \\ q & \text{if } a = 0 \text{ and } \chi = \varepsilon\,. \end{cases}$$

Proof. If $a \neq 0$ and $\chi \neq \varepsilon$, it is easily checked that $\chi(a)g_a(\chi)$. If $a \neq 0$, then

$$g_a(\varepsilon) = \sum_{t \in F} \zeta^{\mathrm{Tr}_{F/\mathbb{F}_p}(at)} = \sum_{t \in F} \zeta^{\mathrm{Tr}_{F/\mathbb{F}_p}(t)} = \sum_{t \in F} \psi(t) = 0$$

by Prop. 1.3.6 (3). Finally, for $a = 0$ we have $g_0(\chi) = \sum_{t \in F} \chi(t)$. By the orthogonality relation (Thm. 1.3.5 (3)), $g_0(\varepsilon) = q$ and $g_0(\chi) = 0$ for $\chi \neq \varepsilon$. □

Proposition 1.3.10. *If $\chi \neq \varepsilon$, then*

$$\overline{g}(\chi) = \chi(-1)g(\overline{\chi}) \quad \text{and} \quad g(\chi)\overline{g}(\chi) = q\,.$$

(If $C = \mathbb{C}$, the second equality means $|g(\chi)| = \sqrt{q}$.)

Proof. Direct computation yields

$$\overline{g}(\chi) = \sum_{t \in F} \overline{\chi}(t)\psi(-t) = \overline{\chi}(-1) \sum_{t \in F} \overline{\chi}(-t)\psi(-t) = \chi(-1) \sum_{t \in F} \overline{\chi}(t)\psi(t) = \chi(-1)g(\overline{\chi})\,.$$

We have used the fact that $\overline{\chi}(-1) = \chi(-1)$, which is obvious since $\chi(-1)^2 = \chi(1) = 1$.

It remains to prove the second equality. The proof is similar to that of Remark 1.1.4: We calculate the sum $\sum_{a \in F} g_a(\chi)\overline{g}_a(\chi)$ in two ways.

By Prop. 1.3.9,

$$g_a(\chi)\overline{g}_a(\chi) = \begin{cases} \chi(a^{-1})g(\chi)\overline{\chi}(a^{-1})\overline{g}(\chi) = g(\chi)\overline{g}(\chi) & \text{if } a \neq 0\,, \\ 0 & \text{if } a = 0\,. \end{cases}$$

So our sum has the value $(q-1)g(\chi)\overline{g}(\chi)$.

On the other hand,

$$g_a(\chi)\overline{g}_a(\chi) = \sum_{x,\, y \in F} \chi(x)\overline{\chi}(y)\psi(a(x-y))\,.$$

Summing both sides over $a \in F$ and using Cor. 1.3.7, we find

$$\sum_{a \in F} g_a(\chi)\overline{g}_a(\chi) = (q-1)q\,.$$

Since $q - 1 \neq 0$ in C, the result follows. □

Remark 1.3.11. Suppose p is odd and $F = \mathbb{F}_p$. If χ is the Legendre symbol, we have $\chi(a) = \chi(a^{-1})$ for $a \in F^*$ and $\overline{\chi} = \chi$. So the two equalities in (1.1.3.2) are generalized in Props. 1.3.9 and 1.3.10. ■

1.4 Jacobi sums over finite fields

Jacobi sum is a notion closely related to Gauss sums. As we will see, it provides a simple means of counting solutions of equations over finite fields.

Recall that F denotes a finite extension of $\mathbb{F}_p$ and $q = |F|$.

Definition 1.4.1. Let $\chi_1, \cdots, \chi_r$ $(r \geq 1)$ be characters of the field F. The associated ***Jacobi sum*** is defined by the formula

$$J(\chi_1, \cdots, \chi_r) := \sum_{\substack{t_i \in F \\ t_1 + \cdots + t_r = 1}} \chi_1(t_1)\chi_2(t_2)\cdots\chi_r(t_r)\,. \tag{1.4.1.1}$$

(If $r = 1$, then $J(\chi_1) = 1$.)

We will also use the sum, which will be left unnamed:

$$J_0(\chi_1, \cdots, \chi_r) := \sum_{\substack{t_i \in F \\ t_1 + \cdots + t_r = 0}} \chi_1(t_1)\chi_2(t_2)\cdots\chi_r(t_r)\,. \tag{1.4.1.2}$$

(If $r = 1$, then $J(\chi_1) = \chi_1(0)$.) ■

Proposition 1.4.2. *With notation as in Definition 1.4.1 we have:*

1. *If $\chi_1 = \cdots = \chi_r = \varepsilon$, then $J(\chi_1, \cdots, \chi_r) = J_0(\chi_1, \cdots, \chi_r) = q^{r-1}$.*
2. *If some but not all the χ_i are trivial, then $J(\chi_1, \cdots, \chi_r) = J_0(\chi_1, \cdots, \chi_r) = 0$.*
3. *Assume that $\chi_r \neq \varepsilon$. Then*

$$J_0(\chi_1, \cdots, \chi_r) = \begin{cases} \chi_r(-1)(q-1)J(\chi_1, \cdots, \chi_{r-1}) & \text{if } \chi_1\chi_2\cdots\chi_r = \varepsilon\,, \\ 0 & \text{otherwise}\,. \end{cases}$$

Proof. (1) follows easily from the fact

$$\#\left\{(t_1, \cdots, t_r) \in F^{\oplus r} \;\middle|\; \sum t_i = 1\right\} = \#\left\{(t_1, \cdots, t_r) \in F^{\oplus r} \;\middle|\; \sum t_i = 0\right\} = |F|^{r-1}\,.$$

(2) We may assume that $\chi_1, \cdots, \chi_s$ are nontrivial and that $\chi_{s+1} = \cdots = \chi_r = \varepsilon$ for some $1 \leq s < r$. Then

$$\begin{aligned} J(\chi_1, \cdots, \chi_r) &= \sum_{t_1 + \cdots + t_r = 0} \chi_1(t_1)\cdots\chi_r(t_r) = \sum_{t_1, \cdots, t_{r-1}} \chi_1(t_1)\cdots\chi_s(t_s) \\ &= q^{r-s-1}\left(\sum_{t_1}\chi_1(t_1)\right)\cdots\left(\sum_{t_s}\chi_s(t_s)\right) = 0\,. \end{aligned}$$

Here we have used the first orthogonality relation in Thm. 1.3.5 (3).

Similarly, $J_0(\chi_1, \cdots, \chi_r) = 0$.

(3) Since $\chi_r \neq \varepsilon$, we have $\chi_r(0) = 0$. Thus,

$$J_0(\chi_1, \cdots, \chi_r) = \sum_{a \in F^*} \left(\sum_{t_1 + \cdots + t_{r-1} = -a} \chi_1(t_1) \cdots \chi_{r-1}(t_{r-1}) \right) \chi_r(a)$$

$$\begin{aligned} (\text{putting } t_i' = -a^{-1} t_i) \quad &= \sum_{a \in F^*} \chi_1 \cdots \chi_{r-1}(-a) \left(\sum_{t_1' + \cdots + t_{r-1}' = 1} \chi_1(t_1') \cdots \chi_{r-1}(t_{r-1}') \right) \chi_r(a) \\ &= \chi_1 \cdots \chi_{r-1}(-1) J(\chi_1, \cdots, \chi_{r-1}) \sum_{a \in F^*} \chi_1 \cdots \chi_r(a) \,. \end{aligned}$$

By the first orthogonality relation again,

$$\sum_{a \in F^*} \chi_1 \cdots \chi_r(a) = \begin{cases} q-1 & \text{if } \chi_1 \cdots \chi_r = \varepsilon \,, \\ 0 & \text{otherwise} \,. \end{cases}$$

So the result follows. □

Now we relate Jacobi sums to Gauss sums.

Theorem 1.4.3. *Assume that $\chi_1, \cdots, \chi_r$ are nontrivial characters on F. Then*

$$g(\chi_1) g(\chi_2) \cdots g(\chi_r) = \begin{cases} \chi_r(-1)(q-1) J(\chi_1, \cdots, \chi_{r-1}) - J(\chi_1, \cdots, \chi_r) & \text{if } \chi_1 \cdots \chi_r = \varepsilon \\ J(\chi_1, \cdots, \chi_r) g(\chi_1 \cdots \chi_r) & \text{otherwise.} \end{cases}$$

Proof. Recall that the Gauss sum $g(\chi)$ is given by $g(\chi) = \sum_{t \in F} \chi(t)\psi(t)$, where $\psi(t) = \zeta^{\mathrm{Tr}_{F/\mathbb{F}_p}(t)}$. We have

$$\begin{aligned} g(\chi_1) \cdots g(\chi_r) &= \sum_{t_1, \cdots, t_r} \chi_1(t_1) \chi_2(t_2) \cdots \chi_r(t_r) \psi(t_1) \cdots \psi(t_r) \\ &= \sum_{a \in F} \left(\sum_{t_1 + \cdots + t_r = a} \chi_1(t_1) \chi_2(t_2) \cdots \chi_r(t_r) \right) \psi(a) \,. \end{aligned}$$

For $a = 0$, $\sum_{t_1 + \cdots + t_r = a} \chi_1(t_1) \cdots \chi_r(t_r) = J_0(\chi_1, \cdots, \chi_r)$. For $a \neq 0$, the substitution $t_i' = a^{-1} t_i$ shows that

$$\sum_{t_1 + \cdots + t_r = a} \chi_1(t_1) \chi_2(t_2) \cdots \chi_r(t_r) = \chi_1 \cdots \chi_r(a) J(\chi_1, \cdots, \chi_r) \,.$$

Notice that $\sum_{a \in F^*} \psi(a) = \sum_{a \in F} \psi(a) - \psi(0) = -1$ by Prop. 1.3.6 (3). Putting these observations together and using Prop. 1.4.2 (3), we obtain

$$\begin{aligned} g(\chi_1) \cdots g(\chi_r) &= J_0(\chi_1, \cdots, \chi_r) + J(\chi_1, \cdots, \chi_r) \sum_{a \in F^*} \chi_1 \cdots \chi_r(a) \psi(a) \\ &= \begin{cases} \chi_r(-1)(q-1) J(\chi_1, \cdots, \chi_{r-1}) - J(\chi_1, \cdots, \chi_r) & \text{if } \chi_1 \cdots \chi_r = \varepsilon \\ J(\chi_1, \cdots, \chi_r) g(\chi_1 \cdots \chi_r) & \text{otherwise} \end{cases} \end{aligned}$$

as asserted in the theorem. □

Corollary 1.4.4. *Assume that $\chi_1, \cdots, \chi_r$ $(r \geq 2)$ are nontrivial characters on F and that $\chi_1 \cdots \chi_r = \varepsilon$.*

Then

$$g(\chi_1)g(\chi_2)\cdots g(\chi_r) = q\chi_r(-1)J(\chi_1, \cdots, \chi_{r-1})\,.$$

Proof. Since $\chi_1 \cdots \chi_{r-1} = \chi_r^{-1} = \overline{\chi}_r$, we have

$$g(\chi_1 \cdots \chi_r)g(\chi_r) = g(\overline{\chi}_r)g(\chi_r) = \chi_r(-1)\overline{g}(\chi_r)g(\chi_r) = q\chi_r(-1)$$

by Prop. 1.3.10. On the other hand, Thm. 1.4.3 yields

$$g(\chi_1)\cdots g(\chi_{r-1}) = J(\chi_1, \cdots, \chi_{r-1})g(\chi_1 \cdots \chi_{r-1})\,.$$

Multiplying both sides by $g(\chi_r)$ proves the desired result. □

Corollary 1.4.5. *Let the hypotheses be as in Corollary 1.4.4.*

Then

$$J(\chi_1, \cdots, \chi_r) = -\chi_r(-1)J(\chi_1, \cdots, \chi_{r-1})\,.$$

Proof. We have seen in Thm. 1.4.3 that

$$g(\chi_1)\cdots g(\chi_r) = \chi_r(-1)(q-1)J(\chi_1, \cdots, \chi_{r-1}) - J(\chi_1, \cdots, \chi_r)\,.$$

The left hand side is equal to $q\chi_r(-1)J(\chi_1, \cdots, \chi_{r-1})$ by Cor. 1.4.4. So the result follows. □

Theorem 1.4.6. *Let us assume $C = \mathbb{C}$. Assume that $\chi_1, \cdots, \chi_r$ are nontrivial characters on F.*

1. *If $\chi_1 \cdots \chi_r \neq \varepsilon$, then*
$$|J(\chi_1, \cdots, \chi_r)| = q^{\frac{r-1}{2}}\,.$$
2. *If $\chi_1 \cdots \chi_r = \varepsilon$, then*
$$|J_0(\chi_1, \cdots, \chi_r)| = (q-1)q^{\frac{r}{2}-1} \quad \textit{and} \quad |J(\chi_1, \cdots, \chi_r)| = q^{\frac{r}{2}-1}\,.$$

Proof. In Prop. 1.3.10 we have seen that for a nontrivial character χ, $|g(\chi)| = q^{1/2}$. So (1) is immediate from Thm. 1.4.3. The first equality in (2) follows similarly, and for the second equality in (2) one can simply apply Cor. 1.4.5. □

1.5 Equations over finite fields

In this section, we show some examples of using Jacobi sums to count solutions of equations of certain particular type. We assume all characters take values in the field $C = \mathbb{C}$.

(1.5.1) First assume $|F| = q$ is odd. Then there is a unique character χ of order two on F, i.e., $\chi^2 = \varepsilon$ and $\chi \neq \varepsilon$. As an easy exercise, one can show that

$$\chi(-1) = (-1)^{\frac{q-1}{2}} \quad \text{and} \quad N(X^2 = a) = 1 + \chi(a) \ \text{ for all } a \in F\,.$$

Thus, for any $r \geq 1$, we have

$$\begin{aligned}
&N(X_1^2 + \cdots + X_r^2 = 1) \\
&= \sum_{a_1+\cdots+a_r=1} N(X_1^2 = a_1) \cdots N(X_r^2 = a_r) = \sum_{a_1+\cdots+a_r=1} \big(1 + \chi(a_1)\big) \cdots \big(1 + \chi(a_r)\big) \\
&= \sum_{a_1+\cdots+a_r=1} \big(\varepsilon(a_1) + \chi(a_1)\big) \cdots \big(\varepsilon(a_r) + \chi(a_r)\big) \\
&= \sum_{a_1+\cdots+a_r=1} \sum_{\chi_1,\cdots,\chi_r \in \{\varepsilon,\chi\}} \chi_1(a_1) \cdots \chi_n(a_r) = \sum_{\chi_1,\cdots,\chi_r \in \{\varepsilon,\chi\}} J(\chi_1, \cdots, \chi_r) \\
&= J(\varepsilon, \cdots, \varepsilon) + J(\chi, \cdots, \chi) = q^{r-1} + J(\chi, \cdots, \chi) \quad \text{by Prop. 1.4.2 (1) and (2)}.
\end{aligned}$$

We may use Thm. 1.4.3 and Cor. 1.4.5 to evaluate $J(\chi, \cdots, \chi)$.

Indeed, if r is odd, then $\chi^r = \chi \neq \varepsilon$, so that by Thm. 1.4.3,

$$J(\chi, \cdots, \chi) = g(\chi)^{r-1}.$$

Note that $g(\chi)^2 = \chi(-1)q$ by Prop. 1.3.10. It follows that when r is odd,

$$J(\chi, \cdots, \chi) = \big(\chi(-1)q\big)^{\frac{r-1}{2}} = (-1)^{\frac{q-1}{2}\cdot\frac{r-1}{2}} q^{\frac{r-1}{2}}.$$

If r is even, then the above formula combined with Cor. 1.4.5 yields

$$J(\chi, \cdots, \chi) = -\chi(-1) \cdot (-1)^{\frac{q-1}{2}\cdot\frac{r-2}{2}} q^{\frac{r-2}{2}} = -(-1)^{\frac{q-1}{2}\cdot\frac{r}{2}} q^{\frac{r}{2}-1}.$$

We have thus obtained an explicit formula for $N(X_1^2 + \cdots + X_r^2 = 1)$, which we restate in Prop. 1.5.2 below. ■

Proposition 1.5.2. *Suppose $|F| = q$ is odd and $r \in \mathbb{N}^*$. Then*

$$N(X_1^2 + \cdots + X_r^2 = 1) = \begin{cases} q^{r-1} + (-1)^{\frac{q-1}{2}\cdot\frac{r-1}{2}} q^{\frac{r-1}{2}} & \text{if } r \text{ is odd}, \\ q^{r-1} - (-1)^{\frac{q-1}{2}\cdot\frac{r}{2}} q^{\frac{r}{2}-1} & \text{if } r \text{ is even}. \end{cases}$$

Next we prove a general theorem.

Theorem 1.5.3. *Let $r \in \mathbb{N}^*$, $a_1, \cdots, a_r \in F^*$, $b \in F$ and suppose $n_1, \cdots, n_r \in \mathbb{N}^*$ are divisors of $q-1$. Put $N = N(a_1X_1^{n_1} + \cdots + a_rX_r^{n_r} = b)$ and define*

$$\begin{aligned}
\mathcal{C} &:= \{(\chi_1, \cdots, \chi_r) \in \mathbf{X}(F)^{\oplus r} \,|\, \chi_i^{n_i} = \varepsilon \neq \chi_i \text{ for every } i\}, \\
\mathcal{C}_0 &:= \{(\chi_1, \cdots, \chi_r) \in \mathbf{X}(F)^{\oplus r} \,|\, \chi_i^{n_i} = \varepsilon \neq \chi_i \text{ for every } i \text{ and } \chi_1 \cdots \chi_r = \varepsilon\}, \\
\mathcal{C}_1 &:= \{(\chi_1, \cdots, \chi_r) \in \mathbf{X}(F)^{\oplus r} \,|\, \chi_i^{n_i} = \varepsilon \neq \chi_i \text{ for every } i \text{ and } \chi_1 \cdots \chi_r \neq \varepsilon\}.
\end{aligned}$$

1. *If $b = 0$, then*

$$N = q^{r-1} + \sum_{(\chi_1,\cdots,\chi_r)\in\mathcal{C}_0} \chi_1(a_1^{-1}) \cdots \chi_r(a_r^{-1}) J_0(\chi_1, \cdots, \chi_r)$$

and $|N - q^{r-1}| \leq |\mathcal{C}_0|(q-1)q^{\frac{r}{2}-1}$.

2. *If $b \neq 0$, then*

$$N = q^{r-1} + \sum_{(\chi_1,\cdots,\chi_r)\in\mathcal{C}} \chi_1\cdots\chi_r(b)\chi_1(a_1^{-1})\cdots\chi_r(a_r^{-1})J(\chi_1,\cdots,\chi_r)$$

and $|N - q^{r-1}| \leq |\mathcal{C}_0|q^{\frac{r}{2}-1} + |\mathcal{C}_1|q^{\frac{r-1}{2}}$.

Proof. Recall that by Prop. 1.3.4, $N(X_i^{n_i} = u_i) = \sum_{\chi_i^{n_i}=\varepsilon} \chi_i(u_i)$ for any $u_i \in F$. Hence

$$\begin{aligned} N &= \sum_{a_1u_1+\cdots+a_ru_r=b} N(X_1^{n_1} = u_1)\cdots N(X_r^{n_r} = u_r) \\ &= \sum_{\chi_1^{n_1}=\cdots=\chi_r^{n_r}=\varepsilon} \sum_{a_1u_1+\cdots+a_ru_r=b} \chi_1(u_1)\cdots\chi_r(u_r) \end{aligned}$$

If $b = 0$, let $t_i = a_iu_i$. Then

$$\sum_{a_1u_1+\cdots+a_ru_r=b} \chi_1(u_1)\cdots\chi_r(u_r) = \chi_1(a_1^{-1})\cdots\chi_r(a_r^{-1})J_0(\chi_1,\cdots,\chi_r)\,.$$

If $b \neq 0$, let $t_i = b^{-1}a_iu_i$. Then

$$\sum_{a_1u_1+\cdots+a_ru_r=b} \chi_1(u_1)\cdots\chi_r(u_r) = \chi_1\cdots\chi_r(b)\chi_1(a_1^{-1})\cdots\chi_r(a_r^{-1})J(\chi_1,\cdots,\chi_r)\,.$$

Applying Prop. 1.4.2 to finish the computation, we get the desired result. □

Theorem 1.5.3 is due originally to Weil [Wei49] and independently (and almost simultaneously) to Loo-Keng Hua (华罗庚) and H.S. Vandiver [HV49]. Inspired by this theorem (and some further results), Weil raised the famous *Weil conjectures*, which are proved in full generality by Pierre Deligne in 1974 [Del74]. The proof utilizes the most advanced techniques of modern algebraic geometry in the 1970s and represents one of the most remarkable mathematical achievements in the 20th century.

2 Algebraic Integers and Number Fields

2.1 Integral extensions

In this section, let $A \subseteq B$ be an inclusion of rings.

2.1.1 Integral elements and integral closures

Definition 2.1.1. An element $x \in B$ is said to be ***integral*** over A if there is a monic polynomial $f(t) \in A[t]$ such that $f(x) = 0$. In other words, x satisfies an equation

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

with coefficients $a_i \in A$ and $n \geq 1$. Such an equation will be called an ***integral equation*** of x over A. The ***minimal polynomial*** of x over A is the unique monic polynomial $f \in A[t]$ such that $f(x) = 0$ is an integral equation of minimal degree.

We say B is ***integral*** over A if every element of B is integral over A. In this case, we shall say that $A \subseteq B$ is an ***integral extension*** of rings. ■

Proposition 2.1.2. *For every $x \in B$, the following assertions are equivalent:*

(i) *x is integral over A.*

(ii) *The subring $A[x]$ of B generated by x and A is a finitely generated A-module.*

(iii) *There exists a subring $A' \subseteq B$ containing $A[x]$ such that A' is finitely generated as an A-module.*

(iv) *B contains a finitely generated A-submodule M satisfying the following two properties:*

(a) $xM \subseteq M$, i.e., M is an $A[x]$-module.

(b) The annihilator of M in $A[x]$ is zero, i.e.,

$$\mathrm{Ann}_{A[x]}(M) := \{z \in A[x] \,|\, zM = 0\} = 0\,.$$

Proof. The implications (i)⇒(ii)⇒(iii)⇒(iv) are easy. We now prove (iv)⇒(i). Assume M is generated by $v_1 \ldots, v_n \in M$ as an A-module. Then there is a square matrix $C = (\alpha_{ij})$ of order n with coefficients in A such that

$$(xv_1, \ldots, xv_n) = (v_1, \ldots, v_n)C\,.$$

Let I_n be the identity matrix of order n. Then $D := xI_n - C$ is a square matrix with coefficients in $A[x]$ such that

$$(v_1, \ldots, v_n)D = 0\,.$$

Let $D^* = (d^*_{ij})$ denote the adjunct matrix of D, i.e., $d^*_{ij} = (-1)^{i+j}\det(D_{ij})$, where D_{ij} is obtained from D by deleting the i-th column and the j-th row. Then we have $DD^* = \det(D)I_n$. Therefore, we have

$$(v_1, \ldots, v_n).\det(xI - C) = (v_1, \ldots, v_n)DD^* = (0, \cdots, 0)$$

which shows $\det(xI - C) \in \mathrm{Ann}_{A[x]}(M) = 0$. Hence $\det(xI_n - C) = 0$. Developing the determinant $\det(xI_n - C)$ yields an integral equation of x over A. □

Proposition 2.1.3. *The set A' of elements of B which are integral over A is a subring of B, called the* **integral closure** *of A in B.*

Proof. Let x, $y \in A'$. By Prop. 2.1.2, the subrings $A[x] \subseteq B$ and $A[y] \subseteq B$ are finitely generated A-modules. The subring $A[x, y]$ is thus finitely generated as an A-module. Since $x \pm y$, $xy \in A[x, y]$, we conclude from Prop. 2.1.2 (iii) that $x \pm y$ and xy are integral over A. □

Proposition 2.1.4. *Let $A \subseteq B$ be an inclusion of rings. Then the following assertions are equivalent:*

(i) *B is integral over A and is finitely generated as an A-algebra.*

(ii) *B is finitely generated as an A-module.*

Proof. (ii)⇒(i). This is immediate from Prop. 2.1.2 (iii).

(i)⇒(ii). We may prove this by induction on the number of ring generators, and thus we may assume that $B = A[x]$ for some $x \in B$ integral over A. But then the result is shown in Prop. 2.1.2. □

Proposition 2.1.5. *Let $A \subseteq B \subseteq C$ be three rings. If B is integral over A and C is integral over B, then C is integral over A.*

Proof. Let $x \in C$. Then x satisfies an integral equation

$$x^n + b_{n-1}x^{n-1} + \cdots + b_0 = 0$$

with $b_i \in B$. Let $B_1 = A[b_0, \ldots, b_{n-1}]$. Since every b_i is integral over A, B_1 is a finitely generated A-module by Prop. 2.1.4. $B_1[x]$ is a finitely generated B_1-module, whence a finitely generated A-module. By Prop. 2.1.4, $B_1[x]$ is integral over A. In particular, x is integral over A. □

Definition 2.1.6. Let $A \subseteq B$ be an inclusion of rings. We say A is ***integrally closed*** in B if the integral closure of A in B is equal to A itself. An integral domain is called ***integrally closed*** if it is integrally closed in its fraction field. ■

Lemma 2.1.7. *Let S be a multiplicative subset of A not containing 0. Let A' be the integral closure of A in B.*

Then $S^{-1}A'$ is the integral closure of $S^{-1}A$ in $S^{-1}B$.

In particular, if A is an integrally closed domain, then so is $S^{-1}A$.

Proof. Exercise. □

Corollary 2.1.8. *Let A be an integrally closed domain with fraction field K and L/K an algebraic field extension. Let B be the integral closure of A in L.*

Then $K.B = K \otimes_A B = L$, L is the fraction field of B, and B is integrally closed.

Proof. Take $S = A \setminus \{0\}$, so that $K = S^{-1}A$, $K.B = S^{-1}B = K \otimes_A B$. Lemma 2.1.7 shows that the integral closure of $K = S^{-1}A$ in $L = S^{-1}L$ is $S^{-1}B$. Since L/K is an algebraic extension, it is obvious that L is the integral closure of K in L. The first assertion is thus proved, and the second one is then immediate. The third assertion follows easily from the second, in view of Prop. 2.1.5. □

(2.1.9) Let R be an integral domain and let R^* denotes its group of units. Recall that an element $\pi \in R$ is called a ***prime element***[†] if the ideal πR is a nonzero prime ideal in R. An ***irreducible element*** in R is a nonzero, non-unit element $p \in R$ satisfying the following condition: whenever a factorization $p = ab$ with $a, b \in R$, we must have $a \in R^*$ or $b \in R^*$. Prime elements are all irreducible.

[†]In these notes, only occasionally the Greek letter π will refer to the circular constant (the ratio of the circumference of a circle to its diameter). In most of the time, we use π for other purposes. The context should make the usage clear.

A ***UFD*** (***unique factorization domain***) is an integral domain in which every nonzero non-unit element a has a factorization $a = up_1 \cdots p_r$ where $u \in R^*$ and $p_i \in R$ are irreducible, and such a factorization is unique up to units and recordings. In a UFD irreducible elements are also prime.

Any principal ideal domain (PID) is a UFD. If R is a UFD, then so is the polynomial ring $R[X_1, \cdots, X_n]$ for every $n \in \mathbb{N}^*$. ■

Proposition 2.1.10. *Every UFD is integrally closed.*

Proof. Exercise. □

Proposition 2.1.11. *Let A be an integral domain with fraction field K, L/K a finite extension and $N_{L/K} : L \to K$ and $\mathrm{Tr}_{L/K} : L \to K$ the norm map and the trace map. Let $x \in L$ and let*

$$f(t) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \ \in \ K[t]$$

be the minimal polynomial of x over K.

If x is integral over A, then all the elements $N_{L/K}(x)$, $\mathrm{Tr}_{L/K}(x)$ and $a_0, \ldots, a_{n-1}$ are integral over A.

Proof. By Thm. 1.2.4 (1),

$$N_{L/K}(x) = N_{K(x)/K}(x)^{[L:K(x)]} \quad \text{and} \quad \mathrm{Tr}_{L/K}(x) = [L : K(x)]\,\mathrm{Tr}_{K(x)/K}(x)\,,$$

so we may assume $L = K(x) = K[t]/(f(t))$. Then $N_{L/K}(x) = (-1)^n a_0$ and $\mathrm{Tr}_{L/K}(x) = -a_{n-1}$. It suffices to show that $f(t)$ has coefficients in the integral closure A' of A in K. To see this, let $p(t) \in A[t]$ be the minimal polynomial of x over A. Then $f(t) \,|\, p(t)$ in $K[t]$. Since every root of $p(t)$ in the algebraic closure $\overline{K}$ of K is integral over A, so is every root of $f(t)$. By Viète's theorem, each coefficient of f can be expressed as elementary symmetric polynomials of its roots, hence is integral over A. □

Proposition 2.1.12. *Let A be a Noetherian integrally closed domain with fraction field K and let L/K be a finite* **separable** *field extension.*

Then the integral closure B of A in L is finitely generated as an A-module.

Proof. Let $\mathrm{Tr} : L \to K$ be the trace map of the extension L/K. For every A-submodule M of L, define its ***dual***

$$M^{\#} := \{\, x \in L \,|\, \mathrm{Tr}(xM) \subseteq A \,\}\,.$$

By Prop. 2.1.11, we have $B \subseteq B^{\#}$. Let $\{\, e_i \,\}$ be a basis of L over K with $e_i \in B$ and let V be the free A-module generated by $\{\, e_i \,\}$. Obviously, $V \subseteq B \subseteq B^{\#} \subseteq V^{\#}$.

By Cor. 1.2.6, the condition of separability implies that the map

$$L \times L \longrightarrow K\,; \qquad (x,\, y) \longmapsto \langle x\,,\, y \rangle := \mathrm{Tr}(xy)$$

is a nondegenerate, symmetric bilinear form on the K-vector space L. Let $\{\, f_i \,\}$ be the dual basis of L with respect to the trace map. Then $V^{\#}$ is the free A-module generated by $\{\, f_i \,\}$. Indeed, for any $x \in V^{\#}$, we have $a_i := \mathrm{Tr}(xe_i) \in A$. Put $\alpha = \sum a_i f_i$. Then

$$\forall\ j = 1, \ldots, n\,, \quad \mathrm{Tr}(\alpha e_j) = \sum_i a_i\,\mathrm{Tr}(f_i e_j) = a_j = \mathrm{Tr}(xe_j)\,.$$

Therefore, $\alpha - x$ is orthogonal to every e_j with respect to Tr. As Tr is nondegenerate, $x = \alpha \in \oplus A f_i$, proving that $V^{\#} = \oplus A f_i$. Thus, it follows from the Noetherian hypothesis on A that B is finitely generated as an A-module. □

2.1.2 Prime ideals in an integral extension

Lemma 2.1.13. *Let $A \subseteq B$ be an inclusion of rings with B integral over A. Let $\mathfrak{P} \subseteq \mathfrak{Q}$ be an inclusion of prime ideals of B such that $\mathfrak{P} \cap A = \mathfrak{Q} \cap A$. Then $\mathfrak{P} = \mathfrak{Q}$.*

Proof. Let $\mathfrak{p} = \mathfrak{P} \cap A$. Then $A' = A/\mathfrak{p}$ is a subring of $B' = B/\mathfrak{P}$ and B' is integral over A'. So, by passing to the quotient by $\mathfrak{P}$, we may assume $\mathfrak{P} = 0$. If $\mathfrak{Q} \neq 0$, there exists a nonzero $x \in \mathfrak{Q}$. Let

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0\,, \quad a_i \in A$$

the integral equation given by the minimal polynomial of x over A. One has $a_0 \neq A$, and $a_0 \in xB \subseteq \mathfrak{Q}$. Therefore, a_0 is a nonzero element of $\mathfrak{Q} \cap A = \mathfrak{P} \cap A = 0$, which is absurd. □

Proposition 2.1.14. *Let $A \subseteq B$ be an inclusion of integral domains with B integral over A.*

1. *B is a field if and only if A is a field.*
2. *If $\mathfrak{P}$ is a prime ideal of B and $\mathfrak{p} = \mathfrak{P} \cap A$, then $\mathfrak{P}$ is a maximal ideal of B if and only if $\mathfrak{p}$ is a maximal ideal of A.*

Proof. By considering the inclusion $A/\mathfrak{p} \hookrightarrow B/\mathfrak{p}$, we see that (1) implies (2).

First assume A is a field. Let $x \in B$ be a nonzero element. Let

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

be the integral equation given by the minimal polynomial of x over A. Since B is a domain, we must have $a_0 \neq 0$. It follows that

$$x.(x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1) \cdot (-a_0)^{-1} = 1$$

whence $x^{-1} \in B$.

Conversely, if B is a field and $a \neq 0$ is a nonzero element of A, then $x = a^{-1}$ exists in B and satisfies an integral equation as above. Thus,

$$x = x^n a^{n-1} = a^{n-1}(-a_{n-1}x^{n-1} - \cdots - a_0) = -a_{n-1} - a_{n-2}a - \cdots - a^{n-1}a_0 \in A\,.$$

This shows that A is a field. □

Let $\varphi : R \to S$ be a ring homomorphism and let I and J be ideals of R and S respectively. One says that J ***lies over*** I if $I = \varphi^{-1}(J)$. In particular, for an inclusion of rings $A \subseteq B$, an ideal J of B lies over an ideal I of A if $I = J \cap A$.

Proposition 2.1.15. *Let $A \subseteq B$ be an integral extension of rings and $\mathfrak{p}$ a prime ideal of A.*

Then the ideal $\mathfrak{p}B$ lies over $\mathfrak{p}$ (so in particular $\mathfrak{p}B \neq B$), and there exists a prime ideal $\mathfrak{P}$ of B lying over $\mathfrak{p}$.

Proof. The second assertion is stronger than the first one. So we need only to show the existence of $\mathfrak{P}$.

Let $\varphi : A \to A_{\mathfrak{p}}$ be the natural map and $\phi : B \to B_{\mathfrak{p}} = B \otimes_A A_{\mathfrak{p}}$ the extension to B. The induced map $A_{\mathfrak{p}} \to B_{\mathfrak{p}} = B \otimes_A A_{\mathfrak{p}}$ is injective (although φ may not be injective).

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & A_{\mathfrak{p}} \\ \downarrow & & \downarrow \\ B & \xrightarrow{\phi} & B_{\mathfrak{p}} \end{array}$$

If $\mathfrak{P}'$ is a prime ideal of $B_{\mathfrak{p}}$ lying over $\mathfrak{p}A_{\mathfrak{p}}$, then $\mathfrak{P} := \phi^{-1}(\mathfrak{P}')$ is a prime ideal of B such that $\mathfrak{P} \cap A = \varphi^{-1}(\mathfrak{p}A_{\mathfrak{p}}) = \mathfrak{p}$. We may therefore reduce to the case where $A = A_{\mathfrak{p}}$ is local and $\mathfrak{p}$ is the maximal ideal of A.

Now take any maximal ideal $\mathfrak{P}$ of B. By Prop. 2.1.14, $\mathfrak{P} \cap A$ is a maximal ideal of A. Hence $\mathfrak{P} \cap A$ is equal to the unique maximal ideal $\mathfrak{p}$ of A. The proposition is thus proved. □

2.1.3 Decomposition group and inertia group

In this subsection, let A denote an integrally closed domain with fraction field K, L/K a finite Galois extension with Galois group $G = \mathrm{Gal}(L/K)$, and B the integral closure of A in L. From the definition we see easily that for every $\sigma \in G$, $\sigma(B) = B$ and if $\mathfrak{P}$ is a prime ideal of B, $\sigma(\mathfrak{P}) \cap A = \sigma(\mathfrak{P}) \cap \sigma(A) = \sigma(\mathfrak{P} \cap A)$ (the last equality following from the injectivity of σ).

Proposition 2.1.16. *With notation as above, let $\mathfrak{p}$ be a prime ideal of A, and let $\mathfrak{P}$, $\mathfrak{Q}$ be prime ideals of B lying over $\mathfrak{p}$.*

Then there exists $\sigma \in G$ such that $\sigma\mathfrak{P} = \mathfrak{Q}$.

In particular, the number of prime ideals of B lying over $\mathfrak{p}$ is at most $|G| = [L : K]$.

Proof. By localization at $\mathfrak{p}$, we may assume $\mathfrak{p}$ is a maximal ideal. Thus, by Prop. 2.1.14, prime ideals lying over $\mathfrak{p}$ are maximal and hence coprime to each other. Suppose that $\mathfrak{Q} \neq \sigma\mathfrak{P}$ for any $\sigma \in G$. Then by the Chinese remainder theorem, there exists an element $x \in B$ such that

$$\begin{cases} x \equiv 0 \pmod{\mathfrak{Q}} \\ x \equiv 1 \pmod{\sigma\mathfrak{P}} \quad \text{for all } \sigma \in G\,. \end{cases}$$

On the one hand, the norm

$$N_{L/K}(x) = \prod_{\sigma \in G} \sigma(x)$$

lies in $A = B \cap K$ by Prop. 2.1.11. On the other hand, $x \in \mathfrak{Q}$ since $\sigma(x) = x \in \mathfrak{Q}$ for $\sigma = \mathrm{Id}$. Hence, $x \in \mathfrak{P} \cap A = \mathfrak{p} = \mathfrak{Q} \cap A$. But $x \notin \sigma\mathfrak{P}$ for all $\sigma \in G$, so that $\sigma(x) \notin \mathfrak{P}$ for

all $\sigma \in G$. This contradicts the fact that the product $\prod_{\sigma\in G} \sigma(x)$ lies in the prime ideal $\mathfrak{P}$ of B. □

(2.1.17) Let $\mathfrak{p}$ be a maximal ideal of A and $\mathfrak{P}$ a maximal ideal of B lying over $\mathfrak{p}$. We write $\kappa(\mathfrak{p}) = A/\mathfrak{p}$ and $\kappa(\mathfrak{P}) = B/\mathfrak{P}$ for the residue fields.

We define the ***decomposition group*** $G_{\mathfrak{P}}$ of $\mathfrak{P}$ by

$$G_{\mathfrak{P}} := \{\, \sigma \in G \,|\, \sigma\mathfrak{P} = \mathfrak{P} \,\}\,.$$

The fixed field $L_{\mathfrak{P}} := L^{G_{\mathfrak{P}}}$ is called the ***decomposition field*** of $\mathfrak{P}$. If B_0 denotes the integral closure of A in $L_{\mathfrak{P}}$ and $\mathfrak{P}_0 = \mathfrak{P} \cap B_0$, then Prop. 2.1.16 implies that $\mathfrak{P}$ is the only prime ideal of B lying over $\mathfrak{P}_0$. ■

Proposition 2.1.18. *With notation as in (2.1.17), we have:*

1. *If $G = \cup \sigma_j G_{\mathfrak{P}}$ is a coset decomposition of $G_{\mathfrak{P}}$ in G, then the prime ideals $\sigma_j\mathfrak{P}$ are precisely the distinct prime ideals of B lying over $\mathfrak{p}$. In particular, the number of such prime ideals is $[G : G_{\mathfrak{P}}] = [L_{\mathfrak{P}} : K]$.*
2. *For any $\sigma \in G$, the decomposition group of $\sigma\mathfrak{P}$ is $G_{\sigma\mathfrak{P}} = \sigma G_{\mathfrak{P}} \sigma^{-1}$.*
3. *The decomposition field $L_{\mathfrak{P}}$ is the smallest subfield E of L containing K such that $\mathfrak{P}$ is the only prime ideal of B lying over $\mathfrak{P} \cap E$ (which is a maximal ideal in $B \cap E$).*

Proof. For any two elements $\sigma, \tau \in G$, we have $\sigma\mathfrak{P} = \tau\mathfrak{P}$ if and only if $\tau^{-1}\sigma\mathfrak{P} = \mathfrak{P}$, i.e. $\tau^{-1}\sigma \in G_{\mathfrak{P}}$. From this one easily obtains (1) and (2).

(3) Let $H = \mathrm{Gal}(L/E)$ and $\mathfrak{q} = \mathfrak{P} \cap E$. Suppose that $\mathfrak{P}$ is the unique prime ideal of B lying over $\mathfrak{q}$. For any $\sigma \in H$, it is clear that $\sigma\mathfrak{P}$ lies over $\sigma\mathfrak{q} = \mathfrak{q}$. So we have $\sigma\mathfrak{P} = \mathfrak{P}$. Hence $H \subseteq G_{\mathfrak{P}}$ and $E \supseteq L_{\mathfrak{P}}$. □

Proposition 2.1.19. *With notation as in (2.1.17), let $B_0 = B \cap L_{\mathfrak{P}}$ be the integral closure of A in the decomposition field $L_{\mathfrak{P}}$, $\mathfrak{P}_0 = \mathfrak{P} \cap B_0$ and $\kappa(\mathfrak{P}_0) = B_0/\mathfrak{P}_0$.*

Then the natural injection $\kappa(\mathfrak{p}) = A/\mathfrak{p} \to \kappa(\mathfrak{P}_0) = B_0/\mathfrak{P}_0$ is an isomorphism.

Proof. Let $x \in B_0$. We need to show that there is an element $z \in A$ such that $z \equiv x \pmod{\mathfrak{P}_0}$.

For any $\sigma \in G$ not in $G_{\mathfrak{P}}$, one has $\sigma\mathfrak{P} \neq \mathfrak{P}$ and $\sigma^{-1}\mathfrak{P} \neq \mathfrak{P}$. Put

$$\mathfrak{Q}_\sigma := \sigma^{-1}\mathfrak{P} \cap B_0\,.$$

Since $\mathfrak{P}$ is the only prime ideal lying over $\mathfrak{P}_0$, we have $\mathfrak{Q}_\sigma \neq \mathfrak{P}_0$. By the Chinese remainder theorem, there exists an element $y \in B_0$ such that

$$y \equiv x \pmod{\mathfrak{P}_0} \quad \text{and} \quad y \equiv 1 \pmod{\mathfrak{Q}_\sigma} \ \text{ for all } \ \sigma \in G \setminus G_{\mathfrak{P}}\,.$$

In particular,

$$y \equiv x \pmod{\mathfrak{P}} \quad \text{and} \quad y \equiv 1 \pmod{\sigma^{-1}\mathfrak{P}} \ \text{ for all } \ \sigma \in G \setminus G_{\mathfrak{P}}\,.$$

The second congruence yields

$$\sigma(y) \equiv 1 \pmod{\mathfrak{P}} \text{ for all } \sigma \in G \setminus G_{\mathfrak{P}}\,.$$

Let $z = N_{L_{\mathfrak{P}}/K}(y)$ be the norm of y from $L_{\mathfrak{P}}$ to K. This is a product of y and some other factors of form $\sigma(y)$ with $\sigma \notin G_{\mathfrak{P}}$. Here we use the fact that for any subextension E/K of L/K, every K-embedding $E \hookrightarrow \overline{K}$ is the restriction of some $\tau \in \mathrm{Gal}(L/K) = \mathrm{Hom}_{K\text{-alg}}(L, \overline{K})$ (see e.g. [Mor96, Prop. 3.28]). Thus we obtain $z \equiv x \pmod{\mathfrak{P}}$, or equivalently, $z \equiv x \pmod{\mathfrak{P}_0}$ since both x and z lies in B_0. Finally, $z \in A$ by Prop. 2.1.11 (since A is integrally closed). This completes the proof of our proposition. □

(2.1.20) Notation being as in (2.1.17), the decomposition group $G_{\mathfrak{P}}$ operates in a natural way on the residue field $\kappa(\mathfrak{P}) = B/\mathfrak{P}$, and leaves $\kappa(\mathfrak{p}) = A/\mathfrak{p}$ fixed. We have thus a group homomorphism

$$G_{\mathfrak{P}} \longrightarrow \mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))\,; \qquad \sigma \longmapsto \bar{\sigma}\,.$$

Here for an arbitrary (not necessarily Galois) field extension E/F, we still denote by $\mathrm{Gal}(E/F)$ the group of all F-automorphisms of the field E. The kernel of this homomorphism, denoted

$$\begin{aligned} I_{\mathfrak{P}} :&= \{\sigma \in G_{\mathfrak{P}} \,|\, \sigma(x) \equiv x \pmod{\mathfrak{P}} \text{ for all } x \in B\} \\ &= \{\sigma \in G \,|\, \sigma(x) \equiv x \pmod{\mathfrak{P}} \text{ for all } x \in B\}\,, \end{aligned}$$

is called the ***inertia group*** of $\mathfrak{P}$. Its fixed field

$$L^{I_{\mathfrak{P}}} := \{x \in L \,|\, \forall\, \sigma \in I_{\mathfrak{P}}\,,\ \sigma(x) = x\}$$

is called the ***inertia field*** of $\mathfrak{P}$.

It is clear that $I_{\sigma\mathfrak{P}} = \sigma I_{\mathfrak{P}} \sigma^{-1}$ for any $\sigma \in G$. ■

Proposition 2.1.21. *With notation as in (2.1.20), the field extension $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ is normal (but not necessarily separable), the maximal separable subextension of $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ has degree bounded by $[L : K]$, and the homomorphism*

$$G_{\mathfrak{P}} \longrightarrow \mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))\,; \qquad \sigma \longmapsto \bar{\sigma}$$

is surjective.

Proof. The extension $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ is algebraic since B is integral over A. Let $\ell/\kappa(\mathfrak{p})$ be the maximal separable subextension of $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$.

Take any $\overline{x} \in \kappa(\mathfrak{P})$. We claim that all the roots of the minimal polynomial of $\overline{x}$ over $\kappa(\mathfrak{p})$ are still in $\kappa(\mathfrak{P})$, and that the extension $\kappa(\mathfrak{p})(\overline{x})/\kappa(\mathfrak{p})$ has degree bounded by $[L : K]$. This claim clearly implies that $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ is a normal extension, and that every simple extension contained in it has degree bounded by $[L : K]$. In particular, every finite separable extension in $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ has degree $\leq [L : K]$, from which it follows that $\ell/\kappa(\mathfrak{p})$ is a finite extension.

To prove the above claim, let $x \in B$ be a lifting of $\overline{x}$. The minimal polynomial f of x over K has coefficients in A and all the roots of f are integral over A. Since L/K is normal, the polynomial f splits into linear factors. Namely,

$$f(t) = \prod_{i=1}^{m}(t - x_i) \quad \text{with each } x_i \in B\,.$$

It follows that the reduction $\bar{f}$ of f in $\kappa(\mathfrak{p})[t]$ has the factorization $\bar{f}(t) = \prod(t - \bar{x}_i)$ with $\bar{x}_i \in \kappa(\mathfrak{P})$. The minimal polynomial of $\overline{x}$ over $\kappa(\mathfrak{p})$ divides $\bar{f}$, and hence has all its roots in $\kappa(\mathfrak{P})$. Moreover,

$$[\kappa(\mathfrak{p})(\overline{x}) : \kappa(\mathfrak{p})] \leq \deg(f) = [K(x) : K] \leq [L : K]\,.$$

This finishes the proof of our claim, whence the first two assertions in the proposition.

There remains to prove that the map $\sigma \to \overline{\sigma}$ is surjective. To do this, we shall give an argument which reduces our problem to the case when $\mathfrak{P}$ is the only prime ideal of B lying over $\mathfrak{p}$. Indeed, by Prop. 2.1.19, the residue fields $\kappa(\mathfrak{p})$ and $\kappa(\mathfrak{P}_0)$ are the same. This means that to prove our surjectivity, we may take the decomposition field $L_{\mathfrak{P}}$ as ground field. This is the desired reduction, and we can assume $K = L_{\mathfrak{P}}$ and $G = G_{\mathfrak{P}}$.

This being the case, take a generator of the maximal separable subextension $\ell/\kappa(\mathfrak{p})$, and let it be $\overline{x}$, for some $x \in B$. Let f be the minimal polynomial of x over K. Any automorphism of $\kappa(\mathfrak{P})$ is determined by its effect on $\bar{x}$, and maps $\overline{x}$ to some root of $\bar{f}$. Given any root x_i of f, there exists an element of $G = G_{\mathfrak{P}}$ such that $\sigma(x) = x_i$. Hence the automorphism of $\kappa(\mathfrak{P})$ over $\kappa(\mathfrak{p})$ induced by elements of G operate transitively on the roots of $\bar{f}$. Hence they give us all automorphisms of $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$, as was to be shown. □

Remark 2.1.22. In Prop. 2.1.21 we don't claim that $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ is a finite extension. In fact, when A is not Noetherian, this extension may not be finite (see [Bou06, p.74, Chap. V, Exercise 2.9 (c)] for a counterexample).

Fortunately, we are mostly interested in the case where A is Noetherian. In this case, B is a finitely generated A-module by Prop. 2.1.12 and hence $\kappa(\mathfrak{P})/\mathfrak{p}$ is a finite extension. ■

(2.1.23) As before, let $\mathfrak{p}$ be a fixed maximal ideal of A. We say $\mathfrak{p}$ ***splits completely*** in a finite extension E/K, if the integral closure of A in E has exactly $[E : K]$ prime ideals lying over $\mathfrak{p}$. For a finite Galois extension L/K, $\mathfrak{p}$ splits completely in L/K if and only if $G_{\mathfrak{P}} = 1$ because $\mathrm{Gal}(L/K)$ permutes the prime ideals over $\mathfrak{p}$ transitively. ■

A field extension is called an ***abelian extension*** if it is Galois and its Galois group is abelian.

Corollary 2.1.24. *Let L/K be an abelian extension with group $G = \mathrm{Gal}(L/K)$. Then the decomposition field $L_{\mathfrak{P}}$ is the largest subfield of L containing K in which $\mathfrak{p}$ splits completely.*

Proof. Let $G = \bigcup_{i=1}^{r} \sigma_i G_{\mathfrak{P}}$ be a coset decomposition of $G_{\mathfrak{P}}$ in G. We know that $\mathfrak{P}$ is the only prime ideal of B lying over $\mathfrak{P}_0 = \mathfrak{P} \cap L_{\mathfrak{P}}$. For each i, $\sigma_i\mathfrak{P}$ is the only prime ideal lying over $\sigma_i\mathfrak{P}_0$. Since L/K is abelian, $L_{\mathfrak{P}}/K$ is a Galois extension. So $\sigma_i\mathfrak{P}_0$ are prime

ideals of $B_0 = B \cap L_{\mathfrak{P}} = \sigma_i(B) \cap \sigma_i(L_{\mathfrak{P}})$. Since $\sigma_1\mathfrak{P}, \cdots, \sigma_r\mathfrak{P}$ are all distinct, it follows that $\sigma_1\mathfrak{P}_0, \ldots, \sigma_r\mathfrak{P}_0$ are distinct prime ideals lying over $\mathfrak{p}$. Now $r = [G : G_{\mathfrak{P}}] = [L_{\mathfrak{P}} : K]$. Hence $\mathfrak{p}$ splits completely in $L_{\mathfrak{P}}$.

Now let F be an intermediate field between K and L such that $\mathfrak{p}$ splits completely in F. Let $H = \mathrm{Gal}(L/F)$ and $\mathfrak{P}_F = \mathfrak{P} \cap F$. For every $\sigma \in G_{\mathfrak{P}}$, we have clearly $\sigma\mathfrak{P}_F = \mathfrak{P}_F$. However, the decomposition group of $\mathfrak{P}_F$ in $\mathrm{Gal}(F/K)$ must be trivial since $\mathfrak{p}$ splits completely in F. Therefore, the restriction of σ to F is the identity, proving that $G_{\mathfrak{P}} \subseteq H$. This implies that $F \subseteq L_{\mathfrak{P}}$, and concludes the proof of the corollary. □

2.2 Quadratic fields, cubic and quartic reciprocity

2.2.1 Algebraic integers in quadratic fields

(2.2.1) Let K be a subfield of $\mathbb{C}$ and consider the inclusion $\mathbb{Z} \subseteq K$. An element in K is called an ***algebraic integer*** if it is integral over $\mathbb{Z}$. The set of all algebraic integers in K is denoted by $\mathcal{O}_K$. It is a subring of K by Prop. 2.1.3, called the ***ring of algebraic integers*** (or simply the ***ring of integers***) of K.

Since $\mathbb{Z}$ is integrally closed (Prop. 2.1.10), we have $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$. That is, algebraic integers in $\mathbb{Q}$ are precisely the usual integers.

If $\overline{\mathbb{Q}}$ denotes the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$, then clearly algebraic integers are all contained in $\overline{\mathbb{Q}}$, so that $\mathcal{O}_K = \mathcal{O}_{K \cap \overline{\mathbb{Q}}}$. Without loss of generality, when studying algebraic integers we may always assume $K \subseteq \overline{\mathbb{Q}}$.

If K is a finite extension of $\mathbb{Q}$, we say that K is an ***algebraic number field*** or simply a ***number field***. ■

Proposition 2.2.2. *Let K be a subfield of $\overline{\mathbb{Q}}$.*

1. *The ring $\mathcal{O}_K$ is integrally closed with fraction field K.*
2. *Let $\alpha \in K$ and let $f(t) \in \mathbb{Q}[t]$ be its (monic) minimal polynomial over $\mathbb{Q}$. Then $\alpha \in \mathcal{O}_K$ if and only if $f \in \mathbb{Z}[t]$.*

Proof. Exercise. □

Example 2.2.3. Let K be a ***quadratic field***, i.e., K is a quadratic extension of $\mathbb{Q}$. We can find a square-free integer $d \in \mathbb{Z} \setminus \{0, 1\}$ such that $K = \mathbb{Q}(\sqrt{d})$. If $K \subseteq \mathbb{R}$ (i.e., $d > 0$), we say that K is ***real***. Otherwise we say K is ***imaginary***.

As an exercise, the reader may check that

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}\left[\sqrt{d}\right] & \text{if } d \equiv 2,\ 3 \pmod 4, \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \mathbb{Z}\left[\frac{-1+\sqrt{d}}{2}\right] & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

For $d = -1$, the ring $\mathcal{O}_{\mathbb{Q}(\mathrm{i})} = \mathbb{Z}[\mathrm{i}]$ is often called the ring of ***Gauss integers***. For $d = -3$, the number $\omega := \exp\left(\frac{2}{3}\pi\mathrm{i}\right) = \frac{-1+\sqrt{-3}}{2}$ is a primitive third root of unity. The ring $\mathbb{Z}[\omega] = \mathcal{O}_{\mathbb{Q}(\omega)} = \mathcal{O}_{\mathbb{Q}(\sqrt{-3})}$ is called the ring of ***Eisenstein integers***.

By Example 1.2.2 (1), if K is an imaginary quadratic field, then the norm map $N_{K/\mathbb{Q}}$ coincides with the map $\alpha \mapsto |\alpha|^2$, where $|\cdot|$ denotes the usual absolute value on $\mathbb{C}$. In particular, $N_{K/\mathbb{Q}}$ always takes nonnegative rational values and $N_{K/\mathbb{Q}}(\mathcal{O}_K) \subseteq \mathbb{N}$. ■

(2.2.4) Let R be an integral domain. By a ***Euclidean function*** on R we mean a function $\varphi : R \to \mathbb{N}$ such that for all a, $b \in R$, $b \neq 0$, there exist q, $r \in R$ satisfying

$$a = bq + r \quad \text{and either } r = 0 \text{ or } \varphi(r) < \varphi(b)\,.$$

If there exists a Euclidean function on R, we say that R is a ***Euclidean domain***.

Any Euclidean domain is a PID and hence also a UFD.

A field is a Euclidean domain. The ring $\mathbb{Z}$ is Euclidean, and for any field F the one-variable polynomial ring $F[X]$ is Euclidean.

The ring of Gauss integers $\mathbb{Z}[\mathrm{i}]$ is Euclidean with a Euclidean function φ given by the norm map $N_{\mathbb{Q}(\mathrm{i})/\mathbb{Q}}$. ■

Example 2.2.5. Let $K = \mathbb{Q}(\sqrt{d})$. We leave it to the reader to check that for

$$d = -11,\ -7,\ -3,\ -2\,,\ 2,\ 3,\ 5 \text{ or } 13\,,$$

the ring $\mathcal{O}_K$ is Euclidean with a Euclidean function given by $\varphi(x) = |N_{K/\mathbb{Q}}(x)|$. ■

Remark 2.2.6. Let us mention the following results, although their proofs are difficult:

1. There are precisely 5 imaginary quadratic fields whose ring of integers is Euclidean. These fields are $\mathbb{Q}(\sqrt{d})$ for $d = -1,\ -2,\ -3,\ -7,\ -11$.

   There are precisely 9 imaginary quadratic fields whose ring of integers is a PID. In addition to the above 5 fields, the other 4 such fields are $\mathbb{Q}(\sqrt{d})$ for $d = -19,\ -43,\ -67,\ -163$.

   Gauss found that for these 9 fields K the ring $\mathcal{O}_K$ is a PID, and he conjectured that there are no other imaginary quadratic fields with this property. This conjecture was solved independently by Alan Baker [Bak66], a Fields medalist of the year 1970, and H.M. Stark [Sta67].

2. There are precisely 16 real quadratic fields K for which the map $\varphi(x) = |N_{K/\mathbb{Q}}(x)|$ is a Euclidean function on $\mathcal{O}_K$. These fields are $\mathbb{Q}(\sqrt{d})$ for

   $$d = 2,\ 3,\ 5,\ 6,\ 7,\ 11,\ 13,\ 17,\ 19,\ 21,\ 29,\ 33,\ 37,\ 41,\ 57,\ 73\,.$$

   However, for other real quadratic fields K it is still unknown whether some other function can be a Euclidean function on $\mathcal{O}_K$.

   Gauss conjectured that there are infinitely many real quadratic fields K such that $\mathcal{O}_K$ is a PID. We do have quite a number of examples of such fields K. But this conjecture of Gauss is still open. ■

Lemma 2.2.7. *Let K be a number field and let $\pi \in \mathcal{O}_K$.*

1. *The group of units in $\mathcal{O}_K$ is $\mathcal{O}_K^* = \{\alpha \in \mathcal{O}_K \mid N_{K/\mathbb{Q}}(\alpha) = \pm 1\}$.*
2. *If $|N_{K/\mathbb{Q}}(\pi)|$ is a prime number, then π is an irreducible element in $\mathcal{O}_K$.*

3. *Suppose K is a quadratic field. If π is a prime element in $\mathcal{O}_K$, then $|N_{K/\mathbb{Q}}(\pi)| = p$ or p^2, where $p \in \mathbb{N}$ is a prime number.*

Proof. Exercise. □

Proposition 2.2.8. *Let $R = \mathbb{Z}[\mathrm{i}]$ be the ring of Gauss integers.*

1. *The group of units of R is $R^* = \{\pm 1, \pm \mathrm{i}\}$.*
2. *An element $\pi \in R$ is a prime element if and only if there exists $u \in R^*$ such that one of the following holds:*
   (a) *$\pi u = 1 + \mathrm{i}$;*
   (b) *$\pi u = a + b\mathrm{i}$ with $a, b \in \mathbb{Z}$ such that $a > |b| > 0$ and $a^2 + b^2 = p$ for some prime number $p \equiv 1 \pmod 4$;*
   (c) *$\pi u = p$ for some prime number $p \equiv 3 \pmod 4$.*

Proof. Exercise. □

Example 2.2.9. Here is an example of how the ring $\mathbb{Z}[\mathrm{i}]$ can be used to solve integer equations.

We want to find all the integer solutions to the equation $x^2 + 1 = y^3$. Suppose $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ is one solution. Then in $\mathbb{Z}[\mathrm{i}]$ we have $(x + \mathrm{i})(x - \mathrm{i}) = y^3$.

We first show that $x + \mathrm{i}$ and $x - \mathrm{i}$ are coprime. Indeed, a prime element in $\mathbb{Z}[\mathrm{i}]$ that divides both $x + \mathrm{i}$ and $x - \mathrm{i}$ must divide $2\mathrm{i}$, so it is up to units equal to $1 + \mathrm{i}$. However, $\frac{x+\mathrm{i}}{1+\mathrm{i}} = \frac{(x+1)+(1-x)\mathrm{i}}{2}$. Here x must be even, for otherwise $x^2 + 1$ is never a cube as it is congruent to 2 mod 4. So $1 + \mathrm{i}$ does not divide $x + \mathrm{i}$ in $\mathbb{Z}[\mathrm{i}]$. This shows that $x + \mathrm{i}$ and $x - \mathrm{i}$ are coprime.

Since $\mathbb{Z}[\mathrm{i}]$ is a UFD and each element in $(\mathbb{Z}[\mathrm{i}])^*$ is a cube, we can now conclude that $x + \mathrm{i} = (a + b\mathrm{i})^3$ for some $a, b \in \mathbb{Z}$. This yields

$$x = a(a^2 - 3b^2) \quad \text{and} \quad 1 = b(3a^2 - b^2)\,.$$

It follows that $b = \pm 1$, and an inspection of both cases shows that the only solution is $(a, b) = (0, -1)$. This implies that the only solution to our original equation is $x = 0$, $y = 1$. In other words, a nonzero square is never followed by a cube in $\mathbb{Z}$. ■

Proposition 2.2.10. *Let $R = \mathbb{Z}[\omega]$, where $\omega = \frac{-1+\sqrt{-3}}{2}$, be the ring of Eisenstein integers.*

1. *The group of units of R is $R^* = \{\pm 1, \pm\omega, \pm\omega^2\}$.*
2. *An element $\pi \in R$ is a prime element if and only if there exists $u \in R^*$ such that one of the following holds:*
   (a) *$\pi u = 1 - \omega$;*
   (b) *$\pi u = a + b\omega$ with $a, b \in \mathbb{Z}$, $a^2 - ab + b^2 = p$ for some prime number $p \equiv 1 \pmod 3$;*

(c) $\pi u = p$ *for some prime number* $p \equiv 2 \pmod 3$.

Proof. Exercise. □

Example 2.2.11. Here is an example of how to use the prime elements in the ring of Eisenstein integers.

Let p be a prime number $\neq 3$. We claim that the equation $p = x^2 + 3y^2$ has integer solutions if and only if $p \equiv 1 \pmod 3$.

The necessity is obvious, so we only prove the sufficiency. Let us assume $p \equiv \pmod 3$. Let π be a prime factor of p in $R = \mathbb{Z}[\omega]$. From Prop. 2.2.10 we find easily that the norm $N(\pi) := N_{\mathbb{Q}(\omega)/\mathbb{Q}}(\pi)$ must be equal to p. Write $\pi = a + b\omega$ with $a, b \in \mathbb{Z}$. If b is even, then $x = a - \frac{b}{2}$, $y = \frac{b}{2}$ are integers such that $\pi = x + y\sqrt{-3}$. If a is even, then

$$\pi.\omega^2 = (b - a) + a\omega = \left(b - \frac{3a}{2}\right) + \frac{a}{2}\sqrt{-3} = x + y\sqrt{-3}$$

with $x = b - \frac{3a}{2} \in \mathbb{Z}$, $y = \frac{3a}{2} \in \mathbb{Z}$. Finally, if a and b are both odd, then $c := a - b$ is even and

$$\pi.\omega = -b + c\omega = \left(-b - \frac{c}{2}\right) + \frac{c}{2}\sqrt{-3} = x + y\sqrt{-3}$$

with $x = -b - \frac{c}{2} \in \mathbb{Z}$, $y = \frac{c}{2} \in \mathbb{Z}$. Since $p = N(\pi) = N(\pi\omega^2) = N(\pi\omega)$, in each of the above three cases, we get $p = x^2 + 3y^2$ as desired. ■

Proposition 2.2.12. *Let* $R = \mathbb{Z}[\mathrm{i}]$ *or* $R = \mathbb{Z}[\omega]$. *Let* $N = N_{K/\mathbb{Q}} : K \to \mathbb{Q}$ *be the norm map of the fraction field* K *of* R.

Then for every prime element π *in* R, $R/\pi R$ *is a finite field with* $|R/\pi R| = N(\pi)$.

Proof. Exercise. □

As an immediate corollary, we have the following analog of Fermat's little theorem:

Corollary 2.2.13. *With notation as in Prop. 2.2.12, let* $\pi \in R$ *be a prime element and* $\alpha \in R$ *be an element such that* $\pi \nmid \alpha$.

Then $\alpha^{N(\pi)-1} \equiv 1 \pmod{\pi R}$.

2.2.2 The cubic reciprocity law

In this subsection, let $\omega = \frac{-1+\sqrt{-3}}{2} \in \mathbb{C}$ and let $R = \mathbb{Z}[\omega]$ be the ring of Eisenstein integers. Let N denote the norm map $N_{\mathbb{Q}(\omega)/\mathbb{Q}} : \mathbb{Q}(\omega) \to \mathbb{Q}$.

Lemma 2.2.14. *Let* $\pi \in R$ *be a prime element with* $N(\pi) \neq 3$.

1. *We have* $N(\pi) \equiv 1 \pmod 3$ *in* $\mathbb{Z}$.
2. *The elements* $1, \omega, \omega^2$ *are pairwise incongruent modulo* πR.
3. *For any* $\alpha \in R$ *with* $\pi \nmid \alpha$, *there is a unique* $m \in \{0, 1, 2\}$ *such that*

$$\alpha^{\frac{N(\pi)-1}{3}} \equiv \omega^m \pmod{\pi R}.$$

Proof. (1) By Prop. 2.2.10 (2), either $N(\pi) = p$ for a prime number $p \equiv 1 \pmod 3$ or $N(\pi) = p^2$ for a prime $p \equiv 2 \pmod 3$. In any case, $N(\pi) \equiv 1 \pmod 3$.

(2) We have $N(1-\omega) = N(\omega - \omega^2) = N(1-\omega^2) = 3$. By (1), $N(\pi) \nmid 3$. Hence none of $1-\omega$, $\omega - \omega^2$ and $1 - \omega$ is divisible by π.

(3) Put $\beta = \alpha^{\frac{N(\pi)-1}{3}}$. By Cor. 2.2.13, we have

$$(\beta - 1)(\beta - \omega)(\beta - \omega^2) = \beta^3 - 1 = \alpha^{N(\pi)-1} - 1 \equiv 0 \pmod{\pi R}.$$

Since $R/\pi R$ is a domain (Prop. 2.2.12), we have $\beta \equiv 1$, ω or $\omega^2 \bmod \pi R$. This proves the existence. The uniqueness statement follows from (2). □

(2.2.15) Let $\pi \in R$ be a prime element with $N(\pi) \neq 3$. Let $\alpha \in R$. Thanks to Lemma 2.2.14 we can define the ***cubic residue symbol*** $\left(\frac{\alpha}{\pi}\right)_3$ of α modulo π as follows:

If $\pi \mid \alpha$, put $\left(\frac{\alpha}{\pi}\right)_3 = 0$; otherwise let $\left(\frac{\alpha}{\pi}\right)_3$ be the unique element in $\{1, \omega, \omega^2\}$ such that

$$\alpha^{\frac{N(\pi)-1}{3}} \equiv \left(\frac{\alpha}{\pi}\right)_3 \pmod{\pi R}.$$

From the definition it is clear that the function $\left(\frac{\cdot}{\pi}\right)_3 : R \longrightarrow \mathbb{C}$ is multiplicative (i.e., $\left(\frac{\alpha\beta}{\pi}\right)_3 = \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_3$ for all $\alpha, \beta \in R$), and that the value of $\left(\frac{\alpha}{\pi}\right)_3$ depends only on the residue class of $\alpha \pmod{\pi R}$. So we may also regard $\left(\frac{\cdot}{\pi}\right)_3$ as a character on the finite field $F := R/\pi R$. Therefore, we sometimes write $\chi_\pi = \left(\frac{\cdot}{\pi}\right)_3$ and we call this function (defined on R or F) the ***cubic residue character*** modulo π. ■

Lemma 2.2.16. *Let $\pi \in R$ be a prime element with $N(\pi) \neq 3$. Let $\alpha \in R$ be such that $\pi \nmid \alpha$.*

Then $\left(\frac{\alpha}{\pi}\right)_3 = 1$ if and only if there exists $x \in R$ such that $x^3 \equiv \alpha \pmod{\pi R}$.

In particular, $\left(\frac{-1}{\pi}\right)_3 = 1$.

Proof. Put $F = R/\pi R$. The multiplicative group F^* is cyclic of order divisible by 3 (by Prop. 2.2.12 and Lemma 2.2.14 (1)). Choose $\gamma \in R$ such that its canonical image in F is a generator of F^*. Then the result is easily proved by expressing the residue classes of α and ω as powers of γ. □

Proposition 2.2.17. *Let $\pi \in R$ be a prime element with $N(\pi) \neq 3$ and let $\alpha \in R$.*

1. *We have $\overline{\chi_\pi(\alpha)} = \chi_\pi(\alpha)^2 = \chi_\pi(\alpha^2)$ and $\overline{\chi_\pi(\alpha)} = \chi_{\overline{\pi}}(\overline{\alpha})$ in $\mathbb{C}$.*
2. *Let $q \in \mathbb{N}$ be a prime number such that $q \equiv 2 \pmod 3$. (We may consider q as a prime element in R, by Prop. 2.2.10.)*

   Then $\chi_q(\overline{\alpha}) = \chi_q(\alpha)^2$ and for every $n \in \mathbb{Z}$ which is coprime to q, $\chi_q(n) = 1$.

Proof. (1) This is immediate from the fact that the nonzero values of χ_3 are cubic roots of unity in $\mathbb{C}$.

(2) This follows easily from (1). □

(2.2.18) A prime element in R is called ***primary*** if it is congruent to 2 modulo $3R$.

Let $\pi \in R$ be a prime element and write $\pi = a+b\omega$ with $a, b \in \mathbb{Z}$. Then π is primary if and only if $a \equiv 2 \pmod 3$ and $b \equiv 0 \pmod 3$.

If $N(\pi) = 3$, then

$$\pi \in (1-\omega)R^* = \{\pm(1-\omega)\,,\ \pm\omega(1-\omega) = \pm(1+2\omega)\,,\ \pm\omega^2(1-\omega) = \mp(2+\omega)\}\,.$$

In this case, π is not primary. Hence, a primary prime element π must satisfy $N(\pi) \equiv 1 \pmod 3$, or equivalently, either $N(\pi)$ is a prime number $p \equiv 1 \pmod 3$, or $N(\pi) = q^2$ for some prime number $q \equiv 2 \pmod 3$. ■

Recall that two nonzero elements a, b in a domain are called ***associate*** to each other, if ab^{-1} is a unit in the domain.

Proposition 2.2.19. *Let $\pi \in R$ be a prime element such that $N(\pi) \equiv 1 \pmod 3$.*

1. *If $N(\pi) = q^2$ for prime number $q \equiv 2 \pmod 3$, then π is primary if and only if $\pi = q$.*

   A primary prime element with this property is called **rational**.

2. *If $N(\pi)$ is a prime number, then among the six associates of π (i.e. elements in $\pi R^* = \{\pm\pi,\ \pm\pi\omega\,,\ \pm\pi\omega^2\}$) exactly one is primary.*

   A primary prime element with this property is called **complex**.

Proof. This is a direct verification through elementary calculations. The details are left to the reader as an exercise. □

Lemma 2.2.20. *Let $\pi \in R$ be a complex primary prime element with $p = N(\pi)$ and let $\chi = \chi_\pi$, which we regard as a character on the finite field $\mathbb{F}_p = R/\pi R$ (Prop. 2.2.12).*

Then we have $J(\chi,\, \chi) = \pi$ and $g(\chi)^3 = p\pi$.

Proof. Since $\chi(-1) = 1$ (Lemma 2.2.16), by Cor. 1.4.4 we have $g(\chi)^3 = pJ(\chi,\, \chi)$. So we only need to prove the first equality.

First, we claim that $J(\chi,\, \chi)$ is a primary prime in R of norm p. Since χ takes values in $\{1,\, \omega,\, \omega^2\} \subseteq R$, from the definition we see that $J(\chi,\, \chi) \in R$. By Thm. 1.4.6 (1), the norm of $J(\chi,\, \chi)$ is $|J(\chi,\, \chi)|^2 = p$. So $J(\chi,\, \chi)$ is a prime element of norm p in R. We need to show that it is primary. That is, writing $J(\chi,\, \chi) = a + b\omega$ with $a, b \in \mathbb{Z}$, we have $a \equiv 2 \pmod 3$ and $b \equiv 0 \pmod 3$.

In fact, since $\chi(0) = 0$ and $\chi(t)^3 = 1$ for all $t \in \mathbb{F}_p^*$,

$$g(\chi)^3 = \left(\sum_{t\in\mathbb{F}_p} \chi(t)\zeta^t\right)^3 \equiv \sum_{t\in\mathbb{F}_p} \chi(t)^3\zeta^{3t} = \sum_{t\in\mathbb{F}_p^*} \zeta^{3t} = -1 \pmod{3R}\,.$$

Thus, we obtain $pa + pb\omega = pJ(\chi,\, \chi) \equiv -1 \pmod{3R}$. But $p = N(\pi) \equiv 1 \pmod 3$. So we get

$$a + b\omega \equiv pJ(\chi,\, \chi) \equiv -1 \pmod{3R}\,.$$

Since R is a free $\mathbb{Z}$-module generated by $1, \omega$, this implies $a \equiv -1 \pmod 3$ and $b \equiv 0 \pmod 3$ in $\mathbb{Z}$. This prove the claim.

Now write $\pi' = J(\chi, \chi)$. Since $\pi'\overline{\pi}' = p = \pi\overline{\pi}$, we have $\pi \,|\, \pi'$ or $\pi \,|\, \overline{\pi}'$. Since all the prime elements involved here are primary, by Prop. 2.2.19 (2), we must have $\pi = \pi'$ or $\pi = \overline{\pi}'$. We wish to eliminate the latter possibility.

From the definitions,

$$J(\chi, \chi) = \sum_{t \in \mathbb{F}_p} \chi(t)\chi(1-t) \equiv \sum_{t \in \mathbb{F}_p} t^{\frac{p-1}{3}} (1-t)^{\frac{p-1}{3}} \pmod{\pi R}.$$

The polynomial $f(X) = X^{\frac{p-1}{3}}(1-X)^{\frac{p-1}{3}}$ has degree $\frac{2}{3}(p-1) < p-1$. So it is easily seen that $\sum_{t \in \mathbb{F}_p} f(t) = 0$ in $\mathbb{F}_p$. This shows that $J(\chi, \chi) \equiv 0 \pmod{\pi R}$, i.e., $\pi \,|\, \pi'$. Therefore, $\pi = \pi'$. □

Theorem 2.2.21 (Cubic reciprocity law)**.** *Let π_1, π_2 be distinct primary prime elements in R. Then $\left(\frac{\pi_1}{\pi_2}\right)_3 = \left(\frac{\pi_2}{\pi_1}\right)_3$.*

Proof. There are three cases to consider. Namely, both π_1 and π_2 are rational, π_1 is rational and π_2 is complex, and both π_1 and π_2 are complex.

Case 1. Both π_1 and π_2 are rational.

Then $\pi_1 = q_1$ and $\pi_2 = q_2$ for two distinct prime numbers q_1, q_2 such that $q_1 \equiv q_2 \equiv 2 \pmod 3$ (by Prop. 2.2.19). The result then follows immediately from Prop. 2.2.17 (2).

Case 2. $\pi_1 = q$ is rational and π_2 is complex.

Let $p = N(\pi_2)$, which is a prime number $\equiv 1 \pmod 3$. Let $\chi = \chi_{\pi_2} = \left(\frac{\cdot}{\pi_2}\right)_3$. Consider the Jacobi sum $J(\chi, \cdots, \chi)$ associated with q characters all equal to χ. Since $3 \,|\, q+1$ and $\chi(-1) = 1$ (Lemma 2.2.16), by Cor. 1.4.4 we have

$$g(\chi)^{q+1} = pJ(\chi, \cdots, \chi). \tag{2.2.21.1}$$

By Lemma 2.2.20, we also have

$$g(\chi)^{q+1} = (p\pi_2)^{\frac{q+1}{3}}. \tag{2.2.21.2}$$

On the other hand, $J(\chi, \cdots, \chi)$ is equal to the following sum

$$\sum_{x_1 + \cdots + x_q = 1\,,\, x_i \in \mathbb{F}_p} \chi(x_1) \cdots \chi(x_q) \tag{2.2.21.3}$$

where the number of terms is p^{q-1}. Consider the term with $x_1 = \cdots = x_q = 1/q \in \mathbb{F}_p$. That term is $\chi(q^{-1})^q = \chi(q)^{-q} = \chi(q)$, since $-q \equiv 1 \pmod 3$ and $\chi^3 = \varepsilon$. For all the other terms in (2.2.21.3), not all the x_i are equal, and there are q different q-tuples obtained from $(x_1, \cdots, x_q)$ by cyclic permutation. The corresponding terms of the sum (2.2.21.3) all have the same value. It follows that

$$J(\chi, \cdots, \chi) = \sum_{x_1 + \cdots + x_q = 1\,,\, x_i \in \mathbb{F}_p} \chi(x_1) \cdots \chi(x_q) \equiv \chi(q) \pmod{qR}. \tag{2.2.21.4}$$

Combining (2.2.21.1), (2.2.21.2) and (2.2.21.4) yields

$$p^{\frac{q-2}{3}} \cdot \pi_2^{\frac{q+1}{3}} \equiv \chi(q) \pmod{qR}.$$

Raising both sides to the $(q-1)$-st power (and remembering that $q-1 \equiv 1 \pmod 3$ and that $p^{q-1} \equiv 1 \pmod q$) we obtain

$$\chi_q(\pi_2) \equiv \pi_2^{\frac{N(q)-1}{3}} = \pi_2^{\frac{q^2-1}{3}} \equiv \chi(q)^{q-1} = \chi(q) \pmod{qR}.$$

By Lemma 2.2.14 (2), it follows that $\chi_q(\pi_2) = \chi(q)$, i.e., $\chi_{\pi_1}(\pi_2) = \chi_{\chi_2}(\pi_1)$.

Case 3. Both π_1 and π_2 are complex.

Let $p_i = N(\pi_i)$ and let $\chi' = \chi_{\overline{\pi}_1}$. Since $p_2 \equiv 1 \pmod 3$, using Thm. 1.4.3 we find $g(\chi')^{p_2} = J(\chi', \cdots, \chi')g(\chi')$, where in the Jacobi sum χ' appears p_2 times. Thus,

$$\left(g(\chi')^3\right)^{\frac{p_2-1}{3}} = J(\chi', \cdots, \chi'). \tag{2.2.21.5}$$

By isolating the diagonal term of the Jacobi sum (as we have done in Case 2) we see that

$$J(\chi', \cdots, \chi') \equiv \chi'(p_2)^2 \mod p_2 R.$$

Using this and the fact that $g(\chi')^3 = p_1\overline{\pi}_1$ (Lemma 2.2.20), we obtain from (2.2.21.5) the congruence

$$\chi_{\pi_2}(p_1\overline{\pi}_1) \equiv (p_1\overline{\pi}_1)^{\frac{p_2-1}{3}} \equiv \chi_{\overline{\pi}_1}(p_2)^2 \pmod{\pi_2 R}.$$

Therefore, by Lemma 2.2.14 (2),

$$\chi_{\pi_2}(p_1\overline{\pi}_1) = \chi_{\overline{\pi}_1}(p_2)^2. \tag{2.2.21.6}$$

Similarly one proves that

$$\chi_{\pi_1}(p_2\pi_2) = \chi_{\pi_2}(p_1)^2. \tag{2.2.21.7}$$

Noticing that $\chi_{\overline{\pi}_1}(p_2)^2 = \chi_{\pi_1}(p_2)$ by Prop. 2.2.17 (1), we can now use (2.2.21.6) and (2.2.21.7) to calculate

$$\begin{aligned}\chi_{\pi_1}(\pi_2)\chi_{\pi_2}(p_1\overline{\pi}_1) &= \chi_{\pi_1}(\pi_2)\chi_{\overline{\pi}_1}(p_2)^2 = \chi_{\pi_1}(\pi_2)\chi_{\pi_1}(p_2) \\ &= \chi_{\pi_1}(p_2\pi_2) = \chi_{\pi_2}(p_1^2) = \chi_{\pi_2}(p_1\overline{\pi}_1\pi_1).\end{aligned}$$

It now follows immediately that $\chi_{\pi_1}(\pi_2) = \chi_{\pi_2}(\pi_1)$. This completes the proof of the theorem. □

2.2.3 The quartic reciprocity law

In this subsection, let $R = \mathbb{Z}[\mathrm{i}]$ be the ring of Gauss integers. Let N denote the norm map $N_{\mathbb{Q}(\mathrm{i})/\mathbb{Q}} : \mathbb{Q}(\mathrm{i}) \to \mathbb{Q}$.

As an analog of Lemma 2.2.14 we have:

Lemma 2.2.22. *Let $\pi \in R$ be a prime element with $N(\pi) \neq 2$.*

1. *We have $N(\pi) \equiv 1 \pmod 4$ in $\mathbb{Z}$.*
2. *The elements $\pm 1, \pm \mathrm{i}$ are pairwise incongruent modulo πR.*
3. *For any $\alpha \in R$ with $\pi \nmid \alpha$, there is a unique $m \in \{0, 1, 2, 3\}$ such that*

$$\alpha^{\frac{N(\pi)-1}{4}} \equiv \mathrm{i}^m \pmod{\pi R}.$$

Proof. Exercise. □

Definition 2.2.23. Let $\pi \in R$ be a prime element with $N(\pi) \neq 2$.

The ***quartic (or biquadratic) residue symbol*** modulo π is the function $\left(\frac{\cdot}{\pi}\right)_4 : R \to \mathbb{C}$ defined as follows: If $\pi \mid \alpha$, then $\left(\frac{\cdot}{\pi}\right)_4 = 0$; otherwise $\left(\frac{\cdot}{\pi}\right)_4$ is the unique element in $\{\pm 1, \pm \mathrm{i}\}$ such that

$$\alpha^{\frac{N(\pi)-1}{4}} \equiv \left(\frac{\alpha}{\pi}\right)_4 \pmod{\pi R}.$$

We say that the prime element π is ***primary*** if $\pi \equiv 1 \pmod{(1+\mathrm{i})^3 R}$. (Note that $(1+\mathrm{i})^3 R = (2+2\mathrm{i})R$.) ■

Theorem 2.2.24 (Quartic reciprocity law)**.** *Let π_1, π_2 be distinct primary prime elements in $R = \mathbb{Z}[\mathrm{i}]$. Then*

$$\left(\frac{\pi_1}{\pi_2}\right)_4 = (-1)^{\frac{N(\pi_1)-1}{4} \cdot \frac{N(\pi_2)-1}{4}} \left(\frac{\pi_2}{\pi_1}\right)_4.$$

Proof. See e.g. [IR90, § 9.9]. □

The first complete proofs for the cubic and quartic reciprocity laws were published in 1844 by Eisenstein, who also found generalizations of these laws.

2.3 Dedekind domains and ideal theory

2.3.1 Fractional ideals

In this subsection, let R be an integral domain and $K = \mathrm{Frac}(R)$ be its fraction field.

(2.3.1) For R-submodules I_1, I_2 of K, in addition to the intersection $I_1 \cap I_2$ we can define

$$\begin{aligned} I_1 + I_2 &:= \{a + b \mid a \in I_1,\, b \in I_2\}, \\ I_1 \cdot I_2 &:= \text{ the } R\text{-submodule generated by the set } \{ab \mid a \in I_1,\, b \in I_2\}, \\ (I_1 : I_2) &:= \{x \in K \mid xI_2 \subseteq I_1\}. \end{aligned}$$

We also put

$$I^{-1} := (R : I) = \{x \in K \mid xI \subseteq R\}$$

for every R-submodule I of K. ■

Lemma 2.3.2. *The operations on R-submodules of K defined in (2.3.1) have the following properties:*

1. *Addition, intersection and multiplication are commutative and associative.*
2. *$I(I_1 + I_2) = II_1 + II_2$; $(I : I) \supseteq R \supseteq II^{-1}$.*
3. *If $I \subseteq R$, then $I^{-1} \supseteq R$.*

Proof. Exercise. □

(2.3.3) A ***fractional ideal*** of R is a nonzero R-submodule $I \subseteq K$ such that $I^{-1} \neq 0$. In other words, a fractional ideal is a nonzero R-submodule of K for which there exists a nonzero element $a \in K$ such that $aI \subseteq R$. Such an element a can always be chosen to lie in R. In fact, if $a = b/c$ with b, $c \in R$, then $bI \subseteq R$.

Clearly, for any nonzero element $x \in K$, the submodule xR is a fractional ideal. Such a fractional ideal is called a ***principal fractional ideal***.

If I is a nonzero ideal (in the usual sense) in R, then clearly I is a fractional ideal. In the sequel, sometimes to emphasize an ideal I that lies in R, we call such an ideal an ***integral ideal*** of R. For two fractional ideals I_1, I_2, we say I_1 ***divides*** I_2, written $I_1 \,|\, I_2$, if there is an integral ideal I such that $I_1 I = I_2$. ■

Lemma 2.3.4. *If I_1, I_2 are fractional ideals, then so are $I_1 + I_2$, $I_1 \cap I_2$, $I_1 I_2$ and $(I_1 : I_2)$.*

In particular, if I is a fractional ideal, then so is I^{-1}.

Proof. For $i = 1, 2$, let $a_i \in R$ be a nonzero element such that $a_i I_i \subseteq R$ and let b_i be a nonzero element in I_i. We may assume that $b_i \in R$, for if a fraction b'/b'' (with b', $b'' \in R$, $b'' \neq 0$) lies in I_i, then $b' \in I_i$.

Then b_1 is a nonzero element in $I_1 + I_2$, $b_1 b_2$ is a nonzero element in $I_1 I_2 \subseteq I_1 \cap I_2$, and $a_2 b_1$ is a nonzero element in $(I_1 : I_2)$. Moreover, $a_1 a_2 \neq 0$, $a_1 b_2 \neq 0$ and clearly

$$a_1 a_2 (I_1 + I_2) \subseteq R\,,\ a_1 a_2 (I_1 \cap I_2) \subseteq R\,,\ a_1 a_2 I_1 I_2 \subseteq R \ \text{ and } \ a_1 b_2 (I_1 : I_2) \subseteq R\,.$$

The lemma is thus proved. □

Lemma 2.3.5. *Suppose R is Noetherian. A nonzero R-submodule I of K is a fractional ideal if and only if it is finitely generated.*

Proof. Necessity. Let $a \in R$ be a nonzero element such that $aI \subseteq R$. Then the ideal aI of R is finitely generated as R is Noetherian. Clearly $I \cong aI$ as R-modules. So I is finitely generated too.

Sufficiency. Multiplying I up by the denominator product of the generators sends I into R. □

2.3.2 Discrete valuation rings

Definition 2.3.6. A ring R is called a ***discrete valuation ring*** (DVR) if it is a principal ideal domain (PID) that has a unique nonzero prime ideal $\mathfrak{m}$. Here we require R to have at least one nonzero prime ideal. So a field is *not* a DVR in our terminology. Any generator of $\mathfrak{m}$ is called a ***uniformizer*** (or ***uniformizing element***, ***parameter***, ***regular parameter***, etc.) of R. ■

Proposition 2.3.7. *For any ring R, the following statements are equivalent:*

(i) *R is a DVR.*

(ii) *R is a PID which has one and only one prime element up to associates.*

(iii) *R is a local PID which is not a field.*

(iv) *R is a Noetherian local domain, and its maximal ideal is a nonzero principal ideal.*

Proof. (i)⇔(ii). Use the fact that in a PID the nonzero prime ideals are precisely ideals that can be generated by one prime element.

(i)⇔(iii). In a PID which is not a field, a nonzero ideal is prime if and only if it is maximal.

(iii)⇒(iv). Every ideal in a PID is generated by one element, so a PID is Noetherian.

(iv)⇒(iii). Suppose that R has the properties stated in (iv). We need to show that R is a PID. Let π be a generator of the maximal ideal $\mathfrak{m}$ of R. It suffices to prove the following:

Claim. Every nonzero element $a \in R$ can be written uniquely in the form $a = u\pi^n$, where $u \in R^*$ and $n \in \mathbb{N}$.

Indeed, since R is Noetherian, any nonzero ideal I in R can be generated by finitely many nonzero elements $a_1, \cdots, a_r$. Assuming that the above claim is true, we can write each $a_i = u_i\pi^{n_i}$ with $u_i \in R^*$, $n_i \in \mathbb{N}$. Then

$$I = a_1R + \cdots + a_rR = \pi^{n_1}R + \cdots + \pi^{n_r}R = \pi^nR \text{ for } n := \min\{n_1, \cdots, n_r\}.$$

It remains to prove our claim. Let $a \in R$ be a nonzero element. If $a = u\pi^n = w\pi^m$ with $u, w \in R^*$ and $n, m \in \mathbb{N}$, then we must have $m = n$, for if $m > n$, π^{m-n} lies in $\mathfrak{m} = \pi R$ and hence cannot be a unit. This proves the uniqueness of the asserted expression. To prove the existence, note that if $a \in R^*$, we can simply take $n = 0$ and $u = a$. If $a \notin R^*$, then a belongs to the unique maximal ideal $\mathfrak{m} = \pi R$. Hence $a = \pi x_1$ for some nonzero element $x_1 \in R$. If $x_1 \in R^*$, then taking $n = 1$ and $u = x_1$ yields the desired factorization. Otherwise we can continue to obtain a factorization $x_1 = \pi x_2$, whence $a = \pi^2 x_2$. Repeat the procedure whenever possible, we can find inductively expressions

$$a = \pi x_1 = \pi^2 x_2 = \pi^3 x_3 = \cdots$$

with $x_i = \pi x_{i+1}$ for each $i \geq 1$. There must be some $n \in \mathbb{N}$ such that $x_n \in R^*$, so that we get the desired expression, because otherwise we would have an infinite strictly ascending chain of ideals

$$x_1R \subset x_2R \subset x_3R \subset \cdots$$

But this is absurd since R is Noetherian. □

Definition 2.3.8. Let K be a field. By a ***normalized discrete valuation*** of K we mean a map $v : K \to \mathbb{Z} \cup \{+\infty\}$ with the following properties:

1. v defines a surjective group homomorphism from K^* to $\mathbb{Z}$;
2. $v(0) = +\infty$;
3. $v(x + y) \geq \min\{v(x), v(y)\}$ for all $x, y \in K$.

By the surjectivity of $v : K^* \to \mathbb{Z}$, we can find an element $\pi \in K^*$ such that $v(\pi) = 1$. Such an element is called a ***uniformizer*** for v. ■

(2.3.9) Let R be a discrete valuation ring with fraction field K. In the proof of Prop. 2.3.7, we have seen that if $\pi \in R$ is a fixed uniformizer, every nonzero element in R can be written uniquely as a product of a power of π with a unit in R. From this it follows easily that for nonzero element x in the fraction field K, there is a unique factorization $x = \pi^n u$, with $u \in R^*$ and $n \in \mathbb{Z}$ this time. The integer n is independent of the choice of the uniformizer π and is called the ***valuation*** or ***order*** of x. We denote it by $v(x)$. With the addition convention that $v(0) = +\infty$ we construct from R a normalized discrete valuation $v : K \longrightarrow \mathbb{Z} \cup \{+\infty\}$, and we have $R = \{x \in K \mid v(x) \geq 0\}$. We say that this v is ***associated to*** the given discrete valuation ring R.

Conversely, if we start with a normalized discrete valuation v of K, then $R_v := \{x \in K \mid v(x) \geq 0\}$ is a subring of K, called the ***valuation ring*** of v. The set $\mathfrak{p}_v := \{x \in K \mid v(x) > 0\}$ is a maximal ideal of R_v, called the ***valuation ideal*** of v. It is easy to see that $R_v \setminus \mathfrak{p}_v$ is the same as the set of units of R_v. In particular, R_v is a local ring with maximal ideal $\mathfrak{p}_v$.

Let $\pi \in R_v$ be a uniformizer for v. For any $x \in K^*$, one can choose $N \in \mathbb{N}$ large enough such that $y = \pi^N x \in R_v$. Therefore, K is the fraction field of R_v. For every nonzero ideal $I \subseteq R$,

$$v(I) := \min\{v(x) \mid x \in I\}$$

is a well defined natural number, by the well ordering property of $\mathbb{N}$. One checks easily that $I = \pi^{v(I)} R$. This shows that R_v is a local PID. By Prop. 2.3.7, R_v is a DVR. ■

We have thus proved:

Proposition 2.3.10. *For any field K, via the rule $v \mapsto R_v$ the normalized discrete valuations of K correspond bijectively to the discrete valuation rings with fraction field K.*

Lemma 2.3.11. *Let R be a discrete valuation ring with fraction field K, $\mathfrak{m}$ its maximal ideal and v the associated normalized discrete valuation of K.*

Then every fractional ideal I of R can be written uniquely in the form $I = \mathfrak{m}^r$, $r \in \mathbb{Z}$; in fact $r = v(I) := \min\{v(x) \mid x \in I\}$.

Proof. Exercise. □

Proposition 2.3.12. *An integral domain R is a discrete valuation ring if and only if it is Noetherian, integrally closed and possesses one and only one nonzero prime ideal.*

Proof. By Props. 2.3.7 and 2.1.10, a DVR is Noetherian and integrally closed.

Conversely, suppose R is a Noetherian, integrally closed domain which has a unique nonzero prime ideal. Then R is a local ring and its maximal ideal $\mathfrak{m}$ is its unique nonzero prime ideal. By Prop. 2.3.7, it is now sufficient to show that $\mathfrak{m}$ is a principal ideal.

By Lemma 2.3.4, $\mathfrak{m}$ and $\mathfrak{m}^{-1}$ are fractional ideals of R. Note that $\mathfrak{m} = \mathfrak{m}R \subseteq \mathfrak{m}\mathfrak{m}^{-1} \subseteq R$. As $\mathfrak{m}$ is a maximal ideal of R, either $\mathfrak{m}\mathfrak{m}^{-1} = \mathfrak{m}$ or $\mathfrak{m}\mathfrak{m}^{-1} = R$.

To prove that $\mathfrak{m}$ is principal, we now proceed in three steps.

Step 1. We show $\mathfrak{m}^{-1} \neq R$.

Choose a nonzero element $a \in \mathfrak{m}$. Then a^{-1} lies in $(aR)^{-1}$ but not in R. Consider the set $\mathscr{S}$ consisting of nonzero ideals I of R with $I^{-1} \neq R$. We have $aR \in \mathscr{S}$, so $\mathscr{S}$ is non-empty. We claim that $\mathscr{S}$ has a maximal element.

Let $\mathscr{T}$ be any totally ordered subset of $\mathscr{S}$. The nonzero ideal

$$J := \sum_{I_\alpha \in \mathscr{T}} I_\alpha$$

lies in $\mathscr{T} \subseteq \mathscr{S}$. In fact, since R is Noetherian, J is finitely generated. As $\mathscr{T}$ is totally ordered, these generators will lie in one common I_{α_0} so that $J = I_{\alpha_0} \in \mathscr{T}$. By Zorn's lemma, $\mathscr{S}$ has a maximal element, say I.

It suffices to show that I is prime and hence equal to $\mathfrak{m}$. (So then we have $\mathfrak{m}^{-1} = I^{-1} \neq R$.)

Suppose $x\,, y \in R$, $x \notin I$ and $xy \in I$. Choose $z \in I^{-1} \setminus R$. Then $zy(xR + I) \subseteq R$, hence zy lies in $(xR + I)^{-1}$ which must be equal to R by the maximality of I. Thus $z(yR + I) \subseteq R$. Therefore, $z \in (yR + I)^{-1}$, so that $(yR + I)^{-1} \neq R$. By the maximality of I, we get $yR + I = I$ and $y \in I$. This proves that I is a prime ideal, as needed.

Step 2. We show $\mathfrak{m}\mathfrak{m}^{-1} = R$.

For any $x \in R(\mathfrak{m}) := \{x \in K \,|\, x\mathfrak{m} \subseteq \mathfrak{m}\}$, $R[x]$ is a submodule of $R(\mathfrak{m})$. By Lemma 2.3.4, $R(\mathfrak{m})$ is a fractional ideal. It follows that $R\mathfrak{m}$ is a finitely generated R-module, hence so is $R[x]$. This shows that x is integral over R, and since R is integrally closed, it follows that $x \in R$. Thus we get $R(\mathfrak{m}) \subseteq R$.

If $\mathfrak{m}\mathfrak{m}^{-1} = \mathfrak{m}$, then $\mathfrak{m}^{-1} \subseteq R(\mathfrak{m}) \subseteq R$, which yields $\mathfrak{m}^{-1} = R$. This contradicts the result in Step 1. Therefore $\mathfrak{m}\mathfrak{m}^{-1} = R$.

Step 3. End of the proof.

Since $\mathfrak{m} = \mathfrak{m}R \subset \mathfrak{m}\mathfrak{m}^{-1} = R$, there exist $x \in \mathfrak{m}$ and $y \in \mathfrak{m}^{-1}$ such that $xy \notin \mathfrak{m}$. Therefore, $xy \in R^*$. If $z \in \mathfrak{m}$, one has $zR = xyzR$. We have $yz \in R$ since $y \in \mathfrak{m}^{-1}$. Hence $z \in zR = (xy)zR = x(yz)R \subseteq xR$. It then follows that $\mathfrak{m} = xR$. This shows that $\mathfrak{m}$ is principal, as desired. □

Example 2.3.13. Here are two basic examples of normalized discrete valuations (or of discrete valuation rings).

(1) Let p be a prime number. There is a unique normalized discrete valuation v_p on $\mathbb{Q}$ such that

$$v_p(f) = n\,, \quad \text{if } f \in \mathbb{Z} \text{ and } p^n \text{ is largest power of } p \text{ dividing } f\,.$$

This valuation is usually called the ***p-adic valuation***. Its valuation ring is the localization

$$\mathbb{Z}_{(p)} = \{a/b \,|\, a,\, b \in \mathbb{Z}\,,\, p \nmid b\}$$

of $\mathbb{Z}$ at the prime ideal $p\mathbb{Z}$.

(2) Let $K = k(t)$ be a one-variable rational function field over a field k. For any irreducible polynomial $p = p(t) \in k[t]$, similar to the previous example, there is a unique normalized discrete v_p on $k(t)$ such that

$$v_p(f) = n\,, \quad \text{if } f \in k[t] \text{ and } p(t)^n \text{ is largest power of } p(t) \text{ dividing } f\,.$$

We call v_p the ***p-adic valuation*** on $k(t)$.

Also, there is a unique normalized discrete valuation v_∞ on $k(t)$ such that

$$\forall\, 0 \neq f \in k[t]\,, \quad v_\infty(f) = -\deg(f)\,.$$

This is called the ***degree valuation*** of $k(t)$. ■

2.3.3 Dedekind domains and their fractional ideals

Definition 2.3.14. An integral domain is called a ***Dedekind domain*** if it is Noetherian, integrally closed and its maximal ideals are exactly the nonzero prime ideals. (In particular, a Dedekind domain has at least one nonzero prime ideal. So a field is *not* considered as a Dedekind domain.) ■

Example 2.3.15. If R is a PID which is not a field, then R is a Dedekind domain. (That R is integrally closed follows from Prop. 2.1.10.)

In particular, $\mathbb{Z}$ is a Dedekind domain, and for any field k, the one-variable polynomial ring $k[t]$ is a Dedekind domain. ■

Definition 2.3.16. Let R be an integral domain. A fractional ideal I of R is called ***invertible*** if $II^{-1} = R$. This is equivalent to saying that there exists a fractional ideal J such that $IJ = R$. Indeed, $IJ = R$ implies $J \subseteq I^{-1}$ and $I^{-1} = I^{-1}R = I^{-1}IJ \subseteq RJ = J$.

It is easy to see that any principal fractional ideal is invertible. ■

Proposition 2.3.17. *Let R be an integral domain which is not a field. Then the following are equivalent:*

(i) *R is a Dedekind domain.*

(ii) *R is Noetherian, and for every nonzero prime ideal $\mathfrak{p}$, $R_\mathfrak{p}$ is a discrete valuation ring.*

(iii) *Every fractional ideal of R is invertible.*

Proof. (i)⇒(ii). Let $\mathfrak{p}$ be a nonzero prime ideal of R. We shall use Prop. 2.3.12 to show that $R_\mathfrak{p}$ is a DVR. A localization of a Noetherian ring is also Noetherian. Moreover, $R_\mathfrak{p}$ is integrally closed as R is, according to Lemma 2.1.7. So it remains to show that $R_\mathfrak{p}$ has a unique nonzero prime ideal.

In fact, the rule $I \mapsto I \cap R$ gives an inclusion-preserving one-to-one correspondence between the proper ideals of $R_{\mathfrak{p}}$ and the proper ideals of R which are contained in $\mathfrak{p}$. In this correspondence, prime ideals corresponds to prime ones. As nonzero prime ideals of R are maximal, one finds that $R_{\mathfrak{p}}$ has only one nonzero prime ideal $\mathfrak{p}R_{\mathfrak{p}}$.

(ii)⇒(iii). Let I be a fractional ideal of R. By Lemma 2.3.5, I can be generated by finitely many nonzero elements $a_1, \ldots, a_n$ in the field K of fractions of R. Let $\mathfrak{p}$ be any maximal ideal of R, and let $v_{\mathfrak{p}}$ be the normalized discrete valuation of K associated with the discrete valuation ring $R_{\mathfrak{p}}$. We may assume $v_{\mathfrak{p}}(a_1) = \min\{v_{\mathfrak{p}}(a_i) \mid 1 \le i \le n\}$. Then each a_i/a_1 belongs to $R_{\mathfrak{p}}$. We have

$$a_i/a_1 = x_i/y \quad \text{for some } \ x_i \in R\ ,\ y \in R \setminus \mathfrak{p}\ .$$

Then $y/a_1 \in I^{-1}$ and hence $y \in II^{-1}$. But $y \notin \mathfrak{p}$. Thus we have proved that the ideal II^{-1} is not contained in any of the maximal ideals of R. Therefore, $II^{-1} = R$.

(iii)⇒(i). Let I be any nonzero ideal of R. Then there exist $a_1, \ldots, a_n \in I$ and $b_1, \ldots, b_n \in I^{-1}$ such that $\sum a_i b_i = 1$. If $x \in I$, then $x = \sum a_i(bx_i)$ and $b_i x \in R$. Hence $a_1, \ldots, a_n$ generate I. Thus R is Noetherian.

Let $x \in K$ be integral over R. By Lemma 2.3.5, $S = R[x]$ is a fractional ideal of R. It is also a ring, i.e., $S^2 \subseteq S$. Hence $S = SR = S(SS^{-1}) = S^2S^{-1} \subseteq SS^{-1} = R$. Thus R is integrally closed.

Let $\mathfrak{p}$ be a nonzero prime ideal of R, $\mathfrak{m}$ a maximal ideal containing it. Then $J := \mathfrak{p}\mathfrak{m}^{-1} \subseteq \mathfrak{m}\mathfrak{m}^{-1} = R$ and $J\mathfrak{m} = \mathfrak{p}R = \mathfrak{p}$. As $\mathfrak{p}$ is prime, we must have either $J \subseteq \mathfrak{p}$ or $\mathfrak{m} \subseteq \mathfrak{p}$. But the first relation would imply that

$$R \subseteq \mathfrak{m}^{-1} = \mathfrak{p}^{-1}\mathfrak{p}\mathfrak{m}^{-1} = \mathfrak{p}^{-1}J \subseteq \mathfrak{p}^{-1}\mathfrak{p} = R\ .$$

Thus $\mathfrak{m}^{-1} = R$ and hence $R = \mathfrak{m}\mathfrak{m}^{-1} = \mathfrak{m}R = \mathfrak{m}$, which is absurd. □

For any ring A, let $\mathrm{Spec}(A)$ denote the set of all prime ideals of A, and let $\mathrm{Spm}(A)$ denote the set of maximal ideals of A. We call $\mathrm{Spec}(A)$ and $\mathrm{Spm}(A)$ the (***prime***) ***spectrum*** and the ***maximal spectrum*** of A respectively.

Lemma 2.3.18. *Let R be an integral domain, and $\mathfrak{p} \in \mathrm{Spec}(R)$. Let I, J be fractional ideals of R.*

1. *$(IR_{\mathfrak{p}}) \cdot (JR_{\mathfrak{p}}) = (IJ)R_{\mathfrak{p}}$, $IR_{\mathfrak{p}} + JR_{\mathfrak{p}} = (I+J)R_{\mathfrak{p}}$ and $(I \cap J)R_{\mathfrak{p}} = IR_{\mathfrak{p}} \cap JR_{\mathfrak{p}}$.*
2. *$(IR_{\mathfrak{p}} : JR_{\mathfrak{p}}) = (I : J)R_{\mathfrak{p}}$ if J is finitely generated.*
3. *If $IR_{\mathfrak{m}} = JR_{\mathfrak{m}}$ for every $\mathfrak{m} \in \mathrm{Spm}(R)$ of R, then $I = J$. In fact[‡], $I = \bigcap_{\mathfrak{m} \in \mathrm{Spm}(R)} IR_{\mathfrak{m}}$.*

Proof. Exercise. □

In what follows, if R is a Dedekind domain and $\mathfrak{p} \in \mathrm{Spm}(R)$, we will denote by $v_{\mathfrak{p}}$ the normalized discrete valuation of $K = \mathrm{Frac}(R)$ associated to the discrete valuation ring $R_{\mathfrak{p}}$.

[‡]Thanks to LIU Yuhan (刘宇涵) for pointing out a gap in my proof in an earlier version of the notes.

Proposition 2.3.19. *Let R be a Dedekind domain.*

1. *The fractional ideals of R form an abelian group $\mathscr{I}(R)$ under multiplication. The subset $\mathscr{P}(R) \subseteq \mathscr{I}(R)$ consisting of principal fractional ideals is a subgroup of $\mathscr{I}(R)$.*

   The quotient group $\mathcal{C}l(R) = \mathscr{I}(R)/\mathscr{P}(R)$ is called the **ideal class group** *(or simply* **class group***) of R.*

2. *The group $\mathscr{I}(R)$ is a free abelian group, and the set $\mathrm{Spm}(R)$ is a basis of $\mathscr{I}(R)$ (as a $\mathbb{Z}$-module). In other words, every fractional ideal I can be written uniquely in the form*

   $$I = \prod_{\mathfrak{p}\in \mathrm{Spm}(R)} \mathfrak{p}^{r_\mathfrak{p}} \qquad \text{where } r_\mathfrak{p} \in \mathbb{Z} \text{ and almost all } r_\mathfrak{p} \text{ are zero.} \tag{2.3.19.1}$$

   Moreover, for every $\mathfrak{p} \in \mathrm{Spm}(R)$, we have

   $$r_\mathfrak{p} = v_\mathfrak{p}(I) := \min_{x\in I} v_\mathfrak{p}(x) \qquad \text{and} \quad IR_\mathfrak{p} = (\mathfrak{p}R_\mathfrak{p})^{v_\mathfrak{p}(I)} .$$

3. *A fractional ideal I is an integral ideal if and only if $v_\mathfrak{p}(I) \geq 0$ for all $\mathfrak{p} \in \mathrm{Spm}(R)$.*

Proof. (1) is clear from the condition (iii) in Prop. 2.3.17.

(2) There exists a nonzero element $a \in R$ such that $I = (aR)^{-1}(aI)$ where $aI \subseteq R$. Thus, to show that maximal ideals generate $\mathscr{I}(R)$, it suffices to show that every integral ideal (i.e., ideals in R), different from R, is a finite product of maximal ideals. We may assume now I itself lies in R and $I \neq R$.

We can find a maximal ideal $\mathfrak{p} \supseteq I$. Hence $I = \mathfrak{p}(I\mathfrak{p}^{-1})$ with $I \subset I\mathfrak{p}^{-1} \subseteq R$. The ascending chain condition now yields the existence of a factorization of the form (2.3.19.1), by considering $I\mathfrak{p}^{-1}$ in place of I.

For any factorization in the form of (2.3.19.1), by Lemma 2.3.18 (1), we have $IR_\mathfrak{p} = (\mathfrak{p}R_\mathfrak{p})^{r_\mathfrak{p}}$. Thus, using Lemma 2.3.11 we find

$$r_\mathfrak{p} = v_\mathfrak{p}(IR_\mathfrak{p}) = v_\mathfrak{p}(I) ,$$

which in return implies the uniqueness of the expression (2.3.19.1).

(3) In the proof of (2) we have seen that an integral ideal in R is a finite product of maximal ideals. So the conclusion is immediate. □

Corollary 2.3.20. *For fractional ideals I, J of a Dedekind domain R, the following conditions are equivalent:*

(i) $I \mid J$, *i.e.,* $J = I.N$ *for some integral ideal N.*

(ii) $I \supseteq J$.

(iii) $v_\mathfrak{p}(I) \leq v_\mathfrak{p}(J)$ *for all* $\mathfrak{p} \in \mathrm{Spm}(R)$.

Proof. (i)⇒(ii) Clear.
(ii)⇒(iii) Use the definition $v_{\mathfrak{p}}(I) = \min_{x \in I} v_{\mathfrak{p}}(x)$.
(iii)⇒(i) Note that $v_{\mathfrak{p}}(I^{-1}J) = v_{\mathfrak{p}}(J) - v_{\mathfrak{p}}(I) \geq 0$ for all $\mathfrak{p}$. So by Prop. 2.3.19 (3), $I^{-1}J$ is an integral ideal. □

Corollary 2.3.21. *Let R be a Dedekind domain with fraction field K. Let $a \in K^*$, and let I, J be fractional ideals of R.*

1. *$(I : J) = IJ^{-1}$.*
2. *For every $\mathfrak{p} \in \mathrm{Spm}(R)$, the map $v_{\mathfrak{p}} : \mathscr{I}(R) \longrightarrow \mathbb{Z}\,; I \mapsto v_{\mathfrak{p}}(I)$ is a surjective group homomorphism.*
3. *For every $\mathfrak{p} \in \mathrm{Spm}(R)$, the following relations hold:*

$$\begin{aligned} v_{\mathfrak{p}}(a) &= v_{\mathfrak{p}}(aR) \\ v_{\mathfrak{p}}(I+J) &= \min\{v_{\mathfrak{p}}(I), v_{\mathfrak{p}}(J)\} \\ v_{\mathfrak{p}}(I \cap J) &= \max\{v_{\mathfrak{p}}(I), v_{\mathfrak{p}}(J)\} \\ v_{\mathfrak{p}}(IJ) &= v_{\mathfrak{p}}(I \cap J) + v_{\mathfrak{p}}(I+J). \end{aligned}$$

4. *We have $v_{\mathfrak{p}}(a) = 0$ for all but finitely many $\mathfrak{p} \in \mathrm{Spm}(R)$. In particular, only finitely many prime ideals contain a.*

Proof. (1)–(3) An easy exercise.
(4) The first assertion follows from the fact $aR = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(a)}$. For the second, note that if $a \in \mathfrak{p} \subseteq \mathfrak{p}R_{\mathfrak{p}}$ then $v_{\mathfrak{p}}(a) > 0$. □

Proposition 2.3.22. *For a Dedekind domain R and integral ideals I, J of R, the following conditions are equivalent:*

(i) *I and J are coprime, i.e., $I + J = R$.*
(ii) *$IJ = I \cap J$.*
(iii) *$v_{\mathfrak{p}}(I)v_{\mathfrak{p}}(J) = 0$ for all $\mathfrak{p} \in \mathrm{Spm}(R)$. In other words, the set of maximal ideals dividing I is disjoint with the set of maximal ideals dividing J.*

Proof. (i)⇒(ii) Exercise.
(ii)⇒(iii) Use the equalities $v_{\mathfrak{p}}(I)+v_{\mathfrak{p}}(J) = v_{\mathfrak{p}}(IJ)$ and $v_{\mathfrak{p}}(I \cap J) = \max\{v_{\mathfrak{p}}(I), v_{\mathfrak{p}}(J)\}$.
(iii)⇒(i) One has $v_{\mathfrak{p}}(I+J) = \min\{v_{\mathfrak{p}}(I), v_{\mathfrak{p}}(J)\} = 0$ for all $\mathfrak{p}$. □

2.3.4 Overrings of Dedekind domains

Definition 2.3.23. Let R be an integral domain with fraction field K. An ***overring*** of R is a subring R' of K such that $R \subseteq R' \neq K$. (According to this definition, a field does not have any overring.) ■

Lemma 2.3.24. *If R is a discrete valuation ring, then R has no overring other than itself.*

Proof. Let R' be a subring of the fraction field $K = \mathrm{Frac}(R)$ such that $R \subseteq R'$. Assume there exists $x \in R' \setminus R$. By choosing a uniformizer π of R, we have $x = u\pi^{-m}$ for some $u \in R^*$ and some $m \in \mathbb{N}^*$. Then $\pi^{-1} = u^{-1}x\pi^{m-1} \in R'$. This implies $R' = K$. □

Proposition 2.3.25 (Noether–Grell)**.** *Let R be a Dedekind domain and let R' be an overring of R.*

1. *For every nonzero prime ideal $\mathfrak{p}'$ of R', the intersection $\mathfrak{p} := \mathfrak{p}' \cap R$ is a nonzero prime ideal of R, the localizations $R_{\mathfrak{p}}$ and $R'_{\mathfrak{p}'}$ are equal, and $\mathfrak{p}' = \mathfrak{p}R'_{\mathfrak{p}'} \cap R' = \mathfrak{p}R_{\mathfrak{p}} \cap R'$.*

   In particular, the natural map

   $$\mathrm{Spec}(R') \longrightarrow \mathrm{Spec}(R)\ ; \quad \mathfrak{p}' \longmapsto \mathfrak{p}' \cap R$$

   is injective.

2. *R' is a Dedekind domain.*

Proof. (1) Let $\mathfrak{p}'$ be a nonzero prime ideal of R'. If $x \in \mathfrak{p}'$ is a nonzero element, we can write $x = a/b$ with $a, b \in R \setminus \{0\}$. Then $0 \neq a = bx \in \mathfrak{p}' \cap R = \mathfrak{p}$. Hence $\mathfrak{p}$ is a nonzero prime ideal of R. The inclusion $R_{\mathfrak{p}} \subseteq R'_{\mathfrak{p}'}$ is clear. Since R is a Dedekind domain, $R_{\mathfrak{p}}$ is a discrete valuation ring. Since $\mathfrak{p}' \neq 0$, we have $R'_{\mathfrak{p}'} \neq \mathrm{Frac}(R)$. So $R'_{\mathfrak{p}'}$ is an overring of $R_{\mathfrak{p}}$. By Lemma 2.3.24, $R_{\mathfrak{p}} = R'_{\mathfrak{p}'}$. Now $\mathfrak{p}R_{\mathfrak{p}}$ and $\mathfrak{p}'R'_{\mathfrak{p}'}$ are both the unique maximal ideal of the local ring $R_{\mathfrak{p}} = R'_{\mathfrak{p}'}$. Hence $\mathfrak{p}R_{\mathfrak{p}} = \mathfrak{p}R'_{\mathfrak{p}'} = \mathfrak{p}'R'_{\mathfrak{p}'}$, and it follows that $\mathfrak{p}R'_{\mathfrak{p}'} \cap R' = \mathfrak{p}'R'_{\mathfrak{p}'} \cap R' = \mathfrak{p}'$.

(2) From (1) we see that the localization of R' at every nonzero prime ideal $\mathfrak{p}'$ is a DVR. It remains to prove that R' is a Noetherian ring, by Prop. 2.3.17.

We first show that for any nonzero element $x \in R'$, only finitely many principal ideals of R' can contain x. Indeed, if $\mathfrak{p}'$ is a prime ideal of R' and $x \in \mathfrak{p}'$, then by (1), $\mathfrak{p} = R \cap \mathfrak{p}'$ is a nonzero prime ideal of R and $R_{\mathfrak{p}} = R'_{\mathfrak{p}'}$. Since $x \in \mathfrak{p}' \subseteq \mathfrak{p}'R'_{\mathfrak{p}'} = \mathfrak{p}R_{\mathfrak{p}}$, the $\mathfrak{p}$-adic valuation $v_{\mathfrak{p}}(x)$ of x is strictly positive. But this relation holds only for the finitely many prime ideals of R that appear with positive expoents in the factorization of the fractional ideal xR. By the injectivity of the map $\mathrm{Spec}(R') \to \mathrm{Spec}(R)$, we see that only finitely many $\mathfrak{p}' \in \mathrm{Spec}(R')$ can contain x.

Now let $\mathfrak{a}$ be a nonzero ideal of R'. We shall prove that $\mathfrak{a}$ is finitely generated. We choose a nonzero element $x \in \mathfrak{a}$ and let $\mathcal{P}$ be the finite set of prime ideals of R' that contain x. For each $\mathfrak{p} \in \mathcal{P}$, the localization $R'_{\mathfrak{p}}$ is a DVR by (1). Hence there exists

$a_\mathfrak{p} \in \mathfrak{a}$ such that $\mathfrak{a}R'_\mathfrak{p} = a_\mathfrak{p}R'_\mathfrak{p}$. Denote the ideal of R' generated by x and by all $a_\mathfrak{p}$, for $\mathfrak{p} \in \mathcal{P}$, by $\mathfrak{a}_0$. It is contained in $\mathfrak{a}$, by construction.

It remains to show that $\mathfrak{a} \subseteq \mathfrak{a}_0$. Indeed, if $\mathfrak{q}$ is a prime ideal of R' and $\mathfrak{q} \notin \mathcal{P}$, then $x \notin \mathfrak{q}$, so $\mathfrak{a}_0 \subseteq \mathfrak{q}$. Thus $\mathfrak{a}_0 R'_\mathfrak{q} = R'_\mathfrak{q} \supseteq \mathfrak{a}R'_\mathfrak{q}$. For any $\mathfrak{p} \in \mathcal{P}$, we have $\mathfrak{a}R'_\mathfrak{p} = a_\mathfrak{p}R'_\mathfrak{p} \subseteq \mathfrak{a}_0 R'_\mathfrak{p}$. Therefore,

$$\mathfrak{a} = \bigcap_{\mathfrak{q} \in \mathrm{Spec}(R')} \mathfrak{a}R'_\mathfrak{q} \subseteq \bigcap_{\mathfrak{q} \in \mathrm{Spec}(R')} \mathfrak{a}_0 R'_\mathfrak{q} = \mathfrak{a}_0 .$$

This completes the proof. □

2.4 Extensions of Dedekind domains and ramification of primes

Throughout this section, let A be a Dedekind domain with fraction field K. We denote by $\overline{K}$ an algebraic closure of K and let L/K be a finite field extension. Let B be the integral closure of A in L.

2.4.1 Prime factorizations in finite extensions

Theorem 2.4.1 (Krull–Akizuki)**.** *With notation and hypotheses as above, the ring B is a Dedekind domain.*

Proof. We refer the reader to [Bou06, § VII.2.5] for a proof in the general case. Here we only give a proof under the following hypothesis:

Hypothesis (F): The ring B is a finitely generated A-module.

By Cor. 2.1.8, B is integrally closed in its field of fractions L. Clearly, the hypothesis implies that B is Noetherian. We need to show that the maximal ideals of B are exactly the nonzero prime ideals.

Let $\mathfrak{P}$ be a prime ideal of B and let $\mathfrak{p} = \mathfrak{P} \cap A$. By Lemma 2.1.13, we have $\mathfrak{P} = 0$ if and only if $\mathfrak{p} = 0$. So, if $\mathfrak{P} \neq 0$, then $\mathfrak{p}$ is a maximal ideal of A. By Prop. 2.1.14, $\mathfrak{P}$ is a maximal ideal of B. Conversely, if $\mathfrak{P}$ is maximal, Prop. 2.1.14 implies that $\mathfrak{p}$ is maximal and hence nonzero. Hence $\mathfrak{P} \neq 0$. This completes the proof. □

Remark 2.4.2. Here are some most interesting cases where hypothesis (F) is satisfied:

1. The field extension L/K is a separable extension.

   This case follows from Prop. 2.1.12.

2. The ring A is a localization of a finitely generated algebra over a field.

   (See e.g. [Bou06, § V.3.2, Thm. 2].)

In the next chapter, we will see that the hypothesis is also satisfied when A is a complete DVR (Thm. 3.3.2).

As an immediate consequence of Case 1 above (and Example 2.3.15), the ring of algebraic integers in a number field is a Dedekind domain. ■

(2.4.3) Let $\mathfrak{P}$ be a maximal ideal of B and $\mathfrak{p}$ a maximal ideal of A. Then the following conditions are equivalent (by Prop. 2.1.15 and Cor. 2.3.20):

(1) $\mathfrak{P}$ lies over $\mathfrak{p}$, i.e., $\mathfrak{p} = \mathfrak{P} \cap A$.

(2) $\mathfrak{p}B \subseteq \mathfrak{P}$.

(3) $\mathfrak{p}B$ divides $\mathfrak{P}$ as fractional ideals of B (cf. (2.3.3))

So we will also say that $\mathfrak{P}$ ***divides*** $\mathfrak{p}$ and write $\mathfrak{P} \,|\, \mathfrak{p}$ when $\mathfrak{P}$ lies over $\mathfrak{p}$. ■

(2.4.4) Now we fix a maximal ideal $\mathfrak{P}$ of B, lying over a maximal ideal $\mathfrak{p}$ of A. The ***ramification index*** of $\mathfrak{P}$ over A (or over $\mathfrak{p}$, or over K), denoted $e_{\mathfrak{P}} = e(\mathfrak{P}|\mathfrak{p})$, is defined to be the integer $v_{\mathfrak{P}}(\mathfrak{p}B)$. In other words, $e_{\mathfrak{P}}$ is the exponent of $\mathfrak{P}$ in the decomposition of $\mathfrak{p}B$ into products of maximal ideals:

$$\mathfrak{p}B = \prod_{\mathfrak{Q} \,|\, \mathfrak{p}} \mathfrak{Q}^{e_{\mathfrak{Q}}} .$$

Write $\kappa(\mathfrak{p}) = A/\mathfrak{p}$ and $\kappa(\mathfrak{P}) = B/\mathfrak{P}$. The degree

$$f_{\mathfrak{P}} = f(\mathfrak{P}|\mathfrak{p}) := [\kappa(\mathfrak{P}) \,:\, \kappa(\mathfrak{p})] \;\in\; \mathbb{N} \cup \{ +\infty \}$$

is called the ***residue degree*** or ***inertia degree*** of $\mathfrak{P}$ over A. When hypothesis (F) is satisfied, $B/\mathfrak{p}B$ is a finite-dimensional algebra over the field $\kappa(\mathfrak{p})$. Hence $\kappa(\mathfrak{P}) = B/\mathfrak{P}$ is a finite extension of $\kappa(\mathfrak{p})$, whence $f(\mathfrak{P} \,|\, \mathfrak{p}) < +\infty$.

If M/L is another finite extension and $\mathfrak{Q}$ a maximal ideal of the integral closure of A in M which lies over $\mathfrak{P}$, then

$$e(\mathfrak{Q}|\mathfrak{p}) = e(\mathfrak{Q}|\mathfrak{P})e(\mathfrak{P}|\mathfrak{p}) \;, \quad f(\mathfrak{Q}|\mathfrak{p}) = f(\mathfrak{Q}|\mathfrak{P})f(\mathfrak{P}|\mathfrak{p}) \tag{2.4.4.1}$$

as can be easily seen from the definitions. ■

Definition 2.4.5. Let $\mathfrak{p}$ be a maximal ideal of A. Let $g_{\mathfrak{p}}$ be the number of prime ideals of B lying over $\mathfrak{p}$. Note that $g_{\mathfrak{p}} \geq 1$ by Prop. 2.1.15, and $g_{\mathfrak{p}} < +\infty$ by Prop. 2.3.19 (cf. (2.4.3)).

(1) We say the extension L/K is ***totally ramified*** at $\mathfrak{p}$, or $\mathfrak{p}$ ***totally ramifies*** in L, if $g_{\mathfrak{p}} = 1$ and the only prime $\mathfrak{P}$ of B above $\mathfrak{p}$ has residue degree $f_{\mathfrak{P}} = 1$.

(2) Let $\mathfrak{P}$ be a prime ideal of B lying over $\mathfrak{p}$. We say L/K is ***unramified*** at $\mathfrak{P}$ if $e(\mathfrak{P} \,|\, \mathfrak{p}) = 1$ and if the field extension $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ is separable.

We say L/K is ***unramified*** at $\mathfrak{p}$, or $\mathfrak{p}$ is unramified in L/K, if it is unramified at every prime ideal $\mathfrak{P} \,|\, \mathfrak{p}$. Otherwise we say that $\mathfrak{p}$ is ***ramified*** in L/K.

(3) If $g_{\mathfrak{p}} = 1$ and the only prime $\mathfrak{P}$ of B above $\mathfrak{p}$ has residue degree $f_{\mathfrak{P}} = [L : K]$ and ramification index $e_{\mathfrak{P}} = 1$ (hence $\mathfrak{p}B$ is a maximal ideal B), then we say that $\mathfrak{p}$ is ***inert*** in L/K.

Finally, recall (from (2.1.23)) that $\mathfrak{p}$ is said to ***split completely*** in L/K if $g_{\mathfrak{p}} = [L : K]$. In this case we also say that L/K is ***totally split*** at $\mathfrak{p}$.

By Prop. 2.4.6 below, when hypothesis (F) holds, $\mathfrak{p}$ totally ramifies in L/K if and only if there exists $\mathfrak{P} \in \mathrm{Spm}(B)$ lying over $\mathfrak{p}$ such that $e_{\mathfrak{P}} = [L : K]$, and $\mathfrak{p}$ is inert in L/K if and only if there exists $\mathfrak{P} \in \mathrm{Spm}(B)$ lying over $\mathfrak{p}$ such that $f_{\mathfrak{P}} = [L : K]$. ■

Proposition 2.4.6. *Assume that hypothesis (F) holds. Let $\mathfrak{p}$ be a maximal ideal of A.*

Then the ring $B/\mathfrak{p}B$ is a $\kappa(\mathfrak{p})$-algebra of dimension $n = [L : K]$, isomorphic to the product $\prod_{\mathfrak{P}\,|\,\mathfrak{p}} B/\mathfrak{P}^{e_\mathfrak{P}}$, and we have the formula

$$[L : K] = \sum_{\mathfrak{P}\,|\,\mathfrak{p}} e_\mathfrak{P} f_\mathfrak{P} .$$

Therefore, the number $g_\mathfrak{p}$ of prime ideals $\mathfrak{P}$ which divide $\mathfrak{p}$ is at least 1 and at most $n = [L : K]$.

Proof. Let $S = A \setminus \mathfrak{p}$, $A' = S^{-1}A$ and $B' = S^{-1}B$. The ring $A' = A_\mathfrak{p}$ is a DVR, and B' is its integral closure in L (Lemma 2.1.7). One has $A'/\mathfrak{p}A' = A/\mathfrak{p}$ and since S has no intersection with any maximal ideal of $B/\mathfrak{p}B$, $B'/\mathfrak{p}B' = B/\mathfrak{p}B$. As A' is a PID, hypothesis (F) shows that B' is a free A'-module of rank $n = [L : K]$ and $B'/\mathfrak{p}B'$ is free of rank n over $A'/\mathfrak{p}A'$. Thus $B/\mathfrak{p}B$ is an algebra of dimension n over $\kappa(\mathfrak{p})$.

Since $\mathfrak{p}B = \prod \mathfrak{P}^{e_\mathfrak{P}} = \bigcap \mathfrak{P}^{e_\mathfrak{P}}$, the canonical map

$$B/\mathfrak{p}B \longrightarrow \prod_{\mathfrak{P}\,|\,\mathfrak{p}} B/\mathfrak{P}^{e_\mathfrak{P}}$$

is an isomorphism by the Chinese remainder theorem. By comparing degrees, one finds that

$$n = \sum n_\mathfrak{P} \quad \text{where} \quad n_\mathfrak{P} = \dim_{\kappa(\mathfrak{p})}(B/\mathfrak{P}^{e_\mathfrak{P}}) .$$

For a fixed $\mathfrak{P}$, if R is the localization of B at $\mathfrak{P}$, one has

$$B/\mathfrak{P}^i \cong R/\mathfrak{P}^i R \quad \text{and} \quad B/\mathfrak{P} \cong \mathfrak{P}^i R/\mathfrak{P}^{i+1} R \ \text{ for every } i \in \mathbb{N}$$

as B-modules (hence also as A-modules). Using the exact sequences of $\kappa(\mathfrak{p})$-modules

$$0 \longrightarrow \mathfrak{P}^i R/\mathfrak{P}^{i+1} R \longrightarrow R/\mathfrak{P}^{i+1} R \longrightarrow R/\mathfrak{P}^i R \longrightarrow 0$$

for $0 \le i \le e - 1$, we get

$$n_\mathfrak{P} = \dim_{\kappa(\mathfrak{P})}(B/\mathfrak{P}^{e_\mathfrak{P}}) = \sum_{i=0}^{e_\mathfrak{P}-1} \dim_{\kappa(\mathfrak{P})} \frac{\mathfrak{P}^i R}{\mathfrak{P}^{i+1} R} = f_\mathfrak{P} e_\mathfrak{P} .$$

This completes the proof of the proposition. □

Proposition 2.4.7. *Suppose that L/K is a Galois extension of degree n with group $G = \mathrm{Gal}(L/K)$. Let $\mathfrak{p}$ be a maximal ideal of A, and $g_\mathfrak{p}$ the number of maximal ideals $\mathfrak{P} \subseteq B$ lying over $\mathfrak{p}$.*

Then the integers $e_\mathfrak{P}$ and $f_\mathfrak{P}$ for $\mathfrak{P}\,|\,\mathfrak{p}$ depend only on $\mathfrak{p}$. If one denotes them by $e_\mathfrak{p}$ and $f_\mathfrak{p}$ respectively, then $n = e_\mathfrak{p} f_\mathfrak{p} g_\mathfrak{p}$.

Proof. That $e_\mathfrak{P}$ and $f_\mathfrak{P}$ are independent of $\mathfrak{P}$ follows from Prop. 2.1.16. The relation $n = e_\mathfrak{p} f_\mathfrak{p} g_\mathfrak{p}$ is a special case of the formula in Prop. 2.4.6. □

(2.4.8) Let us keep the notation and hypotheses of Prop. 2.4.7. We fix a maximal ideal $\mathfrak{P}$ lying over $\mathfrak{p}$. Write

$$\begin{aligned}
&\kappa = \kappa(\mathfrak{p})\,,\ \ \ell = \kappa(\mathfrak{P})\,;\ \ \ell_0 = \text{ the separable closure of } \kappa \text{ in } \ell\,;\\
&e = e_{\mathfrak{p}}\,,\ f = f_{\mathfrak{p}}\,,\ \ g = g_{\mathfrak{p}}\,;\ \ f_0 = [\ell_0 : \kappa]\,,\ p^s = [\ell : \ell_0] = f/f_0\,;\\
&D = D(L/K) = G_{\mathfrak{P}} \ \text{(the decomposition group)}\,,\\
&K_D = L^D \ \text{(the decomposition field)}\,;\mathfrak{P}_D = \mathfrak{P} \cap K_D\,,\\
&I = I(L/K) = I_{\mathfrak{P}} \ \text{(the inertia group)}\,,\\
&K_I = L^I \ \text{(the inertia field)}\,;\mathfrak{P}_I = \mathfrak{P} \cap K_I\,,
\end{aligned}$$

For any intermediate field E between K and L, put

$$\begin{aligned}
&B_E = E \cap B\,,\ \ \mathfrak{P}_E = \mathfrak{P} \cap E\,,\ \ \kappa(\mathfrak{P}_E) := B_E/\mathfrak{P}_E\,;\\
&D(L/E) = \text{ the decomposition group of } \mathfrak{P}/\mathfrak{P}_E\,;\\
&I(L/E) = \text{ the decomposition group of } \mathfrak{P}/\mathfrak{P}_E\,;
\end{aligned}$$

and when E/K is Galois,

$$\begin{aligned}
&D(E/K) = \text{ the decomposition group of } \mathfrak{P}_E/\mathfrak{p}\,;\\
&I(E/K) = \text{ the decomposition group of } \mathfrak{P}_E/\mathfrak{p}\,.
\end{aligned}$$

The diagram

$$\begin{array}{ccc}
L & \sim\sim\sim\sim\sim\sim & \ell = \kappa(\mathfrak{P}) \\
{\scriptstyle ep^s}\big| & & \big|{\scriptstyle p^s} \\
K_I & \sim\sim\sim\sim\sim\sim & \ell_0 = \kappa(\mathfrak{P}_I) \\
{\scriptstyle f_0}\big| & & \big|{\scriptstyle f_0} \\
K_D & \sim\sim\sim\sim\sim\sim & \kappa(\mathfrak{P}_D) \\
{\scriptstyle g}\big| & & \big\| \\
K & \sim\sim\sim\sim\sim\sim & \kappa = \kappa(\mathfrak{p})
\end{array}$$

will be part of the next proposition. ■

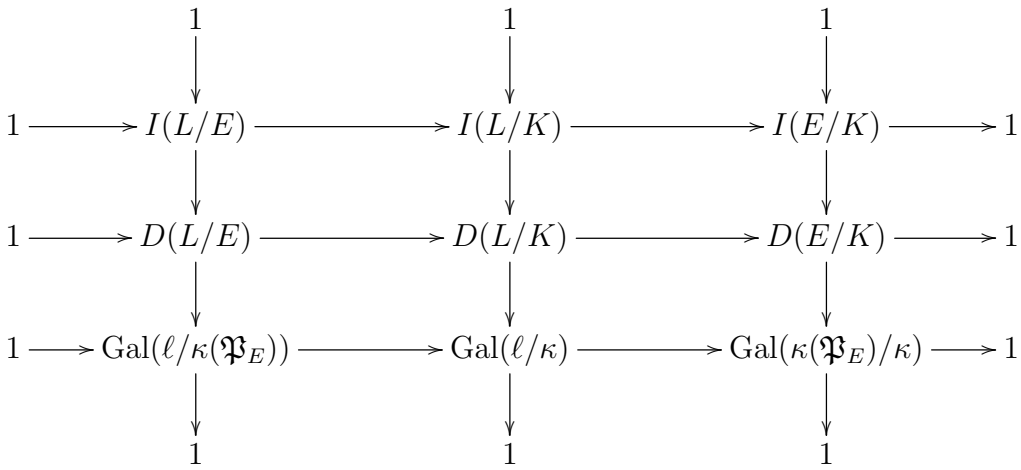
Proposition 2.4.9. *With notation and hypotheses as in* (2.4.8)*, we have:*

1. $[L : K_I] = ep^s$, $[K_I : K_D] = f_0$, $[K_D : K] = g$.
2. $e(\mathfrak{P}|\mathfrak{P}_I) = e$, $e(\mathfrak{P}_I|\mathfrak{P}_D) = e(\mathfrak{P}_D|\mathfrak{p}) = e(\mathfrak{P}_I|\mathfrak{p}) = 1$.
3. $\kappa(\mathfrak{P}_I) = \ell_0$ *and* $\kappa(\mathfrak{P}_D) = \kappa$. *In particular,*

$$[\ell : \kappa(\mathfrak{P}_I)] = p^s\,,\ [\kappa(\mathfrak{P}_I) : \kappa(\mathfrak{P}_D)] = f_0\,,\ [\kappa(\mathfrak{P}_D) : \kappa] = 1\,.$$

4. $D(L/E) = D \cap \mathrm{Gal}(L/E)$ *and* $I(L/E) = I \cap \mathrm{Gal}(L/E)$.

5. *If E/K is Galois, the diagram below is commutative, and its rows and columns are exact:*



Proof. We have seen $[K_D : K] = g$ in Prop. 2.1.18 (1). Hence by Prop. 2.4.7, $|D| = [L : K_D] = n/g = ef = ep^s f_0$. Then from Prop. 2.1.21 we obtain

$$[L : K_I] = |I| = \frac{|D|}{|\operatorname{Gal}(\ell/\kappa)|} = |D|/f_0 = ep^s \text{ and hence } [K_I : K_D] = \frac{[L : K_D]}{[L : K_I]} = f_0 .$$

This proves (1).

The equality $\kappa(\mathfrak{P}_D) = \kappa$ has been proved in Prop. 2.1.19. On the one hand, $[\kappa(\mathfrak{P}_I) : \kappa] = [\kappa(\mathfrak{P}_I) : \kappa(\mathfrak{P}_D)] \leq [K_I : K_D] \leq f_0$. On the other hand, the inertia group of $\mathfrak{P}|\mathfrak{P}_I$ is the whole of the Galois group $\operatorname{Gal}(L/K_I)$ by construction, therefore Prop. 2.1.21 implies that $\ell/\kappa(\mathfrak{P}_I)$ is a purely inseparable extension. In particular, every element of ℓ_0 is purely inseparable over $\kappa(\mathfrak{P}_I)$. But elements of ℓ_0 are separable over κ hence also over $\kappa(\mathfrak{P}_I)$. So $\ell_0 \subseteq \kappa(\mathfrak{P}_I)$, whence $[\kappa(\mathfrak{P}_I) : \kappa] \geq [\ell_0 : \kappa] = f_0$. This proves $[\kappa(\mathfrak{P}_I) : \kappa] = f_0 = [K_I : K_D]$ and $\kappa(\mathfrak{P}_I) = \ell_0$. In Prop. 2.1.18 (3) we have seen that $g(\mathfrak{P}|\mathfrak{P}_D) = 1$. Applying Prop. 2.4.7 to the extension L/K_D yields

$$e(\mathfrak{P}|\mathfrak{P}_D)f = e(\mathfrak{P}|\mathfrak{P}_D)f(\mathfrak{P}|\mathfrak{P}_D) = [L : K_D] = ef .$$

Hence $e(\mathfrak{P}|\mathfrak{P}_D) = e$. Similarly, since $[K_I : K_D] = f_0 = f(\mathfrak{P}_I|\mathfrak{P}_D)$, $e(\mathfrak{P}_I|\mathfrak{P}_D) = 1$. We have thus shown (2) and (3).

The proofs of (4) and (5) are left to the reader as exercises. □

Corollary 2.4.10. *With notation and hypotheses as in (2.4.8), if ℓ/κ is separable, then it is a Galois extension with Galois group $\operatorname{Gal}(\ell/\kappa) \cong D/I$, and one has*

$$\ell = \kappa(K_I) , \quad [L : K_I] = e , \quad [K_I : K_D] = f , \quad [K_D : K] = g .$$

Proof. The extension ℓ/κ is normal by Prop. 2.1.21. So it is a Galois extension when it is separable. The other assertions are immediate from Prop. 2.4.9. □

2.4.2 Ideal norm

(2.4.11) Recall that $A \subseteq B$ be an integral extension of Dedekind domains (Thm. 2.4.1). Let $\mathscr{I}(A)$ and $\mathscr{I}(B)$ be their groups of fractional ideals (cf. Prop. 2.3.19). The inclusion map $\iota : A \hookrightarrow B$ induces a group homomorphism

$$\iota^* \ : \ \mathscr{I}(A) \longrightarrow \mathscr{I}(B)\,; \quad \mathfrak{a} \longmapsto \mathfrak{a}B\,.$$

This homomorphism is injective. In fact, distinct maximal ideals of A have disjoint sets of prime factors in $\mathscr{I}(B)$, so it suffices to show $\iota^*(\mathfrak{p}) \neq B$ for every maximal ideal $\mathfrak{p}$ of A. This latter fact has been proved in Prop. 2.1.15. ■

(2.4.12) We assume further that hypothesis (F) holds. Then we can define the ***ideal norm*** map

$$N = N_{L/K} \ : \ \mathscr{I}(B) \longrightarrow \mathscr{I}(A)$$

by setting

$$N(\mathfrak{P}) = \mathfrak{p}^{f(\mathfrak{P}|\mathfrak{p})}\,, \quad \text{where } \ \mathfrak{p} = \mathfrak{P} \cap A \quad \text{ for } \mathfrak{P} \in \mathrm{Spm}(B)\,.$$

It follows from Prop. 2.4.6 that

$$N_{L/K}(\iota^*(\mathfrak{a})) = \mathfrak{a}^{[L:K]} \tag{2.4.12.1}$$

for every $\mathfrak{a} \in \mathscr{I}(A)$.

Moreover, if E/K is a subextension of L/K, then the integral closure of A in E is a finitely generated A-module since it is a submodule of B. One easily checks that

$$N_{L/K} = N_{E/K} \circ N_{L/E} \ : \ \mathscr{I}(B) \longrightarrow \mathscr{I}(A) \tag{2.4.12.2}$$

by using (2.4.4.1). ■

Lemma 2.4.13. *Assume L/K is a finite Galois extension with group $G = \mathrm{Gal}(L/K)$. Fix a maximal ideal $\mathfrak{P}$ of B lying over a maximal ideal $\mathfrak{p}$ of A and write e, f, g for $e_\mathfrak{p}$, $f_\mathfrak{p}$, $g_\mathfrak{p}$. Then*

$$N_{L/K}(\mathfrak{P}).B = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^{ef} = \prod_{\sigma \in G} \sigma\mathfrak{P}\,,$$

where $\mathfrak{P}_1 = \mathfrak{P}, \mathfrak{P}_2, \ldots, \mathfrak{P}_g$ are the distinct maximal ideals of B lying over $\mathfrak{p}$.

Proof. By Prop. 2.4.7, $\mathfrak{p}B = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e$ and the first equality follows easily. The decomposition group $D = G_\mathfrak{P}$ has order $n/g = ef$. If $G = \cup_{i=1}^g \sigma_i D$ is a coset decomposition such that $\sigma_i\mathfrak{P} = \mathfrak{P}_i$, then

$$\prod_{\sigma \in G} \sigma\mathfrak{P} = \prod_{i=1}^{g} \prod_{\sigma \in \sigma_i D} \sigma\mathfrak{P} = \prod_{i=1}^{g} (\mathfrak{P}_i)^{|D|} = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^{ef}\,.$$

This proves the lemma. □

Proposition 2.4.14. *Suppose that hypothesis (F) holds.*

Then for every $x \in L^*$ we have $N_{L/K}(xB) = N_{L/K}(x)A$.

Proof. In view of (2.4.12.1) and (2.4.12.2), we may assume $L = K(x)$. Let $f(t) \in A[t]$ be the minimal polynomial polynomial of x. In case $K(x)/K$ is inseparable, $[L : K] = p^r$ is a prime power and f is the form $f(t) = t^{p^r} + a_0$, where $p = \mathrm{char}(K)$.

Since both sides are multiplicative, we may assume $x \in B$. Thus $a := N_{L/K}(x) \in A$ (cf. Prop. 2.1.11). If $x^{-1} \in B$, then $N_{L/K}(x)^{-1} = N_{L/K}(x^{-1}) \in A$. Therefore, a is a unit in A if x is a unit in B. In this case, $N_{L/K}(xB) = N_{L/K}(B) = A = aA$.

We may thus assume $x \notin B^*$. Then for any maximal ideal $\mathfrak{P}$ of B containing x, we have $a = N_{L/K}(x) \in \mathfrak{p} = \mathfrak{P} \cap A$. It suffices to show that for any maximal ideal $\mathfrak{p}$ containing a, $v_\mathfrak{p}(N_{L/K}(xB)) = v_\mathfrak{p}(N_{L/K}(x)) = v_\mathfrak{p}(a)$.

We fix such a $\mathfrak{p}$ and put $B_\mathfrak{p} = B \otimes_A A_\mathfrak{p}$. Then

$$N_{L/K}(xB_\mathfrak{p}) = \prod_{\mathfrak{P}\,|\,\mathfrak{p}} N_{L/K}\left(\mathfrak{P}B_\mathfrak{p}\right)^{v_\mathfrak{P}(x)} = \prod_{\mathfrak{P}\,|\,\mathfrak{p}} \left(\mathfrak{p}A_\mathfrak{p}\right)^{f_\mathfrak{P} v_\mathfrak{P}(x)}$$

$$= \prod_{\mathfrak{P}\,|\,\mathfrak{p}} \left(N_{L/K}(\mathfrak{P})A_\mathfrak{p}\right)^{v_\mathfrak{P}(x)} = \left(\prod_{\mathfrak{P}\,|\,\mathfrak{p}} N_{L/K}(\mathfrak{P})^{v_\mathfrak{P}(x)}\right) A_\mathfrak{p} = N_{L/K}(xB)A_\mathfrak{p}\,.$$

Thus, by localization at $\mathfrak{p}$ we may assume A is a DVR, $\mathfrak{p}$ is the maximal ideal of A and $a = N_{L/K}(x) \in \mathfrak{p}$.

If x is inseparable over K, then $f(t) = t^{p^r} + a_0$ and

$$a = N_{L/K}(x) = (-1)^{p^r} a_0 = -a_0 = x^{p^r}\,.$$

Hence $aB = a_0 B = (xB)^{p^r}$ and

$$(aA)^{p^r} = (aA)^{[L:K]} = N_{L/K}(aB) = N_{L/K}((xB)^{p^r}) = N_{L/K}(xB)^{p^r}\,.$$

Since $\mathscr{I}(A)$ is a free abelian group, it follows that $N_{L/K}(xB) = aA = N_{L/K}(x)A$.

It remains to treat the case with x separable over K. Let M/K be the Galois closure of L/K and C the integral closure of A. Then

$$N_{M/K}(xC) = N_{L/K}(xB)^{[M:L]}\,, \quad N_{M/K}(x) = N_{L/K}(x)^{[M:L]}\,.$$

It is sufficient to prove $N_{M/K}(xC) = N_{M/K}(x)A$.

Let $xC = \prod_{\mathfrak{Q}\,|\,\mathfrak{p}} \mathfrak{Q}^{v_\mathfrak{Q}(x)}$ be the factorization of xC in the ideal group $\mathscr{I}(C)$. Then we have

$$\sigma(x)C = \prod_{\mathfrak{Q}\,|\,\mathfrak{p}} \sigma(\mathfrak{Q})^{v_\mathfrak{Q}(x)}$$

for any $\sigma \in G = \mathrm{Gal}(M/K)$ and hence,

$$\begin{aligned}
N_{M/K}(x)C = \prod_{\sigma\in G} \sigma(x)C &= \prod_{\sigma\in G}\prod_{\mathfrak{Q}\,|\,\mathfrak{p}} \sigma(\mathfrak{Q})^{v_\mathfrak{Q}(x)} = \prod_{\mathfrak{Q}\,|\,\mathfrak{p}} \left(\prod_{\sigma\in G} \sigma(\mathfrak{Q})\right)^{v_\mathfrak{Q}(x)} \\
&= \prod_{\mathfrak{Q}\,|\,\mathfrak{p}} \left(N_{M/K}(\mathfrak{Q})C\right)^{v_\mathfrak{Q}(x)} \qquad \text{(by Lemma 2.4.13)} \\
&= \left(\prod_{\mathfrak{Q}\,|\,\mathfrak{p}} N_{M/K}(\mathfrak{Q})^{v_\mathfrak{Q}(x)}\right) C \\
&= N_{M/K}(xC)C \qquad \text{(by the factorization of } xC)
\end{aligned}$$

This shows $N_{M/K}(x)C = N_{M/K}(xC)C$. Since the inclusion map $\mathscr{I}(A) \to \mathscr{I}(C)\,,\ \mathfrak{a} \mapsto \mathfrak{a}C$ is injective (cf. (2.4.11)), we get $N_{M/K}(x)A = N_{M/K}(xC)$ as desired. □

(2.4.15) Now consider the case $K = \mathbb{Q}$ and $A = \mathbb{Z}$. Then L is a number field and B is the ring of algebraic integers $\mathcal{O}_L$ in L. Since every fractional ideal of $\mathbb{Z}$ is principal, for any fractional ideal $\mathfrak{b}$ of $\mathcal{O}_L$, there is a unique positive rational number $\mathbf{N}(\mathfrak{b})$ such that $N_{L/K}(\mathfrak{b}) = \mathbf{N}(\mathfrak{b})\mathbb{Z}$. We call $\mathbf{N}(\mathfrak{b})$ the ***absolute norm*** of $\mathfrak{b}$. Clearly, if $\mathfrak{b}$ is a nonzero integral ideal of $\mathcal{O}_L$, then $\mathbf{N}(\mathfrak{b})$ is a positive integer.

Note that the absolute norm is multiplicative as is the ideal norm. ■

Proposition 2.4.16. *Let L be a number field and let $\mathfrak{b}$ be a nonzero integral ideal of $\mathcal{O}_L$.*

Then the quotient ring $\mathcal{O}_L/\mathfrak{b}$ is finite and $\mathbf{N}(\mathfrak{b}) = \#\big(\mathcal{O}_L/\mathfrak{b}\big)$.

Proof. By the multiplicativity of $\mathbf{N}$ and the Chinese remainder theorem, we may reduce to the case where $\mathfrak{b} = \mathfrak{P}^e$ for some $\mathfrak{P} \in \mathrm{Spm}(\mathcal{O}_L)$ and $e \in \mathbb{N}$. Using the exact sequences

$$0 \longrightarrow \mathfrak{P}^i/\mathfrak{P}^{i+1} \longrightarrow \mathcal{O}_L/\mathfrak{P}^{i+1} \longrightarrow \mathcal{O}_L/\mathfrak{P}^i \longrightarrow 0\,, \quad i \in \mathbb{N}$$

and the isomorphisms $\mathfrak{P}^i/\mathfrak{P}^{i+1} \cong \mathcal{O}_L/\mathfrak{P}$, we find that $\#\big(\mathcal{O}_L/\mathfrak{b}\big) = p^{ef}$, where p is the prime number lying below $\mathfrak{P}$ (i.e., such that $\mathfrak{P} \cap \mathbb{Z} = p\mathbb{Z}$) and $f = f(\mathfrak{P}|p)$ is the corresponding residue degree. On the other hand, $\mathbf{N}(\mathfrak{b}) = p^{ef}$ by definition. □

2.4.3 Discriminant and integral bases

In this subsection, we assume that L/K is a separable extension of degree n. The separability assumption ensures that B is a finitely generated A-module (Remark 2.4.2), and that if $\overline{K}$ denotes an algebraic closure of K, then the set of K-embeddings $\mathrm{Hom}_{K\text{-alg}}(L, \overline{K})$ of L into $\overline{K}$ has precisely n elements (cf. (1.2.3)).

(2.4.17) Let

$$f(t) = a_m t^m + a_{m-1}t^{m-1} + \cdots + a_1 t + a_0 \ \in K[t]$$

be a polynomial of degree $m \geq 1$ over K. Let $r_1, \ldots, r_m$ be the roots (counted with multiplicities) of f in an algebraic closure $\overline{K}$ of K. The ***discriminant*** $\mathrm{disc}(f)$ of f is defined as

$$\mathrm{disc}(f) := a_m^{2m-2} \prod_{1 \leq i < j \leq m} (r_i - r_j)^2 = (-1)^{\frac{m(m-1)}{2}} a_m^{2m-2} \prod_{1 \leq i \neq j \leq m} (r_i - r_j)\,.$$

Clearly, f is separable[§] (i.e. with no multiple roots in $\overline{K}$) if and only if $\mathrm{disc}(f) \neq 0$.

If f is monic, one has

$$\mathrm{disc}(f) = (-1)^{\frac{m(m-1)}{2}} \prod_{i=1}^{m} f'(r_i)$$

where f' denotes the derivative of f.

In low degrees we have the following formulas (assuming $a \neq 0$):

[§]According to our terminology, powers of irreducible polynomials are not separable. This differs from the convention used in [Mor96, p.39, Definition 4.1].

- $\mathrm{disc}(at+b) = 1$.
- $\mathrm{disc}(at^2+bt+c) = b^2 - 4ac$.
- $\mathrm{disc}(at^3+bt^2+ct+d) = b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd$.
  In particular, $\mathrm{disc}(t^3+ct+d) = -4c^3 - 27d^2$. ■

(2.4.18) Let $(\alpha_1, \ldots, \alpha_n)$ be an n-tuple of elements in L. The ***discriminant*** of the n-tuple is defined by

$$\mathrm{disc}_{L/K}(\alpha_1, \ldots, \alpha_n) := \det\big(\mathrm{Tr}_{L/K}(\alpha_i\alpha_j)\big)\,. \tag{2.4.18.1}$$

Note that if every α_i lies in B, then $\mathrm{disc}_{L/K}(\alpha_1, \cdots, \alpha_n) \in A$ by Prop. 2.1.11.

If $(\beta_1, \cdots, \beta_n)$ is another n-tuple with $(\beta_1, \cdots, \beta_n) = (\alpha_1, \cdots, \alpha_n)P$ for some matrix $P \in \mathrm{M}_n(K)$, we have

$$\mathrm{disc}_{L/K}(\beta_1, \cdots, \beta_n) = \det(P)^2 \mathrm{disc}_{L/K}(\alpha_1, \cdots, \alpha_n)\,. \tag{2.4.18.2}$$

since $(\mathrm{Tr}_{L/K}(\beta_i\beta_j)) = P^T\big(\mathrm{Tr}_{L/K}(\alpha_i\alpha_j)\big)P$. In particular,

$$\mathrm{disc}_{L/K}(\alpha_{\sigma(1)}, \cdots, \alpha_{\sigma(n)}) = \mathrm{disc}_{L/K}(\alpha_1, \cdots, \alpha_n) \tag{2.4.18.3}$$

for any permutation σ of $\{1, 2, \cdots, n\}$. ■

Theorem 2.4.19. *Let* $\{\sigma_1, \ldots, \sigma_n\} = \mathrm{Hom}_{K\text{-}alg}(L, \overline{K})$.

1. *For all* $\alpha_1, \ldots, \alpha_n \in L$, *we have*

$$\mathrm{disc}_{L/K}(\alpha_1, \ldots, \alpha_n) = (\det(\sigma_i\alpha_j))^2$$

   and $\mathrm{disc}_{L/K}(\alpha_1, \ldots, \alpha_n) \neq 0$ *if and only if* $\alpha_1, \cdots, \alpha_n$ *form a basis of* L *over* K.

2. *Suppose that* $L = K(\alpha)$ *and let* $f \in K[t]$ *be the monic minimal polynomial of* α *over* K. *Let* $\alpha_1, \ldots, \alpha_n$ *be the roots of* f *in* $\overline{K}$. *Then*

$$\begin{aligned}\mathrm{disc}_{L/K}(1, \alpha, \ldots, \alpha^{n-1}) &= \det(\alpha_i^{j-1})^2 = \mathrm{disc}(f) = \det(s_{i+j-2}) \\ &= (-1)^{n(n-1)/2} N_{L/K}(f'(\alpha))\,,\end{aligned}$$

   where $s_m = \alpha_1^m + \cdots + \alpha_n^m$.

Proof. The K-bilinear form

$$L \times L \longrightarrow K\,; \quad (x,\, y) \longmapsto \mathrm{Tr}_{L/K}(xy)$$

is nondegenerate by the separability of L/K. This implies that the Gram matrix $\big(\mathrm{Tr}_{L/K}(e_ie_j)\big)$, for every K-basis $e_1, \cdots, e_n$ of L, is nonsingular.

(1) When a K-basis $(e_1, \cdots, e_n)$ is fixed, we can find a matrix $P \in \mathrm{M}_n(K)$ such that $(\alpha_1, \cdots, \alpha_n) = (e_1, \cdots, e_n)P$. So by (2.4.18.2), $(\alpha_1, \cdots, \alpha_n)$ is a basis of L if and only if P is invertible, if and only if $\mathrm{disc}_{L/K}(\alpha_1, \cdots, \alpha_n) \neq 0$.

Combining Thm. 1.2.4 (2) and (2.4.18.1) we get

$$\mathrm{disc}_{L/K} = \det\left(\sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j)\right) = \det\left((\sigma_k(\alpha_i))^T \cdot (\sigma_k(\alpha_i))\right) = \det(\sigma_k\alpha_i)^2 .$$

(2) It is a standard fact that $\{\alpha_1, \cdots, \alpha_n\} = \{\sigma_1(\alpha), \cdots, \sigma_n(\alpha)\}$. In view of (2.4.18.3), we may assume without loss of generality that $\alpha_i = \sigma_i(\alpha)$ for each $i = 1, \cdots, n$. Then by (1) we have

$$\mathrm{disc}_{L/K}(1, \alpha, \cdots, \alpha^{n-1}) = \det(\sigma_i(\alpha^{j-1}))^2 = \det(\alpha_i^{j-1})^2 .$$

From the well known formula for the Vandermonde determinant, we see that

$$\det(\alpha_i^{j-1})^2 = \prod_{1\le i<j\le n} (\alpha_i - \alpha_j)^2 = \mathrm{disc}(f) .$$

Computing the matrix product $(\alpha_i^{j-1})^T(\alpha_i^{j-1})$ yields

$$(\alpha_i^{j-1})^T(\alpha_i^{j-1}) = (c_{ij}) \quad \text{with } c_{ij} = \sum_{k=1}^{n} \alpha_k^{i-1}\alpha_k^{j-1} = s_{i+j-2}$$

whence $\det(\alpha_i^{j-1})^2 = \det(s_{i+j-2})$.

Finally, using the factorization $f(t) = (t-\alpha_1)\cdots(t-\alpha_n)$ to compute $f'(\alpha_i)$ we get

$$f'(\alpha_i) = (\alpha_i - \alpha_1)\cdots(\alpha_i - \alpha_{i-1})(\alpha_i - \alpha_{i+1})\cdots(\alpha_i - \alpha_n) = \prod_{j=1,\, j\ne i}^{n} (\alpha_i - \alpha_j) .$$

Thus,

$$\begin{aligned} N_{L/K}(f'(\alpha)) &= \prod_{i=1}^{n} \sigma(f'(\alpha_1)) = \prod_{i=1}^{n} f'(\sigma\alpha_1) = \prod_{i=1}^{n} f'(\alpha_i) \\ &= \prod_{1\le i\ne j\le n} (\alpha_i - \alpha_j) = (-1)^{n(n-1)/2}\mathrm{disc}(f) . \end{aligned}$$

This completes the proof. □

(2.4.20) Let $J \subseteq L$ be an A-submodule which contains a K-basis of L. Its ***discriminant*** over A, denoted by $\mathfrak{d}_{J/A}$ or $\mathfrak{d}(J/A)$, is defined by

$$\mathfrak{d}_{J/A} := \text{the } A\text{-submodule generated by } \{\mathrm{disc}_{L/K}(\alpha_1, \ldots, \alpha_n) \,|\, \alpha_i \in J\} \subseteq K .$$

Note that by Thm. 2.4.19 (1), $\mathfrak{d}_{J/A} \ne 0$.

Now let I be a fractional ideal of B. Note that B contains a K-basis of L (since $L = KB$ by Cor. 2.1.8). Choosing a nonzero element $x \in I$ we get $xB \subseteq I$. So I also contains a K-basis of L. Therefore, the discriminant $\mathfrak{d}_{I/A}$ is defined. Note that I is a finitely generated B-module (Lemma 2.3.5), hence also a finitely generated A-module.

Since $L = KB$, we can find $a \in K^*$ such that $aI \subseteq B$. Then for all $\alpha_1, \cdots, \alpha_n \in I$, we have

$$a^{2n}\mathrm{disc}(\alpha_1, \cdots, \alpha_n) = \mathrm{disc}(a\alpha_1, \cdots, a\alpha_n) \in A\,.$$

This shows that $a^{2n}\mathfrak{d}_{I/A} \subseteq A$. Hence $\mathfrak{d}_{I/A}$ is a fractional ideal of A. When $I \subseteq B$, $\mathfrak{d}_{I/A}$ is an integral ideal in A.

In particular, $\mathfrak{d}_{B/A}$ is defined and it is an integral ideal of A. We call $\mathfrak{d}_{B/A}$ the ***discriminant*** (***ideal***) of B/A. When A is clear from the context, we also write $\mathfrak{d}_{L/K}$ instead of $\mathfrak{d}_{B/A}$ and call it the ***discriminant*** (***ideal***) of L/K. ■

Proposition 2.4.21. *Let $J \subseteq L$ be an A-submodule containing a K-basis of L and let S be a multiplicative subset of A. Then*

$$S^{-1}\mathfrak{d}(J/A) = \mathfrak{d}(S^{-1}J/S^{-1}A)\,.$$

Proof. Clear from definition. □

Lemma 2.4.22. *Let $J \subseteq L$ be an A-submodule containing a K-basis of L and suppose that J is generated by $e_1, \cdots, e_n$ as an A-module.*

Then $\mathfrak{d}(J/A)$ is the principal fractional ideal generated by $\mathrm{disc}(e_1, \cdots, e_n)$.

Proof. Immediate from (2.4.18.2). □

Proposition 2.4.23. *For every fractional ideal I of B we have*

$$\mathfrak{d}(I/A) = N_{L/K}(I)^2\mathfrak{d}_{B/A}\,.$$

Proof. Thanks to Prop. 2.4.21, by passing to localizations we may assume A is a DVR. Then B is a Dedekind domain with only finitely many prime ideals. Hence B is a PID (Exercise). So $I = xB$ is a principal ideal and $N_{L/K}(I) = N_{L/K}(x)A$ by Prop. 2.4.14. Also, by a standard fact about modules over a PID, we know that B admits a free basis $e_1, \ldots, e_n$ over A. Thus $xe_1, \ldots, xe_n$ is a free basis of I over A. Hence,

$$\mathfrak{d}(I/A) = \mathrm{disc}(xe_1, \ldots, xe_n)A = N_{L/K}(x)^2\mathrm{disc}(e_1, \ldots, e_n) = N_{L/K}(x)^2\mathfrak{d}_{B/A}\,,$$

by Lemma 2.4.22. □

Definition 2.4.24. An ***integral basis*** of L/K (***relative to*** A), if it exists, is a collection $\alpha_1, \cdots, \alpha_n$ of n elements $\alpha_i \in B$ such that the A-submodule in L generated by $\alpha_1, \cdots, \alpha_n$ is free and equal to B.

Note that if A is a PID, then L/K always has an integral basis relative to A. ■

Proposition 2.4.25. *Suppose that L/K has an integral basis (relative to A).*

Then a collection $\beta_1, \cdots, \beta_n$ of n elements in B is an integral basis of L/K (relative to A) if and only if $\mathfrak{d}_{B/A} = \mathrm{disc}_{L/K}(\beta_1, \cdots, \beta_n)A$.

Proof. Exercise. □

Definition 2.4.26. Let L be a number field of degree n (over $\mathbb{Q}$). It always has an integral basis relative to $\mathbb{Z}$. Such an integral basis is called an ***absolute integral basis***, or simply an ***integral basis***, of L.

The ***absolute discriminant***, or by abuse of terminology the ***discriminant***, of the number field L, is defined as the integer

$$d_L := \mathrm{disc}_{L/\mathbb{Q}}(\alpha_1, \cdots, \alpha_n)$$

where $\alpha_1, \cdots, \alpha_n$ is any absolute integral basis of L. Since an invertible matrix in $\mathrm{M}_n(\mathbb{Z})$ has determinant ± 1, from (2.4.18.2) we see that d_L is independent of the choice of the integral basis. The discriminant ideal $\mathfrak{d}_{L/\mathbb{Q}}$ is the ideal $d_L\mathbb{Z}$ in $\mathbb{Z}$, by Lemma 2.4.22.

By Prop. 2.4.25, a collection $\beta_1, \cdots, \beta_n$ with each $\alpha_i \in \mathcal{O}_L$ is an absolute integral basis if and only if $\mathrm{disc}_{L/\mathbb{Q}}(\beta_1, \cdots, \beta_n) = d_L$. ■

Example 2.4.27. Let $L = \mathbb{Q}(\sqrt{d})$ be a quadratic field, where $d \in \mathbb{Z} \setminus \{0, 1\}$ is a square-free integer.

If $d \equiv 2, 3 \pmod 4$, then an integral basis of L is $1, \sqrt{d}$ and $d_L = 4d$.

If $d \equiv 1 \pmod 4$, then an integral basis of L is $1, \frac{-1+\sqrt{d}}{2}$ and $d_L = d$. ■

Proposition 2.4.28. *Let L be a number field of degree n (over $\mathbb{Q}$) and let $\alpha_1, \cdots, \alpha_n \in \mathcal{O}_L$ with $\Delta := \mathrm{disc}_{L/\mathbb{Q}}(\alpha_1, \cdots, \alpha_n) \neq 0$.*

1. *If $\Delta \in \mathbb{Z}$ is square-free, then $\alpha_1, \cdots, \alpha_n$ is an integral basis of L.*
2. *We have $\Delta\mathcal{O}_L \subseteq \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$.*

Proof. (1) Use (2.4.18.2) to compare the system $\alpha_1, \cdots, \alpha_n$ with an integral basis.

(2) Let $\sigma_1, \cdots, \sigma_n$ be the embedding of L into $\overline{\mathbb{Q}}$. Since $\Delta \neq 0$, $\alpha_1, \cdots, \alpha_n$ form a $\mathbb{Q}$-basis of L (Thm. 2.4.19 (1)). For any $\alpha \in \mathcal{O}_L$, we can find $x_1, \cdots, x_n \in \mathbb{Q}$ such that $\alpha = x_1\alpha_1 + \cdots + x_n\alpha_n$. Then the column vector $(x_1, \cdots, x_n)^T$ is a solution to the linear system

$$(\sigma_i(\alpha_j)) \cdot X = \begin{pmatrix} \sigma_1(\alpha) \\ \vdots \\ \sigma_n(\alpha) \end{pmatrix}.$$

Apply Cramer's rule to express each x_i and then use Thm. 2.4.19 (1) to conclude. (The missing details are left to the reader.) □

Theorem 2.4.29. *Let M, L be number fields of degree m and n respectively. Let $d = \gcd(d_M, d_L)$. Let $F = ML$ be their composite field, and suppose that $[F : \mathbb{Q}] = mn$.*

1. *We have $\mathcal{O}_F \subseteq \frac{1}{d}\mathcal{O}_M\mathcal{O}_L$.*
2. *Suppose that $d = 1$. Let $\alpha_1, \cdots, \alpha_m$ be an integral basis of M and $\beta_1, \cdots, \beta_n$ an integral basis of L.*

   Then the mn elements $\alpha_i\beta_j$, $1 \leq i \leq m$, $1 \leq j \leq n$ form an integral basis of F and $d_F = d_M^n d_L^m$.

Proof. See e.g. [Mar18, p.24, Thm. 12] or [Neu99, p.13, Prop. I.2.11]. □

Definition 2.4.30. Let L be a number field of degree n and let $J \subseteq L$ be a $\mathbb{Z}$-submodule containing a $\mathbb{Q}$-basis of L. Then J is a free $\mathbb{Z}$-module of rank n. As in Definition 2.4.26, we can choose any $\mathbb{Z}$-basis $\alpha_1, \cdots, \alpha_n$ for J and define the (***absolute***) ***discriminant***

$$d(J) := \mathrm{disc}_{L/\mathbb{Q}}(\alpha_1, \cdots, \alpha_n) .$$

The discriminant ideal $\mathfrak{d}_{J/\mathbb{Z}}$ is the same as the ideal generated by $d(J)$ in $\mathbb{Z}$. ■

Proposition 2.4.31. *Let L be a number field and let J, J' be $\mathbb{Z}$-submodules of L each containing a $\mathbb{Q}$-basis of L. Suppose that $J \subseteq J'$.*

Then the quotient J'/J is finite and $d(J) = |J'/J|^2 d(J')$.

Proof. By the elementary factors theorem for modules over a PID (cf. [Lan02, p.153, Thm. III.7.8]), there exists a $\mathbb{Z}$-basis $\alpha_1, \cdots, \alpha_n$ of J' and positive integers $d_1, \cdots, d_n$ such that $J = \mathbb{Z}d_1\alpha_1 + \cdots + \mathbb{Z}d_n\alpha_n$. Thus $|J'/J| = d_1 \cdots d_n$ and $d(J) = d_1^2 \cdots d_n^2 d(J')$. □

2.4.4 Kummer–Dedekind theorem

As in the previous subsection, we assume L/K is a separable extension of degree n. (Recall that A is a Dedekind domain with fraction field K and that B denotes its integral closure in L.)

We fix an element $\alpha \in B$ such that $L = K(\alpha)$ and let $f(t) \in A[t]$ be the monic minimal polynomial of α over K. Note that the discriminant $\mathfrak{d}(A[\alpha]/A) \subseteq K$ is the principal fractional ideal generated by $\mathrm{disc}_{L/K}(1, \alpha, \cdots, \alpha^{n-1}) = \mathrm{disc}(f)$ by Lemma 2.4.22 (and Thm. 2.4.19 (2)). Since $A[\alpha] \subseteq B$, we have $\mathfrak{d}(A[\alpha]/A) \subseteq \mathfrak{d}(B/A)$, i.e., $\mathfrak{d}(B/A)$ divides $\mathfrak{d}(A[\alpha]/A) = \mathrm{disc}(f)A$ as fractional ideals of A.

Theorem 2.4.32 (Kummer–Dedekind)**.** *With notation as above, fix $\mathfrak{p} \in \mathrm{Spm}(A)$ and let $\bar{f} \in (A/\mathfrak{p})[t]$ be the reduction of f mod $\mathfrak{p}$. Let $\bar{f} = \bar{f}_1^{e_1} \cdots \bar{f}_r^{e_r}$ be the factorization of $\bar{f}$ into powers of monic irreducible factors in $(A/\mathfrak{p})[t]$. Let $f_i \in A[t]$ be a monic polynomial whose reduction mod $\mathfrak{p}$ is $\bar{f}_i$.*

Suppose that $\mathfrak{p}$ does not divide $\mathrm{disc}(f)\mathfrak{d}(B/A)^{-1} = \mathfrak{d}(A[\alpha]/A)\mathfrak{d}(B/A)^{-1}$ (e.g. $B = A[\alpha]$).

Then[¶] *$B_\mathfrak{p} = A_\mathfrak{p}[\alpha]$ and the prime factorization of the ideal $\mathfrak{p}B$ takes the following form*

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r} \quad \text{where} \quad \mathfrak{P}_i = \mathfrak{p}B + f_i(\alpha)B$$

and $f(\mathfrak{P}_i|\mathfrak{p}) = \deg(f_i)$ for each $i \in [\![1, r]\!]$.

Proof. Since $\mathfrak{p} \nmid \mathfrak{d}(A[\alpha]/A)\mathfrak{d}(B/A)^{-1}$, we have

$$\mathfrak{d}(A_\mathfrak{p}[\alpha]/A_\mathfrak{p}) = \mathfrak{d}(A[\alpha]/A)A_\mathfrak{p} = \mathfrak{d}(B/A)A_\mathfrak{p} = \mathfrak{d}(B_\mathfrak{p}/A_\mathfrak{p})$$

by Prop. 2.4.21. Applying Prop. 2.4.25 we see that $1, \alpha, \cdots, \alpha^{n-1}$ is an integral basis of $B_\mathfrak{p}$ over $A_\mathfrak{p}$, i.e., $B_\mathfrak{p} = A_\mathfrak{p}[\alpha]$. This proves the first assertion.

[¶]In this theorem, the separability of L/K is only used to define the discriminants. If we assume $B_\mathfrak{p} = A_\mathfrak{p}[\alpha]$, then the other assertions of the theorem remain valid, as the proof works verbatim.

To prove the factorization of $\mathfrak{p}B$, we may assume $B = A[\alpha]$ by localization at $\mathfrak{p}$. Put $\overline{B} = B/\mathfrak{p}B$ and $\kappa = A/\mathfrak{p}$. By assumption $B = A[\alpha] \cong A[t]/(f)$. Thus

$$\overline{B} = B \otimes_A (A/\mathfrak{p}) = A[t]/(f) \otimes_A \kappa \cong \kappa[t]/(\bar{f}) \cong \prod_{i=1}^{r} \kappa[t]/(\bar{f}_i^{e_i}) \,.$$

by the Chinese remainder theorem. Prime ideals of B lying over $\mathfrak{p}$ correspond bijectively to prime ideals of the quotient $\overline{B} = B/\mathfrak{p}B$, and hence to the prime ideals of the product $\prod_{i=1}^{r} \kappa[t]/(\bar{f}_i^{e_i})$. The explicit expression of the isomorphism $\overline{B} \xrightarrow{\sim} \prod_{i=1}^{r} \kappa[t]/(\bar{f}_i^{e_i})$ is given by $\alpha + \mathfrak{p}B \mapsto (t + \bar{f}_i(t)^{e_i})$. So the only prime ideals $\overline{B}$ are $\overline{\mathfrak{P}}_i := \mathfrak{P}_i \pmod{\mathfrak{p}B}$, where $\mathfrak{P}_i = \mathfrak{p}B + f_i(\alpha)B$ as in the theorem, and their residue fields are $\overline{B}/\overline{\mathfrak{P}_i} \cong \kappa[t]/(\bar{f}_i)$. Therefore, in the prime factorization of $\mathfrak{p}B$ the only prime factors are $\mathfrak{P}_1, \cdots, \mathfrak{P}_r$, and $f(\mathfrak{P}_i|\mathfrak{p}) = \deg(f_i)$.

In $\overline{B}$ we have

$$0 = \overline{\mathfrak{P}}_1^{e_1} \cdots \overline{\mathfrak{P}}_r^{e_r} = \overline{\mathfrak{P}}_1^{e_1} \cdots \overline{\mathfrak{P}}_r^{e_r}$$

since the analogous statement holds in the product $\prod_{i=1}^{r} \kappa[t]/(\bar{f}_i^{e_i})$. Similarly,

$$\overline{\mathfrak{P}}_1^{e_1-1}\overline{\mathfrak{P}}_2^{e_2} \cdots \overline{\mathfrak{P}}_r^{e_r} \,,\ \overline{\mathfrak{P}}_1^{e_1}\overline{\mathfrak{P}}_2^{e_2-1} \cdots \overline{\mathfrak{P}}_r^{e_r} \,, \cdots \,,\ \overline{\mathfrak{P}}_1^{e_1}\overline{\mathfrak{P}}_2^{e_2} \cdots \overline{\mathfrak{P}}_r^{e_r-1}$$

are nonzero ideals in $\overline{B}$. This shows that $\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r} \subseteq \mathfrak{p}B$ but[‖].

$$\mathfrak{P}_1^{e_1-1}\mathfrak{P}_2^{e_2} \cdots \mathfrak{P}_r^{e_r} \not\subseteq \mathfrak{p}B \,, \cdots \,,\ \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2} \cdots \mathfrak{P}_r^{e_r-1} \not\subseteq \mathfrak{p}B \,.$$

Therefore we have $\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ in B. □

(2.4.33) The assumption $\mathfrak{p} \nmid \operatorname{disc}(f)\mathfrak{d}_{B/A}^{-1}$ in Thm. 2.4.32 holds in each of the following cases:

1. The mod $\mathfrak{p}$ reduction $\bar{f} \in \kappa(\mathfrak{p})[t]$ (where $\kappa(\mathfrak{p}) = A/\mathfrak{p}$) is separable.

   In fact, $\bar{f} \in \kappa(\mathfrak{p})[t]$ is separable if and only if $\mathfrak{p} \nmid \operatorname{disc}(f)A$ because $\operatorname{disc}(f) \pmod{\mathfrak{p}}$ is the same as the discriminant of $\bar{f}$. When this condition holds, we have clearly $\mathfrak{p} \nmid \operatorname{disc}(f)\mathfrak{d}_{B/A}^{-1}$. So Thm. 2.4.32 applies in this case, and it follows that $\mathfrak{p}$ is unramified in L. (The residue field $\kappa(\mathfrak{P}_i)$ is isomorphic to $\kappa(\mathfrak{p})[t]/(\bar{f}_i)$ for some factor $\bar{f}_i$ of $\bar{f}$, where $\bar{f}_i$ is separable as $\bar{f}$ is.) This also shows that for a given extension L/K, only finitely many $\mathfrak{p} \in \operatorname{Spm}(A)$ ramifies in L.

   For example, if L is a number field with absolute discriminant d_L and p is a prime number coprime to d_L, then p is unramified in $L/\mathbb{Q}$ and the factorization of $p\mathcal{O}_L$ can be determined by using the Kummer–Dedekind theorem.

2. L is a number field, $A = \mathbb{Z}$ and $\mathfrak{p} = p\mathbb{Z}$ with $p \nmid [\mathcal{O}_L : \mathbb{Z}[\alpha]]$.

   In this case, we have $\operatorname{disc}(f)d_L^{-1} = [\mathcal{O}_L : \mathbb{Z}[\alpha]]^2$ by Prop. 2.4.31. ■

[‖]Thanks to ZHAO Hongxiang (赵泓翔) for pointing out a gap in my proof in an earlier version of the notes.

Example 2.4.34. Let $L = \mathbb{Q}(\sqrt{d})$ be a quadratic field, where $d \in \mathbb{Z} \setminus \{0, 1\}$ is square-free. We know (from Example 2.4.27) that $\mathcal{O}_L = \mathbb{Z} \oplus \mathbb{Z}\alpha = \mathbb{Z}[\alpha]$ with

$$\alpha = \begin{cases} \frac{-1+\sqrt{d}}{2} & \text{if } d \equiv 1 \pmod 4, \\ \sqrt{d} & \text{if } d \equiv 2,\, 3 \pmod 4. \end{cases}$$

Using the Kummer–Dedekind theorem, one can determine explicitly the factorization of $p\mathcal{O}_L$ for every prime number p.

Explicitly, for any odd prime number p, letting $\left(\frac{\cdot}{p}\right)$ denote the Legendre symbol, we have:

1. If $\left(\frac{d}{p}\right) = 0$ (i.e., $p \mid d$), then p is (totally) ramified in L, in fact $p\mathcal{O}_L = \mathfrak{p}^2$ with $\mathfrak{p} = p\mathcal{O}_L + \sqrt{d}\mathcal{O}_L$.
2. If $\left(\frac{d}{p}\right) = 1$, then p is totally split (and unramified) in L. In fact, if $a \in \mathbb{Z}$ is chosen such that $d \equiv a^2 \pmod p$ and σ denotes the nontrivial element in the Galois group $\mathrm{Gal}(L/\mathbb{Q})$, we have $p\mathcal{O}_L = \mathfrak{p}.\sigma\mathfrak{p}$, where $\mathfrak{p} = p\mathcal{O}_L + (a + \sqrt{d})\mathcal{O}_L$ (and $\sigma\mathfrak{p} = p\mathcal{O}_L + (a - \sqrt{d})\mathcal{O}_L \neq \mathfrak{p}$).
3. If $\left(\frac{d}{p}\right) = -1$, then p is inert (and unramified) in L, i.e., $p\mathcal{O}_L$ itself is a prime ideal.

As for the prime factorization of $2\mathcal{O}_L$ we have:

1. If $d \equiv 2,\, 3 \pmod 4$, then 2 is (totally) ramified in L; in fact $2\mathcal{O}_L = \mathfrak{p}^2$ with

$$\mathfrak{p} = \begin{cases} 2\mathcal{O}_L + \sqrt{d}\mathcal{O}_L & \text{if } d \equiv 2 \pmod 4, \\ 2\mathcal{O}_L + (\sqrt{d} - 1)\mathcal{O}_L & \text{if } d \equiv 3 \pmod 4. \end{cases}$$

2. If $d \equiv 1 \pmod 8$, then 2 is totally split (and unramified) in L. In fact, $p\mathcal{O}_L = \mathfrak{p}.\sigma\mathfrak{p}$, where $\mathfrak{p} = 2\mathcal{O}_L + \frac{1+\sqrt{d}}{2}\mathcal{O}_L$ (and $\sigma\mathfrak{p} = 2\mathcal{O}_L + \frac{1-\sqrt{d}}{2}\mathcal{O}_L \neq \mathfrak{p}$).
3. If $d \equiv 5 \pmod 8$, then 2 is inert (and unramified) in L, i.e., $2\mathcal{O}_L$ itself is a prime ideal.

Recall that the discriminant d_L is given by

$$d_L = \begin{cases} d & \text{if } d \equiv 1 \pmod 4, \\ 4d & \text{if } d \equiv 2,\, 3 \pmod 4. \end{cases}$$

In any case we can easily check that a prime number p (with p odd or not) is ramified in L if and only if $p \mid d_L$. ■

Example 2.4.35. Let $\omega \in \mathbb{C}$ be a root of the polynomial $f(t) = t^3 + t + 1$ and let $L = \mathbb{Q}(\omega)$. We have $\mathrm{disc}_{L/\mathbb{Q}}(1, \omega, \omega^2) = \mathrm{disc}(f) = -31$ by Prop. 2.4.28 (1). This discriminant being square-free, we have $\mathcal{O}_L = \mathbb{Z}[\omega]$. So we can apply the Kummer–Dedekind theorem to determine the factorization of $p\mathcal{O}_L$ for every prime number p.

For example, for $p = 31$, the reduction $\bar{f} \in \mathbb{F}_p[t]$ can be factorized as $\bar{f} = (t-3)(t-14)^2$. Thus, $31\mathcal{O}_L = \mathfrak{p}_1\mathfrak{p}_2^2$ where

$$\mathfrak{p}_1 = 31\mathcal{O}_L + (\omega - 3)\mathcal{O}_L \quad \text{and} \quad \mathfrak{p}_2 = 31\mathcal{O}_L + (\omega - 14)\mathcal{O}_L\,.$$

Here $L/\mathbb{Q}$ is unramified at $\mathfrak{p}_1$ but ramified at $\mathfrak{p}_2$. According to Definition 2.4.5, 31 is ramified in $L/\mathbb{Q}$.

For $p \neq 31$, $\bar{f} \in \mathbb{F}_p[t]$ is separable since $\operatorname{disc}(\bar{f}) = \overline{\operatorname{disc}(f)} = -\overline{31} \neq 0 \in \mathbb{F}_p$. So by (2.4.33), such a prime p is unramified in L. Here are some examples of the different ramification behaviors of p.

For $p = 2$, $\bar{f}$ is irreducible in $\mathbb{F}_p[t]$. Hence $2\mathcal{O}_L$ is itself a maximal ideal, i.e., 2 is inert in L.

For $p = 3$, $\bar{f} = (t-1)(t^2+t-1)$ with t^2+t+1 irreducible. Hence $3\mathcal{O}_L = \mathfrak{p}_1\mathfrak{p}_2$ with

$$\mathfrak{p}_1 = 3\mathcal{O}_L + (\omega - 1)\mathcal{O}_L \quad \text{and} \quad \mathfrak{p}_2 = 3\mathcal{O}_L + (\omega^2 + \omega - 1)\mathcal{O}_L\,.$$

Note that $f(\mathfrak{p}_1|3) = 1 \neq 2 = f(\mathfrak{p}_2|3)$.

For $p = 131$, we have $\bar{f} = (t-5)(t-51)(t-75)$. Thus $131\mathcal{O}_L = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ with

$$\mathfrak{p}_1 = 131\mathcal{O}_L + (\omega - 5)\mathcal{O}_L\,,\ \mathfrak{p}_2 = 131\mathcal{O}_L + (\omega - 51)\mathcal{O}_L \ \text{ and } \ \mathfrak{p}_3 = 131\mathcal{O}_L + (\omega - 75)\mathcal{O}_L\,.$$

This is a prime which splits completely in L. ■

2.5 Cyclotomic fields

In this section, let K be a field with a fixed algebraic closure $\overline{K}$ and let n be a positive integer.

2.5.1 Cyclotomic extensions and cyclotomic polynomials

(2.5.1) Let L be an extension field of K. We denote by

$$\mu_n(L) := \{x \in L \,|\, x^n = 1\}$$

the set of n-th roots of unity in L. Clearly, $\mu_n(L)$ is a subgroup of L^*, $|\mu_n(L)| \leq n$ and every element of $\mu_n(L)$ has order dividing n. It is a well known fact that in the multiplicative group of nonzero elements of a field, any finite subgroup is cyclic. So in particular, $\mu_n(L)$ is always a cyclic group of order dividing n.

If ξ is an n-th root of unity, then for any $a \in \mathbb{Z}$ the element ξ^a depends only on the residue class of a modulo n. So the element ξ^α is well defined for any $\alpha \in \mathbb{Z}/n\mathbb{Z}$.

When $L = K(\xi)$ for some root of unity ξ, we say that L/K is a ***cyclotomic extension***. For such an extension, any K-embedding σ of L into any extension of K is uniquely determined by its effect on ξ. If ξ is an n-th root of unity, then so is $\sigma(\xi)$.

Let $\mu_n'(L)$ denote the set of primitive n-th roots of unity in L, i.e.,

$$\mu_n'(L) = \mu_n(L) \setminus \left(\bigcup_{m=1}^{n-1} \mu_m(L) \right) = \mu_n(L) \setminus \left(\bigcup_{\substack{1 \leq m \leq n-1 \\ m \,|\, n}} \mu_m(L) \right).$$

Suppose that $\mathrm{char}(K) \nmid n$. Then the polynomial $f = t^n - 1$ is separable over K. Thus, if L contains a splitting field of f (e.g. $L = \overline{K}$), then $\mu_n(L)$ is a cyclic group of order n; in other words, L contains a primitive n-th root of unity.

On the other hand, if the field K has positive characteristic p and $p \,|\, n$, say $n = p^s m$ with s, $m \in \mathbb{N}$ and $1 < m < n$, then $\xi^n = 1$ holds if and only if $\xi^m = 1$ holds. Therefore, in this case being an n-th root of unity is the same as being an m-th root of unity, and hence there cannot exist any primitive n-th root of unity in any extension field of K. For this reason, *whenever talking about n-th roots of unity, we may and we shall assume that n is not divisible by the characteristic* $\mathrm{char}(K)$ *of the base field K.*

Recall that Euler's phi function $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ is defined by

$$\varphi(m) = \#\{a \in [\![1,\, m]\!] \mid \gcd(a,\, m) = 1\}\,.$$

When $\mathrm{char}(K) \nmid n$, we have $|\mu_n'(\overline{K})| = \varphi(n)$, i.e., the number of primitive n-th roots of unity in $\overline{K}$ is equal to $\varphi(n)$. ■

Definition 2.5.2. Suppose $\mathrm{char}(K) \nmid n$. The n-th ***cyclotomic polynomial*** over K, denoted $\Phi_{n,\,K}$, is defined by

$$\Phi_{n,\,K}(t) := \prod_{\xi \in \mu_n'(\overline{K})} (t - \xi)\,.$$

This is a monic polynomial of degree $\varphi(n)$.

We will write Φ_n instead of $\Phi_{n,\,\mathbb{Q}}$. ■

Example 2.5.3. Suppose $\mathrm{char}(K) \nmid n$. It is clear that as d runs over positive divisors of n, the subsets $\mu_d'(\overline{K})$ form a partition of $\mu_n(\overline{K})$. So we have

$$t^n - 1 = \prod_{d \,|\, n} \Phi_{d,\,K}(t)\,.$$

This formula can help us to determine the cyclotomic polynomials by recursion.

For example, when $K = \mathbb{Q}$, the first few cyclotomic polynomials are given by

$$\begin{aligned}
&\Phi_1(t) = t - 1\,,\ \Phi_2(t) = t + 1\,,\ \Phi_3(t) = t^2 + t + 1\,,\ \Phi_4(t) = t^2 + 1\,,\\
&\Phi_5(t) = t^4 + t^3 + t^2 + t + 1\,,\ \Phi_6(t) = t^2 - t + 1\,,\\
&\Phi_7(t) = t^6 + t^5 + t^4 + t^3 + t^2 + t + 1\,,\\
&\Phi_8(t) = t^4 + 1\,,\ \Phi_9(t) = t^6 + t^3 + 1\,.
\end{aligned}$$

The coefficients of the above cyclotomic polynomials are all 0 or ± 1. But this is not true for general Φ_n. The first cyclotomic polynomial over $\mathbb{Q}$ that has a coefficient other than 0 or ± 1 is Φ_{105}. In fact,

$$\begin{aligned}
\Phi_{105}(t) = {} & t^{48} + t^{47} + t^{46} - t^{43} - t^{42} - 2t^{41} - t^{40} - t^{39} + t^{36} + t^{35} + t^{34} + t^{33} + t^{32} + t^{31}\\
& - t^{28} - t^{26} - t^{24} - t^{22} - t^{20} + t^{17} + t^{16} + t^{15} + t^{14} + t^{13} + t^{12}\\
& - t^9 - t^8 - 2t^7 - t^6 - t^5 + t^2 + t + 1\,.
\end{aligned}$$

(The coefficients of t^{41} and t^7 are both -2.) ■

In the next theorem, we collect some most important facts on cyclotomic extensions and cyclotomic polynomials.

Theorem 2.5.4 ([Hun80, § V.8]). *Let $\xi_n \in \overline{K}$ be a primitive n-th root of unity and $L = K(\xi_n)$.*

1. *The field L is a splitting field of the polynomial $t^n - 1$ over K. In particular, L/K is a Galois extension. We call L the n-th* **cyclotomic field** *over K.*

2. *For every $\sigma \in \mathrm{Gal}(L/K)$, there is a unique $\alpha \in (\mathbb{Z}/n\mathbb{Z})^*$ such that $\sigma(\xi) = \xi^\alpha$. The rule*
$$\mathrm{Gal}(L/K) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^* ; \quad \sigma \longmapsto \alpha$$
defines an injective group homomorphism. In particular, L/K is an abelian extension with $[L : K] \mid \varphi(n)$.

3. *Let F be the prime field of K, i.e., $F = \mathbb{Q}$ if $\mathrm{char}(K) = 0$ or $F = \mathbb{F}_p$ if $\mathrm{char}(K) = p > 0$. The coefficients of the cyclotomic polynomial $\Phi_{n,K}$ lie in F, and $\Phi_{n,K} = \Phi_{n,F}$.*

4. *In the case $K = \mathbb{Q}$, the polynomial $\Phi_n = \Phi_{n,K}$ has all its coefficients in $\mathbb{Z}$ and Φ_n is irreducible over $\mathbb{Q}$. Hence $[\mathbb{Q}(\xi_n) : \mathbb{Q}] = \varphi(n)$ and $\mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$.*

Example 2.5.5. Let p be a prime number and $K = \mathbb{F}_p$. Suppose n is coprime to p and f be the order of p mod n, i.e., $f = \min\{r \in \mathbb{N}^* \mid p^r \equiv 1 \pmod{n}\}$. Then the n-th cyclotomic extension $\mathbb{F}_p(\xi_n)/\mathbb{F}_p$ has degree f (Exercise). ■

Another useful facts about roots of unity is the following:

Proposition 2.5.6. *Let A be an integrally closed domain with fraction field K, $\mathfrak{p} \in \mathrm{Spm}(A)$ and $\kappa = A/\mathfrak{p}$.*

1. *We have $\mu_n(K) \subseteq A$ and the canonical map $A \to \kappa$ induces a well defined group homomorphism*
$$\pi : \mu_n(K) \longrightarrow \mu_n(\kappa) ; \quad \omega \longmapsto \overline{\omega}.$$

2. *Suppose $\mathrm{char}(\kappa) \nmid n$. Then the map π is injective. It is bijective if K contains a primitive n-th of unity, in which case π maps primitive n-th roots of unity to primitive n-th roots of unity.*

3. *Suppose $\mathrm{char}(\kappa) = p > 0$ and n is a power of p. Then π is the trivial homomorphism.*

Proof. (1) Clearly, roots of unity in K are integral over A. Since A is integrally closed, we get $\mu_n(K) \subseteq A$. It is then clear that the map π is a well defined group homomorphism.

(2) The second assertion follows from the first one. To prove the first assertion, replacing K by a cyclotomic extension containing $\mu_n(\overline{K})$ (and A by its integral closure in that extension), we may assume that $\mu_n(\overline{K}) \subseteq K$. Consider the polynomial $f(t) := t^n - 1$ and its canonical image $\bar{f} \in \kappa[t]$. We have $f = \prod_{\omega \in \mu_n(K)}(t - \omega)$ in $A[t]$. So $\bar{f} = \prod_{\omega \in \mu_n(K)}(t - \overline{\omega})$. By the assumption $\mathrm{char}(\kappa) \nmid n$, the polynomial $\bar{f}$ is separable over κ. So $\bar{f}$ has no multiple roots. Therefore, the elements $\overline{\omega}$ for $\omega \in \mu_n(K)$ are all distinct.

(3) In fact $\mu_n(\kappa) = 1$. □

2.5.2 Prime factorization in cyclotomic number fields

In this subsection, we study cyclotomic fields over $\mathbb{Q}$. For each $m \in \mathbb{N}^*$, let $\xi_m \in \overline{\mathbb{Q}}$ denote a primitive m-th root of unity. Note that if m is odd and $n = 2m$, then $\mathbb{Q}(\xi_n) = \mathbb{Q}(\xi_m)$ (Exercise). So we may assume $n \not\equiv 2 \pmod 4$ (i.e. n is either odd or divisible by 4) when studying $\mathbb{Q}(\xi_n)$.

Lemma 2.5.7. *Suppose $n = p^s \geq 3$ where p is a prime number and $s \in \mathbb{N}^*$. Let ξ be a primitive n-th root of unity in $\overline{\mathbb{Q}}$, $L = \mathbb{Q}(\xi)$ and $r = [L : \mathbb{Q}] = \varphi(n) = p^{s-1}(p-1)$.*

1. *Putting $\eta := 1 - \xi$ we have $N_{L/\mathbb{Q}}(\eta) = p$.*
2. *$\mathcal{O}_L = \mathbb{Z}[\xi]$ and*

$$d_L = (-1)^{\frac{r}{2}} p^{sr - p^{s-1}} = (-1)^{\frac{r}{2}} p^{p^{s-1}(sp-s-1)} = (-1)^{\frac{\varphi(n)}{2}} n^{\varphi(n)} \big/ p^{\frac{\varphi(n)}{p-1}} .$$

Proof. (1) Note that the minimal polynomial of ξ over $\mathbb{Q}$ is

$$\Phi(t) := \Phi_n(t) = (t^{p^{s-1}})^{p-1} + (t^{p^{s-1}})^{p-2} + \cdots + t^{p^{s-1}} + 1$$

So the minimal polynomial of $-\eta = \xi - 1$ over $\mathbb{Q}$ is $f(t) := \Phi(t+1)$. Therefore, $N_{L/\mathbb{Q}}(\eta) = (-1)^r N_{L/\mathbb{Q}}(\xi - 1) = (-1)^r (-1)^r f(0) = \Phi(1) = p$.

(2) Let us first compute the discriminant $\Delta := d(\mathbb{Z}[\xi]) = \mathrm{disc}_{L/\mathbb{Q}}(1, \xi, \cdots, \xi^{r-1})$. By Thm. 2.4.19 (2),

$$\Delta = (-1)^{\frac{\det \Phi(\det \Phi - 1)}{2}} N_{L/\mathbb{Q}}(\Phi'(\xi)) = (-1)^{\frac{r(r-1)}{2}} N_{L/\mathbb{Q}}(\Phi'(\xi)) .$$

From the equality $(t^{p^{s-1}} - 1)\Phi(t) = t^{p^s} - 1$ we find $\Phi'(\xi) = p^s \xi^{p^s - 1}/(\omega - 1) = \frac{p^s}{\xi(\omega - 1)}$ where $\omega = \xi^{p^{s-1}}$. Note that $N_{L/\mathbb{Q}}(\xi) = (-1)^{\deg \Phi} \cdot \Phi(0) = 1$. So it remains to compute $N_{L/\mathbb{Q}}(\omega - 1)$. The minimal polynomial of $\omega - 1$ over $\mathbb{Q}$ is

$$g(t) = \Phi_p(t+1) = (t+1)^{p-1} + (t+1)^{p-2} + \cdots + (t+1) + 1 = t^{p-1} + \cdots + p .$$

Therefore,

$$N_{L/\mathbb{Q}}(\omega - 1) = N_{\mathbb{Q}(\omega)/\mathbb{Q}}(\omega - 1)^{[L:\mathbb{Q}(\omega)]} = ((-1)^{p-1} p)^{\frac{r}{p-1}} = (-1)^r p^{p^{s-1}} = p^{p^{s-1}} .$$

So we obtain

$$\Delta = (-1)^{\frac{r(r-1)}{2}} N_{L/\mathbb{Q}}(\Phi'(\xi)) = (-1)^{\frac{r(r-1)}{2}} \frac{N_{L/\mathbb{Q}}(p^s)}{N_{L/\mathbb{Q}}(\xi) N_{L/\mathbb{Q}}(\omega - 1)} = (-1)^{\frac{r}{2}} p^{sr - p^{s-1}} .$$

To prove $\mathcal{O}_L = \mathbb{Z}[\xi]$, note that the inclusion $\mathbb{Z}[\xi] \subseteq \mathcal{O}_L$ is obvious. To show the converse inclusion, it will be more convenient to use the $\mathbb{Z}$-basis $1, \eta, \cdots, \eta^{r-1}$ of $\mathbb{Z}[\xi] = \mathbb{Z}[\eta]$. Let $\alpha \in \mathcal{O}_L$. Since $\mathcal{O}_L \subseteq \frac{1}{\Delta}\mathbb{Z}[\xi]$ by Prop. 2.4.28, we can write

$$\alpha = \frac{a_0 + a_1\eta + \cdots + a_{r-1}\eta^{r-1}}{p^l} \quad \text{where each } a_i \in \mathbb{Z} \text{ and } p^l = |\Delta| .$$

If $\alpha \notin \mathbb{Z}[\eta]$, then not all of the a_i are divisible by p^l, that is,

$$m := \min\{v_p(a_0), \cdots, v_p(a_{r-1})\} < l\,.$$

Choose $0 \le i \le r-1$ such that $m < v_p(a_j)$ for all $0 \le j < i$ and $m = v_p(a_i)$. Then the element

$$\beta := p^{l-m-1}\alpha - \frac{a_0 + \cdots + a_{i-1}\eta^{i-1}}{p^{m+1}} = \frac{a_i\eta^i + \cdots + a_{r-1}\eta^{r-1}}{p^{m+1}}$$

belongs to $\mathcal{O}_L$ and

$$\beta = \frac{b_i\eta^i + \cdots + b_{r-1}\eta^r}{p} \text{ with each } b_j = a_j/p^m \in \mathbb{Z} \text{ and } p \nmid b_i\,.$$

In (1) we have seen that $p = N_{L/\mathbb{Q}}(\eta) = N_{L/\mathbb{Q}}(1-\xi) = \prod_{k\in(\mathbb{Z}/n)^*}(1-\xi^k)$. Clearly, $\eta = 1-\xi$ divides $1-\xi^k$ in $\mathbb{Z}[\xi] = \mathbb{Z}[\eta]$ for each $k \in \mathbb{N}^*$. Since $i+1 \le r$, η^{i+1} divides $\prod_{k\in(\mathbb{Z}/n)^*}(1-\xi^k) = p$ in $\mathbb{Z}[\eta]$. Thus,

$$b_i\eta^{-1} = \frac{p\beta}{\eta^{i+1}} = b_{i+1} + \cdots + b_{r-1}\eta^{r-i-1} \in \mathbb{Z}[\eta] \subseteq \mathcal{O}_L\,.$$

This implies that $N_{L/\mathbb{Q}}(\eta) \,|\, N_{L/\mathbb{Q}}(b_i)$ in $\mathbb{Z}$. But $N_{L/\mathbb{Q}}(\eta) = p$ and $N_{L/\mathbb{Q}}(b_i) = b_i^r$. This leads to a contradiction because $p \nmid b_i$. The lemma is thus proved. □

Now we consider general cyclotomic fields.

Proposition 2.5.8. *Suppose $n \not\equiv 2 \pmod 4$ and let $L = \mathbb{Q}(\xi_n)$.*

Then $\mathcal{O}_L = \mathbb{Z}[\xi_n]$ (hence $1, \xi_n, \cdots, \xi_n^{\varphi(n)-1}$ form an integral basis of $L/\mathbb{Q}$), and

$$d_L = (-1)^{\frac{\varphi(n)}{2}} n^{\varphi(n)} \Big/ \prod_{p\,|\,n} p^{\frac{\varphi(n)}{p-1}}\,,$$

where in the product p runs through prime factors of n.

Proof. The reader checks easily the following fact: For any two positive integers m, r, we have $\mathbb{Q}(\xi_m)\mathbb{Q}(\xi_r) = \mathbb{Q}(\xi_l)$ and $\mathbb{Z}[\xi_m]\mathbb{Z}[\xi_r] = \mathbb{Z}[\xi_l]$, where l is the least common multiple of m and r. Thus, applying Thm. 2.4.29 and Lemma 2.5.7 yields the desired results. □

Theorem 2.5.9. *Suppose $n \not\equiv 2 \pmod 4$ and let $L = \mathbb{Q}(\xi_n)$. For each prime number p, let $a_p = v_p(n)$, so that $n = \prod_p p^{a_p}$. Put $m_p := n/p^{a_p}$ and let f_p be the order of p mod m_p, i.e.,*

$$f_p = \min\{r \in \mathbb{N}^* \,|\, p^r \equiv 1 \pmod{m_p}\}\,.$$

1. *We have the factorization*

$$p\mathcal{O}_L = (\mathfrak{P}_1 \cdots \mathfrak{P}_r)^{\varphi(p^{a_p})}$$

where $\mathfrak{P}_1, \cdots, \mathfrak{P}_r$ are distinct maximal ideals of $\mathcal{O}_L$ lying over p with residue degree $f(\mathfrak{P}_i|p) = f_p$.

2. *A prime number p is unramified in $L = \mathbb{Q}(\xi_n)$ (when $n \not\equiv 2 \pmod 4$) if and and only if $p \mid n$.*

3. *A prime number p splits completely $L = \mathbb{Q}(\xi_n)$ (when $n \not\equiv 2 \pmod 4$) if and and only if $p \equiv 1 \pmod n$.*

Proof. Fix a prime number p and write $a = a_p$, $m = m_p$ for simplicity. Under the assumption $n \not\equiv 2 \pmod 4$, we have

$$\varphi(p^a) = 1 \iff a = 0 \iff p \nmid n \,.$$

So (2) follows from (1). The prime p splits completely in L if and only if for every $\mathfrak{P} \in \mathrm{Spm}(\mathcal{O}_L)$ lying over p, the ramification index $e(\mathfrak{P}|p)$ and the residue degree $f(\mathfrak{P}|p)$ are both equal to 1. Hence (3) is also a consequence of (1).

We have seen that $\mathcal{O}_L = \mathbb{Z}[\xi_n]$ (Prop. 2.5.8). To prove (1), we may apply the Kummer–Dedekind theorem to the minimal polynomial $\Phi = \Phi_n$ of ξ_n. Let $\phi \in \mathbb{F}_p[t]$ be the reduction of Φ mod p. All we need to show is that the factorization of ϕ in $\mathbb{F}_p[t]$ has the form

$$\phi = (h_1 \cdots h_r)^{\varphi(p^a)} \quad \text{with each } h_i \in \mathbb{F}_p[t] \text{ monic, irreducible and } \deg(h_i) = f_p \,.$$

Similar to the bijection $(\mathbb{Z}/n)^* \xrightarrow{\sim} (\mathbb{Z}/m)^* \times (\mathbb{Z}/p^a)^*$, we have the bijection

$$\mu'_m(\overline{\mathbb{Q}}) \times \mu'_{p^a}(\overline{\mathbb{Q}}) \xrightarrow{\sim} \mu'_n(\overline{\mathbb{Q}}) \,; \quad (\omega,\, \eta) \longmapsto \omega\eta \,.$$

Hence, using Prop. 2.5.6 we get

$$\phi(t) = \overline{\Phi(t)} = \prod_{\omega \in \mu'_m(\overline{\mathbb{Q}})} \prod_{\eta \in \mu'_{p^a}(\overline{\mathbb{Q}})} (t - \overline{\omega\eta}) = \Big(\prod_{\omega \in \mu'_m(\overline{\mathbb{Q}})} (t - \overline{\omega}) \Big)^{\varphi(p^a)} = \overline{\Phi_m(t)}^{\varphi(p^a)} \,.$$

We may thus reduce to the case $p \nmid n$.

As a factor of $t^n - 1$, the polynomial $\phi \in \mathbb{F}_p[t]$ has no multiple roots. So its factorization has the form $\phi = h_1 \cdots h_r$ for some monic irreducible polynomial $h_i \in \mathbb{F}_p[t]$. Each h_i is the minimal polynomial of some primitive n-th root of unity ξ over $\mathbb{F}_p$. Hence, $\deg(h_i) = [\mathbb{F}_p(\xi) : \mathbb{F}_p] = f_p$ by Example 2.5.5. This completes the proof. □

2.5.3 Quadratic subfields and a new proof of quadratic reciprocity

As in the previous subsection, ξ_m denotes a primitive m-th root of unity in $\overline{\mathbb{Q}}$ for every $m \in \mathbb{N}^*$.

Proposition 2.5.10. *Let p be an odd prime and $p^* = (-1)^{(p-1)/2} p$. Then $\mathbb{Q}(\sqrt{p^*})$ is the unique quadratic field contained in $\mathbb{Q}(\xi_p)$.*

Proof. Since $\mathrm{Gal}(\mathbb{Q}(\xi_p)/\mathbb{Q}) \cong \mathbb{F}_p^*$ is a cyclic group of order $p-1$ and 2 divides $p-1$, by Galois theory, $\mathbb{Q}(\xi_p)$ contains a unique quadratic subfield F. To see that this field F is

$\mathbb{Q}(\sqrt{p^*})$, one approach is to use the following formula for a particular quadratic Gauss sum (cf. (1.1.3.2)):

$$p^* = \left(\sum_{t=0}^{p-1} \left(\frac{t}{p} \right) \xi_p^t \right)^2 .$$

Here we use another method, coming from the ramification theory. Write $F = \mathbb{Q}(\sqrt{d})$ with $d \in \mathbb{Z} \setminus \{0, 1\}$ square-free. From Example 2.4.34 we know that a prime number q is ramified in F if and only if q is a divisor of $d_F \in \{d, 4d\}$. Such a prime q is certainly ramified in the larger field $\mathbb{Q}(\xi_p)$. But we also know that the only prime number which ramifies in $\mathbb{Q}(\xi_p)$ is p. So the only prime divisor of d_F is p. This forces $d = p^*$. □

Corollary 2.5.11. *Any quadratic field $F/\mathbb{Q}$ is contained in a cyclotomic field $\mathbb{Q}(\xi_m)$. Moreover, the smallest m such that $F \subseteq \mathbb{Q}(\xi_m)$ is $|d_F|$, the absolute value of the discriminant of F.*

Proof. Exercise. □

Remark 2.5.12. By an ***abelian number field*** we mean a finite abelian extension of $\mathbb{Q}$. For example, quadratic (number) fields are abelian number fields.

A generalization of Cor. 2.5.11 is the famous Kronecker–Weber theorem: *Every abelian number field is contained in a cyclotomic field.* This theorem is an easy consequence of class field theory (cf. Thm. 4.3.31). A proof without using class field theory is outlined in a series of exercises in [Mar18, Chap. 4]. ■

Proposition 2.5.13. *Let p be an odd prime number, $p^* = (-1)^{(p-1)/2} p$, $L = \mathbb{Q}(\xi_p)$ and $F = \mathbb{Q}(\sqrt{p^*})$. Let $q \neq p$ be another prime number. Then the following conditions are equivalent:*

(i) *The prime q splits completely in F.*

(ii) *The number of prime ideals in $\mathcal{O}_L$ lying over q is even.*

(iii) *The Legendre symbol $\left(\frac{q}{p}\right)$ equals 1.*

Proof. Choose $\sigma \in \mathrm{Gal}(L/\mathbb{Q}) \setminus \mathrm{Gal}(L/F)$. Then $\sigma|_F$ is the unique nontrivial element of the Galois group $\mathrm{Gal}(F/\mathbb{Q})$.

Let T_q be the set of prime ideals of $\mathcal{O}_L$ lying over q and $g = |T_q|$. Let $f = f(\mathfrak{P}|q)$ and let $D = D(\mathfrak{P}|q) \leq \mathrm{Gal}(L/\mathbb{Q})$ be the decomposition group, for any $\mathfrak{P} \in T_q$. (Since $L/\mathbb{Q}$ is an abelian extension, f and D depend only on q.)

(i)⇒(ii). The assumption means that $q\mathcal{O}_F = \mathfrak{p}\sigma(\mathfrak{p})$ for some $\mathfrak{p} \in \mathrm{Spm}(\mathcal{O}_F)$ lying over q. Let T_q (resp. $T_\mathfrak{p}$, resp. $T_{\sigma(\mathfrak{p})}$) be the set of prime ideals of $\mathcal{O}_L$ lying over q (resp. $\mathfrak{p}$, resp. $\sigma(\mathfrak{p})$). Then T_q is the disjoint union of $T_\mathfrak{p}$ and $T_{\sigma(\mathfrak{p})}$. The map

$$T_\mathfrak{p} \longrightarrow T_{\sigma(\mathfrak{p})} ; \quad \mathfrak{P} \longmapsto \sigma(\mathfrak{P})$$

is bijective, with inverse $\mathfrak{Q} \mapsto \sigma^{-1}(\mathfrak{Q})$. Hence $|T_q| = 2|T_\mathfrak{p}|$.

(ii)⇒(i). The decomposition group D has index g in $\mathrm{Gal}(L/\mathbb{Q})$. So the assumption implies that the decomposition field L^D contains a quadratic subfield, which must be F. Since q splits completely in L^D (Cor. 2.1.24), it also splits completely in F.

(ii)⇔(iii). We know from Thm. 2.5.9 that q is unramified in L and that the residue degree f is the order of $q \pmod p$. Hence $fg = [L:\mathbb{Q}] = p-1$, by Prop. 2.4.7, and we have

$$g \text{ is even} \iff f \,\Big|\, \frac{p-1}{2} \iff q^{\frac{p-1}{2}} \equiv 1 \pmod p \iff \left(\frac{q}{p}\right) = 1\,.$$

Here we have used Euler's theorem which asserts that for any $a \in \mathbb{Z}$ coprime to p,

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p\,.$$

(Note that Euler's theorem can be proved simply by using the cyclicity of the group $\mathbb{F}_p^*$.) □

(2.5.14) We can use Prop. 2.5.13 to give a new proof of Gauss' quadratic reciprocity law. Indeed, if p, q are distinct odd prime numbers, then by Prop. 2.5.13, the Legendre symbol $\left(\frac{q}{p}\right)$ equals 1 if and only if q splits completely in $F = \mathbb{Q}(\sqrt{p^*})$. But in Example 2.4.34 we have seen that q splits completely in F if and only if $\left(\frac{p^*}{q}\right) = 1$. So we get

$$\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right).$$

We can also deduce the supplementary formula $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ from Prop. 2.5.13, since it tells us that $\left(\frac{2}{p}\right) = 1$ if and only if 2 splits completely in $F = \mathbb{Q}(\sqrt{p^*})$. Using Example 2.4.34, we find that $\left(\frac{2}{p}\right) = 1$ if and only if $p^* \equiv 1 \pmod 8$. This last condition is easily seen to be equivalent to $p \equiv \pm 1 \pmod 8$. ■

2.6 Finiteness theorems using geometry of numbers

2.6.1 Minkowski's lattice point theorem

Definition 2.6.1. Let V be a finite dimensional $\mathbb{R}$-vector space. A ***lattice*** (or more precisely, a $\mathbb{Z}$-***lattice***) in V is a finitely generated $\mathbb{Z}$-submodule. A ***complete*** (or ***full***) lattice in V is a lattice $\Gamma \subseteq V$ that contains a $\mathbb{R}$-basis of V.

Every lattice Γ is a finitely generated free $\mathbb{Z}$-module, so its rank $\operatorname{rank}\Gamma$ can be defined. A lattice $\Gamma \subseteq V$ is complete if and only if $\operatorname{rank}\Gamma = \dim V$.

Let $w_1, \cdots, w_m$ be a $\mathbb{Z}$-basis of Γ. Then the set

$$\mathcal{F} = \mathcal{F}(w_1, \cdots, w_m) := \{a_1w_1 + \cdots + a_mw_m \,|\, a_i \in \mathbb{R}\,,\ 0 \le a_i < 1 \text{ for each } i\}$$

is called the ***fundamental mesh*** (or ***fundamental parallelepiped***, ***fundamental domain***) of Γ relative to the basis $w_1, \cdots, w_m$.

Let X be a subset of V. We say that X is ***convex*** if for any two points $x, y \in X$, the line segment $\{(1-t)x + ty \,|\, 0 \le t \le 1\}$ joining x with y is entirely contained in X. We say that X is ***centrally symmetric***, if for every $x \in X$ we have $-x \in X$. ■

Suppose that V is a $\mathbb{R}$-vector space of dimension n. The choice of a basis of V yields a linear isomorphism $V \cong \mathbb{R}^{\oplus n}$, and thus the usual topology of $\mathbb{R}^{\oplus n}$ determines a metric topology on V. It is easy to see that this topology is independent of the choice of basis chosen to get the linear isomorphism $V \cong \mathbb{R}^{\oplus n}$.

Lemma 2.6.2. *Let V be a finite dimensional $\mathbb{R}$-vector space.*

Then an additive subgroup $\Gamma \subseteq V$ is a lattice if and only if Γ is discrete in V, i.e., for every $\gamma \in \Gamma$, there is an open neighborhood U of γ in V such that $U \cap \Gamma$ is finite.

Moreover, a lattice $\Gamma \subseteq V$ is complete if and only if there is a bounded subset $M \subseteq V$ such that the collection of all translates $M + \gamma$, $\gamma \in \Gamma$ cover the entire space V.

Proof. See e.g. [Neu99, Chap. 1, Prop. 4.2 and Lemma 4.3]. □

(2.6.3) By a ***Euclidean space*** we mean a finite dimensional $\mathbb{R}$-vector space equipped with an inner product (i.e. positive definite symmetric bilinear form) $\langle \cdot, \cdot \rangle$.

Let V be a Euclidean space of dimension $n \geq 1$. The inner product $\langle \cdot, \cdot \rangle$ induces a notion of *volume* (or more precisely, *Haar measure*[**]) on V. This volume function is uniquely determined by its values at parallelepipeds. If B is a parallelepiped spanned by an ordered basis $v_1, \cdots, v_n$ of V, i.e.,

$$B = \{a_1 v_1 + \cdots + a_n v_n \,|\, 0 \leq a_i < 1\}$$

then

$$\mathrm{Vol}(B) = \sqrt{|\det(\langle v_i, v_j \rangle)|}\,.$$

Let $(e_1, \cdots, e_n)$ be an ordered orthonormal basis of V. If $P \in \mathrm{GL}_n(\mathbb{R})$ is the transition matrix from $(e_1, \cdots, e_n)$ to $(v_1, \cdots, v_n)$, then the above parallelepiped B has volume equal to $|\det(P)|$. If we use the chosen orthonormal basis to identify V with the standard Euclidean space $\mathbb{R}^n$, then the volume function on V correspond to the usual Lebesgue measure on $\mathbb{R}^n$.

Since the Euclidean space V has a metric space structure, we may speak of ***bounded*** subsets of it.

Let $\Gamma \subseteq V$ be a complete lattice. The ***covolume*** of Γ, denoted $\mathrm{Vol}(V/\Gamma)$, is defined as $\mathrm{Vol}(\mathcal{F})$, the volume of the fundamental mesh $\mathcal{F}$ relative to any $\mathbb{Z}$-basis of Γ. Since the base change matrix between any two $\mathbb{Z}$-bases of Γ has determinant ± 1, $\mathrm{Vol}(V/\Gamma)$ is independent of the choice of $\mathbb{Z}$-bases of Γ. In fact, the Haar measure of V induces a quotient Haar measure on the quotient group V/L, and $\mathrm{Vol}(V/L)$ is the volume of V/L with respect to that quotient measure. ■

Theorem 2.6.4 (Minkowski's lattice point theorem)**.** *Let Γ be a complete lattice in a Euclidean space V of dimension $n \geq 1$. Let $X \subseteq V$ be a bounded, centrally symmetric, convex subset.*

If $\mathrm{Vol}(X) > 2^n \mathrm{Vol}(V/\Gamma)$, then X contains at least one nonzero lattice point of Γ. If moreover X is closed, the same is true when $\mathrm{Vol}(X) = 2^n \mathrm{Vol}(V/\Gamma)$.

Proof. For the first assertion, see e.g. [Neu99, § I.4, (4.4)]. As an exercise, we leave it to the reader to show that the second assertion follows from the first one. □

[**] A Haar measure can be defined more generally on any locally compact Hausdorff group. See e.g. [RV99, § 1.2].

2.6.2 Finiteness of class group

In this subsection, let K be a number field of degree n (over $\mathbb{Q}$).

(2.6.5) We already know that there are precisely n field embeddings of K into $\mathbb{C}$. A field embedding $\tau : K \to \mathbb{C}$ is called ***real*** if $\tau(K) \subseteq \mathbb{R}$; otherwise τ is called ***imaginary*** or ***nonreal***. Note that if $\tau : K \to \mathbb{C}$ is an imaginary embedding, then by composition with the complex conjugation map $z \mapsto \bar{z}$ we obtain a new imaginary embedding

$$\bar{\tau} \ : \ K \longrightarrow \mathbb{C} \, ; \quad x \longmapsto \overline{\tau(x)}$$

called the (complex) ***conjugate*** of τ. We see in particular that the number of imaginary embeddings of K is even. If we denote by r_1 the number of real embeddings of K and r_2 the number of pairs of imaginary embeddings of K, then we have $r_1 + 2r_2 = [K : \mathbb{Q}] = n$.

If $r_2 = 0$, i.e., all complex embeddings of K are real, then we say that K is ***totally real***. If $r_1 = 0$, i.e., K has no real embeddings, then we say that K is ***totally imaginary*** (or ***purely imaginary***). ■

(2.6.6) Put

$$K_{\mathbb{C}} := \prod_{\tau : K \to \mathbb{C}} \mathbb{C} \quad \text{where } \tau \text{ runs over field embeddings of } K \text{ into } \mathbb{C} \, .$$

It can be viewed as $\mathbb{C}$-algebra via componentwise addition and multiplication. The complex conjugation acts on $\mathbb{C}$ as well as on the set of field embeddings $\tau : K \to \mathbb{C}$. It induces a map

$$F \ : \ K_{\mathbb{C}} = \prod_{\tau} \mathbb{C} \longrightarrow K_{\mathbb{C}} = \prod_{\tau} \mathbb{C} \, ; \quad (z_\tau)_\tau \longmapsto \left(\overline{z_{\bar{\tau}}}\right)_\tau \tag{2.6.6.1}$$

called the ***Frobenius correspondence***. Explicitly, for $z = (z_\tau) \in K_{\mathbb{C}}$, the τ-component of Fz is given by the complex conjugate of the $\bar{\tau}$-component $z_{\bar{\tau}}$ of z. Note that F is an $\mathbb{R}$-algebra automorphism of $K_{\mathbb{C}} = \prod_\tau \mathbb{C}$, but it is not $\mathbb{C}$-linear.

On $K_{\mathbb{C}} = \prod_\tau \mathbb{C}$ we have the standard Hermitian inner product

$$\big\langle (z_\tau) \, , \, (w_\tau) \big\rangle := \sum_\tau \overline{z}_\tau w_\tau \, .$$

One checks easily that this Hermitian inner product is equivariant under F, that is,

$$\langle \, Fz \, , \, Fw \, \rangle = \overline{\langle \, z \, , \, w \, \rangle} \quad \text{for all } \ z, \, w \in K_{\mathbb{C}} \, . \tag{2.6.6.2}$$

Now define

$$K_{\mathbb{R}} := \{ z \in K_{\mathbb{C}} \, | \, Fz = z \} = \left\{ (z_\tau) \in \prod_\tau \mathbb{C} \, \middle| \, z_{\bar{\tau}} = \overline{z_\tau} \ \text{ for each } \tau : K \to \mathbb{C} \right\} .$$

This is an $\mathbb{R}$-subalgebra of $K_{\mathbb{C}}$, and the restriction of the Hermitian inner product $\langle \, \cdot, \, \cdot \, \rangle$ to $K_{\mathbb{R}}$ gives an inner product

$$\langle \, \cdot, \, \cdot \, \rangle \ : \ K_{\mathbb{R}} \times K_{\mathbb{R}} \longrightarrow \mathbb{R} \, ,$$

called the ***canonical inner product***, on the $\mathbb{R}$-vector space $K_{\mathbb{R}}$. Indeed, for $x, y \in K_{\mathbb{R}}$, one has $\langle x, y \rangle \in \mathbb{R}$ in view of (2.6.6.2). The Haar measure associated to the canonical inner product is called the ***canonical measure*** on $K_{\mathbb{R}}$. The Euclidean space $(K_{\mathbb{R}}, \langle \cdot, \cdot \rangle)$ is called the ***Minkowski space*** of the number field K.

We have the natural map

$$j' : K \longrightarrow K_{\mathbb{C}} = \prod_{\tau} \mathbb{C} ; \quad x \longmapsto \big(\tau(x)\big)_{\tau} , \tag{2.6.6.3}$$

which is an injective $\mathbb{Q}$-algebra homomorphism. Its image is easily seen to be contained in $K_{\mathbb{R}}$. So we have an induced inclusion

$$j : K \longrightarrow K_{\mathbb{R}} ; \quad x \longmapsto \big(\tau(x)\big)_{\tau} . \tag{2.6.6.4}$$

Clearly, if R is a finitely generated (free) $\mathbb{Z}$-submodule in K, then $j(R)$ is a lattice of the same rank in $K_{\mathbb{R}}$. ■

Remark 2.6.7. Let us mention in passing – it will not be used in the sequel – that the inclusion $j' : K \to K_{\mathbb{C}}$ in (2.6.6.3) induces an isomorphism of $\mathbb{C}$-algebras

$$K \otimes_{\mathbb{Q}} \mathbb{C} \xrightarrow{\sim} K_{\mathbb{C}} = \prod_{\tau : K \to \mathbb{C}} \mathbb{C} ; \quad x \otimes z \longmapsto \big(\tau(x) z\big)_{\tau} , \tag{2.6.7.1}$$

via which j' gets identified with the canonical map $K \to K \otimes_{\mathbb{Q}} \mathbb{C}$; $x \mapsto x \otimes 1$. Moreover, under the identification (2.6.7.1) the Frobenius correspondence $F : K_{\mathbb{C}} \to K_{\mathbb{C}}$ corresponds to the map

$$F : K \otimes_{\mathbb{Q}} \mathbb{C} \longrightarrow K \otimes_{\mathbb{Q}} \mathbb{C} ; \quad x \otimes z \longmapsto x \otimes \bar{z} . \tag{2.6.7.2}$$

Likewise the injection j in (2.6.6.4) induces an isomorphism of $\mathbb{R}$-algebras

$$K \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow{\sim} K_{\mathbb{R}} ; \quad x \otimes \lambda \longmapsto j(x)\lambda = \big(\tau(x)\lambda\big)_{\tau} .$$

Notice that this can also be obtained by taking the F-invariants of the two sides of (2.6.7.1), in view of (2.6.7.2). ■

Lemma 2.6.8. *Let $I \subseteq K$ be a $\mathbb{Z}$-submodule containing a $\mathbb{Q}$-basis of K (i.e., I is a free $\mathbb{Z}$-submodule of rank n). Then*

$$\mathrm{Vol}\big(K_{\mathbb{R}}/j(I)\big) = \sqrt{|d(I)|} .$$

That is, the canonical covolume of the lattice $j(I)$ in the Minkowski space $K_{\mathbb{R}}$ is equal to $\sqrt{|d(I)|}$, where $d(I)$ is the (absolute) discriminant of R (Definition 2.4.30).

Proof. Let $\tau_1, \cdots, \tau_n$ be the embeddings of K into $\mathbb{C}$. Let $x_1, \cdots, x_n$ be a $\mathbb{Z}$-basis of I. Then

$$v_1 := j(x_1) = \big(\tau_1(x_1), \cdots, \tau_n(x_1)\big), \cdots, \; v_n := j(x_n) = \big(\tau_1(x_n), \cdots, \tau_n(x_n)\big)$$

form a $\mathbb{Z}$-basis of the lattice $j(I)$. By definition,

$$\langle\, v_i\,,\, v_j\,\rangle = \sum_{k=1}^{n} \overline{\tau_k(x_i)} \cdot \tau_k(x_j) = \text{ the } (i,\, j)\text{-th entry of the matrix } \overline{M}^T M\,,$$

where $M = (\tau_i(x_j))$. Hence by (2.6.3),

$$\mathrm{Vol}(K_{\mathbb{R}}/j(I)) = \sqrt{|\det(\langle\, v_i,\, v_j\,\rangle)|} = \sqrt{|\det(\overline{M}^T M)|} = |\det(M)| = \sqrt{|d(I)|}\,.$$

Here the last equality follows from Thm. 2.4.19 (1). □

Lemma 2.6.9. *Let r_1 (resp. $2r_2$) be the number of real (resp. imaginary) embeddings $K \to \mathbb{C}$. Let t be a positive real number. In the Minkowski space the subset*

$$X_t := \left\{ (z_\tau) \in K_{\mathbb{R}} \,\middle|\, \sum_{\tau} |z_\tau| \le t \right\}$$

has canonical volume

$$\mathrm{Vol}(X_t) = 2^{r_1}\pi^{r_2}\frac{t^n}{n!}\,.$$

Proof. See e.g. [Neu99, Lemma III.2.15]. □

Theorem 2.6.10. *Let r_2 be the number of pairs of imaginary embeddings of K into $\mathbb{C}$. Let $I \subseteq \mathcal{O}_K$ be a nonzero ideal.*

1. *There exists a nonzero element $x \in I$ such that*

$$|N_{K/\mathbb{Q}}(x)| \le \#\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}\sqrt{|d(I)|} = M_K \cdot \mathbf{N}(I)\,,$$

   where the number

$$M_K := \left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}\sqrt{|d_K|}$$

   is often called the **Minkowski constant** *of K (or of $\mathcal{O}_K$).*

2. *Every ideal class in the class group $\mathcal{C}l(K) := \mathcal{C}l(\mathcal{O}_K)$ contains an integral ideal whose absolute norm is at most M_K. In particular, $\mathcal{C}l(K)$ is generated by the classes of maximal ideals $\mathfrak{p}$ with absolute norm $\mathbf{N}(\mathfrak{p}) \le M_K$.*

3. *The group $\mathcal{C}l(K)$ is finite. The number $h_K := \#\mathcal{C}l(K)$ is called the* **class number** *of K (or of $\mathcal{O}_K$).*

Proof. (1) The image $j(I)$ of I under the natural injection $j : K \to K_{\mathbb{R}}$ is a complete lattice in the Minkowski space $K_{\mathbb{R}}$ with covolume $\mathrm{Vol}\big(K_{\mathbb{R}}/j(I)\big) = \sqrt{|d(I)|}$ (Lemma 2.6.8). Choose the real number $t > 0$ such that the subset X_t in Lemma 2.6.9 has

volume $\mathrm{Vol}(X_t) = 2^n\sqrt{|d(I)|}$, that is, such that $t^n = \left(\frac{4}{\pi}\right)^{r_2} n! \cdot \sqrt{|d(I)|}$. By Minkowski's lattice point theorem (Thm. 2.6.4), there is a nonzero element $x \in I$ such that $j(x) = (\tau(x))_\tau \in X_t$. Then by the arithmetic-geometric mean inequality,

$$\begin{aligned} |N_{K/\mathbb{Q}}(x)| = \prod_\tau |\tau(x)| &\le \left(\frac{1}{n}\sum_\tau |\tau(x)|\right)^n \\ &\le \frac{t^n}{n^n} = \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}\sqrt{|d(I)|} = M_K \cdot \mathbf{N}(I)\,. \end{aligned}$$

(Here $\sqrt{|d(I)|} = \sqrt{|d_K|} \cdot \mathbf{N}(I)$ by Prop. 2.4.31.)

(2) Let $\mathfrak{a}$ be any fractional ideal of K. Choose a nonzero element $b \in K^*$ such that $b\mathfrak{a}^{-1}$ is an integral ideal. Applying (1) with $I = b\mathfrak{a}^{-1}$ we find a nonzero element $x \in I$ such that $\mathbf{N}(xI^{-1}) \le M_K$. Since $xI^{-1} = xb^{-1}\mathfrak{a}$ lies in the same ideal class as $\mathfrak{a}$, the first assertion is proved. The second assertion follows from the first one, because $\mathfrak{a} \subseteq \mathfrak{p}$ implies $\mathbf{N}(\mathfrak{p}) \le \mathbf{N}(\mathfrak{a})$.

(3) By (2), a complete set of representatives of the class group is contained in the set of nonzero integral ideals with norm not exceeding a given upper bound. This latter set is easily seen to be finite. □

Corollary 2.6.11. *The discriminant of a number field K of degree n with $2r_2$ imaginary complex embeddings satisfies*

$$|d_K| \ge \left(\frac{\pi}{4}\right)^{2r_2} \frac{n^{2n}}{(n!)^2} \ge b_n := \left(\frac{\pi}{4}\right)^n \frac{n^{2n}}{(n!)^2}\,.$$

One has $b_n \ge \frac{\pi^n}{4}$ for all n and $\lim_{n\to\infty} \sqrt[n]{b_n} = \pi e^2/4 \approx 5.803$.

Proof. As the absolute norm of any nonzero integral ideal is a positive integer, we must have $M_K \ge 1$ by Thm. 2.6.10 (2). This yields the inequalities for d_K. From the identity

$$\frac{b_{n+1}}{b_n} = \frac{\pi}{4}\left(1 + \frac{1}{n}\right)^{2n} \ge \pi$$

we obtain the lower bound for b_n and the limit behavior

$$\lim_{n\to\infty} \sqrt[n]{b_n} = \lim_{n\to\infty} \sqrt[n]{b_{n+1}} = \lim_{n\to\infty} \frac{b_{n+1}}{b_n} = \frac{\pi e^2}{4}\,.$$

Here we have used the Stolz–Cesàro theorem (also known as the Stolz formula, which is a discrete version of L'Hôpital's rule): If (c_n) is a strictly increasing unbounded sequence of real numbers and (a_n) is a sequence of real numbers such that $\lim_{n\to\infty} \frac{a_{n+1}-a_n}{c_{n+1}-c_n} = l$ exists in $\mathbb{R}$, then $\lim_{n\to\infty} \frac{a_n}{c_n} = l$. □

The following result is immediate from Cor. 2.6.11:

Theorem 2.6.12 (Minkowski)**.** *The discriminant of any number field $K \ne \mathbb{Q}$ satisfies $|d_K| > 1$.*

(2.6.13) An ***order*** (or more precisely, a $\mathbb{Z}$-order) in K is a subring of K which is a (free) $\mathbb{Z}$-module of rank n.

Let $R \subseteq K$ be an order. Then R is Noetherian and integral over $\mathbb{Z}$. In particular, $R \subseteq \mathcal{O}_K$. Let $\mathscr{I}(R)$ denote the set of *invertible* fractional ideals of R, and let $\mathscr{P}(R) \subseteq \mathscr{I}(R)$ be the subset consisting of principal fractional ideals. Then $\mathscr{I}(R)$ is a multiplicative group and $\mathscr{P}(R)$ is a subgroup. The quotient $\mathrm{Pic}(R) := \mathscr{I}(R)/\mathscr{P}(R)$ is called the ***Picard group*** of R. In the case $R = \mathcal{O}_K$, $\mathrm{Pic}(\mathcal{O}_K)$ is the same as the ideal class group $\mathcal{C}l(K) = \mathcal{C}l(\mathcal{O}_K)$.

For any $I \in \mathscr{I}(R)$, choosing a nonzero element $x \in I$ we have $xR \subseteq I$. So I contains a $\mathbb{Q}$-basis of K and the discriminant $d(I)$ is defined (Definition 2.4.30). If $I \subseteq R$, then R/I is finite and $d(I) = |R/I|^2 \cdot d(R)$ by Prop. 2.4.31. We call $\mathbf{N}(I) := |R/I|$ the ***absolute norm*** of I.

We leave it to the reader to check the following facts:

1. For any nonzero element $x \in R$, we have $\mathbf{N}(xR) = \#(R/xR) = |N_{K/\mathbb{Q}}(x)|$. (This can be shown by using a matrix version of the elementary factors theorem. See e.g. [Lan02, p.154, Thm. III.7.9].)

2. Let I, $J \in \mathscr{I}(R)$ with $I \subseteq R$ and $J \subseteq R$. Then $\mathbf{N}(I)\mathbf{N}(J) = \mathbf{N}(IJ)$.

3. Using the same method, one can prove an analog of Theorem 2.6.10 for R in place of $\mathcal{O}_K$. That is, every nonzero ideal $I \subseteq R$ contains a nonzero element x with $|N_{K/\mathbb{Q}}(x)| \le M_R \cdot \mathbf{N}(I)$, every ideal class in $\mathrm{Pic}(R)$ contains an integral ideal with absolute norm $\le M_R$, and $\mathrm{Pic}(R)$ is finite. Here $M_R := \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|d(R)|}$ is called the ***Minkowski constant*** of R.

   The number $h_R := |\mathrm{Pic}(R)|$ is called the ***class number*** of R.

4. Similarly, Cor. 2.6.11 remains true when d_K is replaced by $d(R)$.

More information can be obtained for the order R by using the ***conductor*** (*Führer* in German)

$$\mathfrak{r} := \{x \in \mathcal{O}_K \mid x\mathcal{O}_K \subseteq R\}$$

of R in $\mathcal{O}_K$. See e.g. [Neu99, § I.12]. ■

Example 2.6.14. For a number field with small absolute value of discriminant, the Minkowski bound of norms of integral ideals can help us to determine the structure of its class group.

(1) The quadratic field $K = \mathbb{Q}(\sqrt{-5})$ has ring of integers $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. Then $M_K = \frac{2}{\pi}\sqrt{20} < 3$. We know that $2\mathcal{O}_K = \mathfrak{p}^2$ with $\mathfrak{p} = (2, 1 + \sqrt{-5})$. So the only maximal ideal of R with absolute norm ≤ 2 is $\mathfrak{p}$. So $\mathcal{C}l(K)$ is generated by the class $[\mathfrak{p}]$ of $\mathfrak{p}$ by Thm. 2.6.10 (2). Since $\mathfrak{p}^2$ is principal, we see that $\mathcal{C}l(K) \cong \mathbb{Z}/2$. This shows that $\mathbb{Q}(\sqrt{-5})$ has class number 2.

(2) Let $K = \mathbb{Q}(\sqrt{-19})$. We have $M_K = \frac{2}{\pi}\sqrt{19} < 3$. The principal ideal $2\mathcal{O}_K$ is prime in $\mathcal{O}_K = \mathbb{Z}[\frac{-1+\sqrt{-19}}{2}]$. So there is no maximal ideal of $\mathcal{O}_K$ with absolute norm ≤ 2. This implies that $\mathcal{C}l(K)$ is trivial, i.e., $h_K = 1$. ■

2.6.3 Dirichlet's unit theorem

In this subsection, let K be a number field of degree n which has r_1 real embeddings and $2r_2$ imaginary embeddings into $\mathbb{C}$. Our aim is to prove the following theorem:

Theorem 2.6.15 (Dirichlet's unit theorem)**.** *Let R be an order in K and write $\mu_\infty(R)$ for the multiplicative group of roots of unity in R.*

Then $\mu_\infty(R)$ is finite and there is a group isomorphism $R^* \cong \mu_\infty(R) \times \mathbb{Z}^{\oplus r_1+r_2-1}$.

(2.6.16) In order to prove Thm. 2.6.15 we need to generalize the definition of trace and norm maps given in (1.2.1).

Let A be a commutative ring and let B be an A-algebra which is free of finite rank as an A-module. Then for any $\alpha \in B$, multiplication by α yields an A-linear map $m_\alpha : B \to B$, $x \mapsto \alpha x$. Choosing any basis $e_1, \cdots, e_n$ of B over A and representing the map m_α by a matrix $M_\alpha \in \mathrm{M}_n(A)$, we can define the ***trace*** $\mathrm{Tr}_{B/A}(\alpha)$ and the ***norm*** $N_{B/A}(\alpha)$ by

$$\mathrm{Tr}_{B/A}(\alpha) = \mathrm{Tr}(M_\alpha) \quad \text{and} \quad N_{B/A}(\alpha) = \det(M_\alpha)\,.$$

The trace map $\mathrm{Tr}_{B/A} : B \to A$ is A-linear, and the norm map $N_{B/A} : B \to A$ is multiplicative (i.e., $N_{B/A}(\alpha\beta) = N_{B/A}(\alpha)N_{B/A}(\beta)$). If $B = B_1 \times \cdots \times B_r$ is the direct product of some finite rank free A-algebras $B_1, \cdots, B_r$, then from the definition we see that

$$\mathrm{Tr}_{B/A} = \sum_{i=1}^{r} \mathrm{Tr}_{B_i/A}\,, \quad N_{B/A} = \prod_{i=1}^{r} N_{B_i/A}\,.$$

More precisely, if $\alpha = (\alpha_1, \cdots, \alpha_r)$ with $\alpha_i \in B_i$, then

$$\mathrm{Tr}_{B/A}(\alpha) = \sum_{i=1}^{r} \mathrm{Tr}_{B_i/A}(\alpha_i) \quad \text{and} \quad N_{B/A}(\alpha) = \prod_{i=1}^{r} N_{B_i/A}(\alpha_i)\,. \tag{2.6.16.1}$$

It is also clear that the norm map induces a homomorphism

$$N_{B/A} : B^* \longrightarrow A^*$$

between the groups of units.

If A' is any other A-algebra and $B' = B \otimes_A A'$, then the diagrams

$$\begin{array}{ccc} B & \longrightarrow & B' \\ {\scriptstyle \mathrm{Tr}_{B/A}}\downarrow & & \downarrow{\scriptstyle \mathrm{Tr}_{B'/A'}} \\ A & \longrightarrow & A' \end{array} \quad \text{and} \quad \begin{array}{ccc} B & \longrightarrow & B' \\ {\scriptstyle N_{B/A}}\downarrow & & \downarrow{\scriptstyle N_{B'/A'}} \\ A & \longrightarrow & A' \end{array} \tag{2.6.16.2}$$

are commutative. ∎

(2.6.17) Recall that in (2.6.6) we have defined the $\mathbb{C}$-algebra $K_\mathbb{C} = \prod_\tau \mathbb{C}$ and its $\mathbb{R}$-subalgebra

$$K_\mathbb{R} = \left\{ (z_\tau) \in \prod_\tau \mathbb{C} \;\middle|\; \forall\, \tau\,,\ z_{\overline{\tau}} = \overline{z_\tau} \right\},$$

where τ runs over field embeddings of K into $\mathbb{C}$.

Let $\rho_1, \cdots, \rho_{r_1} : K \to \mathbb{R}$ be the real embeddings and let

$$\sigma_1, \overline{\sigma}_1, \cdots, \sigma_{r_2}, \overline{\sigma}_{r_2} \ : \ K \longrightarrow \mathbb{C}$$

be the imaginary embeddings. Then we have

$$K_{\mathbb{R}} = \left\{ (z_\tau) \in \prod_\tau \mathbb{C} \,\middle|\, z_{\rho_i} \in \mathbb{R}\,,\ i = 1, \cdots, r_1 \text{ and } z_{\overline{\sigma}_j} = \overline{z_{\sigma_j}}\,,\ j = 1, \cdots, r_2 \right\}.$$

As was discussed in (2.6.16), there is a norm map $N : K_{\mathbb{R}}^* \longrightarrow \mathbb{R}^*$. One checks easily that this norm is given explicitly by the formula

$$(z_\tau) \longmapsto \prod_{i=1}^{r_1} z_{\rho_i} \cdot \prod_{j=1}^{r_2} (z_{\sigma_j} z_{\overline{\sigma_j}}) = \prod_{i=1}^{r_1} z_{\rho_i} \cdot \prod_{j=1}^{r_2} |z_{\sigma_j}|^2 .$$

The natural logarithmic function induces a group homomorphism

$$\ell \ : \ K_{\mathbb{R}}^* \longrightarrow \mathbb{R}^{\oplus r_1 + r_2} \ ; \quad (z_\tau) \longmapsto \left(\ln |z_{\rho_1}|, \cdots, \ln |z_{\rho_{r_1}}|, 2 \ln |z_{\sigma_1}|, \cdots, 2 \ln |z_{\sigma_{r_2}}| \right) .$$

A direct computation shows that the diagram

$$\begin{array}{ccccc} K^* & \xrightarrow{\ j\ } & K_{\mathbb{R}}^* & \xrightarrow{\ \ell\ } & \mathbb{R}^{\oplus r_1 + r_2} \\ {\scriptstyle N_{K/\mathbb{Q}}}\downarrow & & \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle \mathrm{Tr}} \\ \mathbb{Q}^* & \longrightarrow & \mathbb{R}^* & \xrightarrow{\ \ln|\cdot|\ } & \mathbb{R} \end{array}$$

is commutative. (The map $j : x \mapsto (\tau(x))$ was defined in (2.6.6.4).) This diagram induces homomorphisms $\mathcal{O}_K^* \xrightarrow{\ j\ } S \xrightarrow{\ \ell\ } H$, where

$$S = \{ \theta \in K_{\mathbb{R}}^* \,|\, N(\theta) = \pm 1 \} \quad \text{(the "norm-one hypersurface" in } K_{\mathbb{R}})$$

and

$$H = \{ x \in \mathbb{R}^{\oplus r_1 + r_2} \mid \mathrm{Tr}(x) = 0 \} \quad \text{(the "trace-zero" hyperplane)}.$$

Since $R \subseteq \mathcal{O}_K$, we obtain a map

$$\lambda : R^* \longrightarrow H \ ; \quad x \longmapsto (\ln |\rho_1(x)|, \cdots, \ln |\rho_{r_1}(x)|, 2 \ln |\sigma_1(x)|, \cdots, 2 \ln |\sigma_{r_2}(x)|) .$$

by restricting the composite map $\mathcal{O}_K^* \xrightarrow{\ j\ } S \xrightarrow{\ \ell\ } H$ to R^*. ■

We now see that Thm. 2.6.14 can be rephrased as follows:

Proposition 2.6.18. *With notation as in* (2.6.17), $\mathrm{Ker}(\lambda)$ *is finite, equal to* $\mu_\infty(R)$ *and* $\Gamma := \lambda(R^*)$ *is a complete lattice in* H.

Proof. For any $\xi \in \mu_\infty(R)$ we have $|\tau(\xi)| = 1$ for every embedding $\tau : K \to \mathbb{C}$. Hence $\mu_\infty(R) \subseteq \mathrm{Ker}(\lambda)$. On the other hand, suppose $\varepsilon \in \mathrm{Ker}(\lambda)$. Then $|\tau(\varepsilon)| = 1$ for every embedding $\tau : K \to \mathbb{C}$. Considering the map $j : K \to K_\mathbb{R}$, we see that $j(\varepsilon) = (\tau(\varepsilon))$ lies in a bounded domain of the vector space $K_\mathbb{R}$. But $j(\varepsilon)$ is also a point of the lattice $j(R) \subseteq K_\mathbb{R}$. Therefore, $\mathrm{Ker}(\lambda)$ contains only finitely many elements. As a finite multiplicative subgroup of R^*, $\mathrm{Ker}(\lambda)$ must consist of roots of unity.

We are left to show that Γ is a complete lattice in H. This proof is based on Lemma 2.6.2. By the definition of λ, it suffices to show that for every real number $c > 0$, the bounded domain

$$X_c := \{(x_i) \in \mathbb{R}^{\oplus r_1 + r_2} \,|\, |x_i| \leq c\}$$

contains only finitely many points of $\Gamma = \ln(j(R))$. The inverse image of X_c under the map ℓ is the bounded domain

$$Z_c := \{(z_\tau) \in K_\mathbb{R} \,|\, \forall\, \tau\,,\ e^{-c} \leq |z_\tau|^{a_\tau} \leq e^c\}\,, \text{ where } a_\tau = 1 \text{ or } 2\,,$$

in $K_\mathbb{R}$. Now Z_c contains only finitely many points of $j(R^*)$ because it is a subset of the lattice $j(R)$ in $K_\mathbb{R}$. It follows that $X_c \cap \Gamma$ is finite. By Lemma 2.6.2, Γ is a lattice.

It remains to prove that Γ is complete. According to Lemma 2.6.2, it is sufficient to find a bounded subset $M \subseteq H$ such that

$$H = \bigcup_{\gamma \in \Gamma} (M + \gamma)\,.$$

We construct this set through its preimage with respect to the surjective group homomorphism $\ln : S \longrightarrow H$. More precisely, we will construct a bounded subset T in the norm-one hypersurface $S \subseteq K_\mathbb{R}$ such that

$$S = \bigcup_{\varepsilon \in R^*} T.j(\varepsilon)\,.$$

For $x = (x_\tau) \in T$, it will follow that the absolute values $|x_\tau|$ are bounded from above and also away from 0, because $\prod_\tau |x_\tau| = 1$. Thus $M := \ell(T)$ will also be bounded and satisfy the required property.

To construct T we choose a real number $c_\tau > 0$ for each embedding $\tau : K \to \mathbb{C}$ such that

$$c_\tau = c_{\overline{\tau}} \quad \text{and} \quad C := \prod_\tau c_\tau > \left(\frac{2}{\pi}\right)^{r_2} \sqrt{|d(R)|}\,,$$

and we consider the set

$$X := \{(z_\tau) \in K_\mathbb{R} \,|\, \forall\, \tau\,,\ |z_\tau| < c_\tau\}\,.$$

For an arbitrary point $y = (y_\tau) \in S$, it follows that

$$X.y = \{(z_\tau) \in K_\mathbb{R} \,|\, \forall\, \tau\,,\ |z_\tau| < c'_\tau := c_\tau |y_\tau|\}\,,$$

and one has

$$c'_{\overline{\tau}} = c'_\tau \quad \text{and} \quad \prod_\tau c'_\tau = \prod_\tau c_\tau = C$$

because $\prod_\tau |y_\tau| = |N(y)| = 1$. In Lemma 2.6.20 below, we will show that there exists a nonzero element $a \in R$ such that $j(a) = (\tau(a))_\tau \in X.y$. Thus, $y \in S \cap X.j(a)^{-1}$.

Note that $j(R) \cap X.y$ is contained in the set $j(B)$, where

$$B := \{b \in R \,|\, 0 < |N_{K/\mathbb{Q}}(b)| < C\}$$

Since there are only finitely many integral ideals with bounded absolute norm, we can find a finite number of elements $b_1, \cdots, b_s \in B$ such that

$$B = \{b_1, \cdots, b_s\} \cdot R^* \,.$$

Now the set $T := S \cap \bigcup_{i=1}^s X.(j(b_i))^{-1}$ has the required property.

Indeed, since X is bounded, so is $X.j(b_i)^{-1}$ and therefore also T. For any $y \in S$, we have found above an element $0 \neq a \in R$ such that $y \in S \cap X.j(a)^{-1}$ and $a \in B$. Here $a = b_i\varepsilon^{-1}$ for some $i \in [\![1,\, s]\!]$ and $\varepsilon \in R^*$. Consequently,

$$y \in X.j(a)^{-1} = X.j(b_i)^{-1}.j(\varepsilon) \subseteq T.j(\varepsilon)\,.$$

Since $j(R^*) \subseteq S$ and $T \subseteq S$, we also have $T.j(\varepsilon) \subseteq S$ for every $\varepsilon \in R^*$. So $S = \bigcup_{\varepsilon \in R^*} T.j(\varepsilon)$ as desired. □

The proof of Prop. 2.6.18 will be completed only after the next two lemmas are proved.

For a complex number z, let $\Re(z)$ denote its real part and $\Im(z)$ denote its imaginary part.

Lemma 2.6.19. *Let $\rho_1, \cdots, \rho_{r_1}$ be the real embeddings of K and let $\sigma_1, \overline{\sigma}_1, \cdots, \sigma_{r_1}, \overline{\sigma}_{r_2}$ be the imaginary embeddings of K. Define the map*

$$f \,:\, K_{\mathbb{R}} \longrightarrow \mathbb{R}^{\oplus n}\,;\; (z_\tau) \longmapsto (x_\tau)$$

with

$$x_{\rho_i} = z_{\rho_i}\,,\; x_{\sigma_j} = \Re(z_{\sigma_j}) = \Re(z_{\overline{\sigma}_j})\,,\; x_{\overline{\sigma}_j} = \Im(z_{\sigma_j}) = -\Im(z_{\overline{\sigma}_j})\,.$$

Then f is an isomorphism of $\mathbb{R}$-vector spaces. The canonical inner product of the Minkowski space is transformed by f into the following inner product on $\mathbb{R}^{\oplus n}$:

$$\langle\, x,\, y\,\rangle = \sum_{\tau : K \to \mathbb{C}} a_\tau x_\tau y_\tau\,, \quad x = (x_\tau)\,,\, y = (y_\tau)$$

where $a_\tau = 1$ if τ is real and $a_\tau = 2$ if τ is imaginary. That is, for any $z = (z_\tau)$, $w = (w_\tau) \in K_{\mathbb{R}}$, with $(x_\tau) = f(z)$ and $(y_\tau) = f(w)$, we have

$$\langle\, z\,,\, w\,\rangle = \sum_\tau a_\tau x_\tau y_\tau\,.$$

In particular, for any $X \subseteq K_{\mathbb{R}}$, we have

$$\mathrm{Vol}(X) = 2^{r_2}\mathrm{Vol}_{\mathrm{Lebesgue}}(f(X))\,.$$

Here $\mathrm{Vol}_{\mathrm{Lebesgue}}$ denotes the usual Lebesgue measure on $\mathbb{R}^{\oplus n}$.

Proof. The map f is obviously an isomorphism of real vector spaces. Let $z = (z_\tau)$, $w = (w_\tau) \in K_{\mathbb{R}}$, with $(x_\tau) = f(z)$ and $(y_\tau) = f(w)$. For an imaginary embedding σ, we have

$$z_\sigma = x_\sigma + x_{\overline{\sigma}}\sqrt{-1}\,,\ z_{\overline{\sigma}} = x_\sigma - x_{\overline{\sigma}}\sqrt{-1}\,,$$
$$w_\sigma = y_\sigma + y_{\overline{\sigma}}\sqrt{-1}\,,\ w_{\overline{\sigma}} = y_\sigma - y_{\overline{\sigma}}\sqrt{-1}\,,$$

so that

$$\overline{z_\sigma}w_\sigma + \overline{z_{\overline{\sigma}}}w_{\overline{\sigma}} = 2\Re(\overline{z_\sigma}w_\sigma) = 2(x_\sigma y_\sigma + x_{\overline{\sigma}}y_{\overline{\sigma}})\,.$$

This proves the assertion about the inner products. □

Lemma 2.6.20. *Let R be an order in K and let $I \subseteq R$ be a nonzero ideal. For each embedding $\tau : K \to \mathbb{C}$ suppose a real number $c_\tau > 0$ is given such that*

$$c_{\overline{\tau}} = c_\tau \quad \textit{and} \quad \prod_\tau c_\tau > \left(\frac{2}{\pi}\right)^{r_2}\sqrt{|d(I)|}\,.$$

Then there exists a nonzero element $a \in I$ such that $|\tau(a)| < c_\tau$ for every embedding $\tau : K \to \mathbb{C}$.

Proof. The set

$$X := \{(z_\tau) \in K_{\mathbb{R}} \,|\, \forall\, \tau\,,\ |z_\tau| < c_\tau\}$$

is convex and centrally symmetric. Its volume can be computed via the map f in Lemma 2.6.19. Indeed,

$$f(X) = \{(x_\tau) \in \mathbb{R}^{\oplus n} \,|\, |x_{\rho_i}| < c_{\rho_i}\,,\ x_{\sigma_j}^2 + x_{\overline{\sigma}_j}^2 < c_{\sigma_j}^2\}\,.$$

This gives

$$\begin{aligned}\mathrm{Vol}(X) &= 2^{r_2}\mathrm{Vol}_{\mathrm{Lebesgue}}\big(f(X)\big) = 2^{r_2}\prod_{i=1}^{r_1}(2c_{\rho_i})\cdot\prod_{j=1}^{r_2}(\pi c_{\sigma_j}^2)\\ &= 2^{r_1+r_2}\pi^{r_2}\prod_\tau c_\tau > 2^{r_1+r_2}\pi^{r_2}\cdot\frac{2^{r_2}}{\pi^{r_2}}\sqrt{|d(I)|} = 2^n\sqrt{|d(I)|}\,.\end{aligned}$$

By Lemma 2.6.8 we have $\mathrm{Vol}(X) > 2^n\mathrm{Vol}(K_{\mathbb{R}}/j(I))$. Hence, by Minkowski's lattice point theorem (Thm. 2.6.4), X contains a nonzero point of $j(I)$. □

As the proof of Thm. 2.6.15 relies on the Minkowski's lattice point theorem, it is not directly constructive and cannot be used to explicitly find unit groups.

Remark 2.6.21. With notation as in Thm. 2.6.15, put $t = r_1 + r_2 - 1$. We now know that there exist units $\eta_1, \cdots, \eta_t \in R^*$ such that

$$R^* = \mu_\infty(R) \times \eta_1^{\mathbb{Z}} \times \cdots \times \eta_t^{\mathbb{Z}}\,.$$

(Here $\eta_i^{\mathbb{Z}}$ denotes the infinite cyclic multiplicative group generated by η_i.) Such a system $\eta_1, \cdots, \eta_t$ is called a system of ***fundamental units*** of R.

Note that if $r_1 > 0$, then $\mu_\infty(R) = \{\pm 1\}$ because there are no other roots of unity in $\mathbb{R}$.

If K is an imaginary quadratic field, then $t = 0$ and hence $R^* = \mu_\infty(R)$. (Compare Props. 2.2.8 (1) and (2.2.10) (2).)

If K is a real quadratic field, then $t = 1$. In this case, any system of fundamental units has a single member ε, and $R^* = \{\pm 1\} \times \eta^{\mathbb{Z}}$. So there is one and only one unit $\varepsilon > 1$ such that $R^* = \mu_\infty(R) \times \varepsilon^{\mathbb{Z}}$. This element ε is called the ***fundamental unit*** of R. (In other words, when talking about system of fundamental units of an order in a real quadratic field, we often mean the unit which is greater than 1 and which forms a system of fundamental units.) An effective method of find the fundamental unit for such an order is to use continued fractions. We refer the interested reader to [Ros11, § 13.4] for more details about this method. ■

(2.6.22) With notation as in (2.6.17), we can consider the trace-zero hyperplane H as a Euclidean space of dimension $t := r_1 + r_2 - 1$, by restricting the standard inner product of $\mathbb{R}^{\oplus r_1 + r_2}$ to H. Then the covolume of the lattice $\lambda(R^*)$ in H is defined. We call the number

$$\mathrm{Reg}(R) := \frac{1}{\sqrt{r_1 + r_2}} \mathrm{Vol}(H/\lambda(R^*))$$

the ***regulator*** of R. Here, when $t = 0$ we use the convention that $\mathrm{Reg}(R) = 1$.

In the special case $R = \mathcal{O}_K$, the regulator $\mathrm{Reg}(\mathcal{O}_K)$ is also called the ***regulator*** of the number field K, and is often denoted by R_K. ■

Proposition 2.6.23. *Let R be an order in K and let $\varepsilon_1, \cdots, \varepsilon_t$ be a system of fundamental units of R. Write each $\lambda(\varepsilon_j) \in H \subseteq \mathbb{R}^{\oplus t+1}$ as a column vector and consider the $(t+1) \times t$ real matrix*

$$M := \big(\lambda(\varepsilon_1)\,,\, \lambda(\varepsilon_2)\,,\, \cdots\,,\, \lambda(\varepsilon_t)\big) = \begin{pmatrix} \ln|\rho_1(\varepsilon_1)| & \ln|\rho_1(\varepsilon_2)| & \cdots & \ln|\rho_1(\varepsilon_t)| \\ \vdots & \vdots & \vdots & \vdots \\ \ln|\rho_{r_1}(\varepsilon_1)| & \ln|\rho_{r_1}(\varepsilon_2)| & \cdots & \ln|\rho_{r_1}(\varepsilon_t)| \\ 2\ln|\sigma_1(\varepsilon_1)| & 2\ln|\sigma_1(\varepsilon_2)| & \cdots & 2\ln|\sigma_1(\varepsilon_t)| \\ \vdots & \vdots & \vdots & \vdots \\ 2\ln|\sigma_{r_2}(\varepsilon_1)| & 2\ln|\sigma_{r_2}(\varepsilon_2)| & \cdots & 2\ln|\sigma_{r_2}(\varepsilon_t)| \end{pmatrix}$$

For each $j \in [\![1, \cdots, t+1]\!]$, let $M_j \in \mathrm{M}_r(\mathbb{R})$ be the submatrix of M obtained by deleting the j-th row from M.

Then we have $\mathrm{Reg}(R) = |\det(M_j)|$ for every $j \in [\![1, \cdots, t+1]\!]$.

Proof. Clearly, the orthogonal complement of H in $\mathbb{R}^{\oplus r_1 + r_2}$ is spanned by the unit vector

$$\lambda_0 := \frac{1}{\sqrt{r_1 + r_2}} (1,\, 1, \cdots, 1)^T\,.$$

Hence the t-dimensional volume of the fundamental mesh of $\lambda(R^*) = \mathbb{Z}.\lambda(\varepsilon_1) \oplus \cdots \oplus \mathbb{Z}.\lambda(\varepsilon_t)$ equals the $(t+1)$-dimensional volume of the parallelepiped spanned by

$$\lambda_0\,,\, \lambda(\varepsilon_1)\,,\, \cdots\,,\, \lambda(\varepsilon_t) \quad \text{ in } \mathbb{R}^{\oplus t+1}\,.$$

This latter volume is equal to $|\det(M')|$, where

$$M' := (\lambda_0\,,\, M) = \begin{pmatrix} \frac{1}{\sqrt{r_1+r_2}} & \ln|\rho_1(\varepsilon_1)| & \ln|\rho_1(\varepsilon_2)| & \cdots & \ln|\rho_1(\varepsilon_t)| \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \frac{1}{\sqrt{r_1+r_2}} & \ln|\rho_{r_1}(\varepsilon_1)| & \ln|\rho_{r_1}(\varepsilon_2)| & \cdots & \ln|\rho_{r_1}(\varepsilon_t)| \\ \frac{1}{\sqrt{r_1+r_2}} & 2\ln|\sigma_1(\varepsilon_1)| & 2\ln|\sigma_1(\varepsilon_2)| & \cdots & 2\ln|\sigma_1(\varepsilon_t)| \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \frac{1}{\sqrt{r_1+r_2}} & 2\ln|\sigma_{r_2}(\varepsilon_1)| & 2\ln|\sigma_{r_2}(\varepsilon_2)| & \cdots & 2\ln|\sigma_{r_2}(\varepsilon_t)| \end{pmatrix}.$$

Adding all the other rows of M' to the j-th row, we obtain $(\sqrt{r_1+r_2},\, 0,\, 0,\, \cdots,\, 0)$. So the result follows. □

3 Valuations in Number Theory

3.1 Absolute values and valued fields

3.1.1 Absolute values and valuations

Definition 3.1.1. Let K be a field. An ***absolute value***[††] on K is a map $|\cdot| : K \to \mathbb{R}_{\geq 0}$ satisfying the following axioms for all $x,\, y \in K$:

(AV1) $|x| > 0$ for all $x \in K^*$ and $|0| = 0$.

(AV2) $|xy| = |x| \cdot |y|$.

(AV3) (Triangle inequality) $|x+y| \leq |x| + |y|$.

The absolute value sending every $x \in K^*$ to $1 \in \mathbb{R}_{\geq 0}$ is called the ***trivial absolute value*** on K.

If an absolute value $|\cdot|$ satisfies the *strong triangle inequality*, i.e.,

(AV3′) $|x+y| \leq \max\{\,|x|\,,\,|y|\,\}$ for all $x,\, y \in K$,

then it is called ***ultrametric*** or ***non-archimedean***. Otherwise the absolute value is called ***archimedean***.

An absolute value $|\cdot|$ on K defines a metric $d : K \times K \to \mathbb{R}_{\geq 0}$ by

$$d(x,\, y) := |x - y| \quad \text{for all } x,\, y \in K\,.$$

In particular, $|\cdot|$ induces a metric topology on K. Two absolute values on K are said to be ***dependent*** or ***equivalent***, if they define the same topology on K. Otherwise they are called ***independent*** or ***inequivalent***. ■

Example 3.1.2.

(1) For $K = \mathbb{R}$ we have the usual absolute value $|\cdot|$, which is obviously archimedean. It induces the usual absolute value on $\mathbb{C}$:

$$|x + y.\mathrm{i}| = \sqrt{x^2 + y^2} \quad \text{for all } x,\, y \in \mathbb{R}\,.$$

[††]Some books (e.g. [Neu99], [O'M00], etc.) use the terminology "valuation" for what we call absolute value.

(2) Any absolute value $|\cdot|$ on finite field $\mathbb{F}$ must be trivial. Indeed, the absolute values of elements in $\mathbb{F}^*$ form a finite subgroup of the group $\mathbb{R}_+^*$ of positive real numbers, which must be trivial. ■

Proposition 3.1.3 (Domination principle, ultrametic property)**.** *Suppose $|\cdot|$ is a non-archimedean absolute valuation on a field K.*

Then for all $x, y \in K$, we have $|x+y| = \max\{|x|, |y|\}$ if $|x| \neq |y|$.

Proof. Let us assume $|x| > |y|$. Then

$$|x| = |-y+x+y| \leq \max\{|-y|, |x+y|\} = \max\{|y|, |x+y|\}\,.$$

This implies $|x| = |x+y|$ since $|x+y| \leq \max\{|x|, |y|\} = |x|$. □

Proposition 3.1.4. *An absolute value $|\cdot|$ on a field K is non-archimedean if and only if the sequence $\{\,|n.1_K|\,\}_{n\in\mathbb{N}}$ is bounded.*

In particular, if $\mathrm{char}(K) > 0$, then K has no archimedean absolute value.

Proof. See [Neu99, Prop. II.3.6] or [O'M00, (11:1)]. □

Proposition 3.1.5. *Let $|\cdot|_1$ and $|\cdot|_2$ be two absolute values on a field K. Then the following assertions are equivalent:*

(i) *The two absolute values $|\cdot|_1$ and $|\cdot|_2$ are equivalent.*

(ii) *For every $x \in K$, $|x|_1 < 1$ if and only if $|x|_2 < 1$.*

(ii′) *For every $x \in K$, $|x|_1 \leq 1$ if and only if $|x|_2 \leq 1$.*

(iii) *There is a real number $s > 0$ such that $|x|_1 = |x|_2^s$ for all $x \in K$.*

Proof. See [Neu99, Prop. II.3.3] or [O'M00, (11:4)]. □

Be careful that for an absolute value $|\cdot|$, the above proposition does not assert that the function $|\cdot|^s$ is again an absolute value for all $s > 0$. (In fact, this is not true for the usual absolute value of $\mathbb{R}$ if $s = 2$.) The proposition only ensures that $|\cdot|$ is equivalent to $|\cdot|^s$, if the latter is again an absolute value.

Definition 3.1.6. Let K be a field. An ***exponential valuation***[‡‡] on K is a map

$$v \,:\, K \longrightarrow \mathbb{R} \cup \{\,+\infty\,\}$$

satisfying the following properties for all $x, y \in K$:

(V1) $v(x) = +\infty$ if and only if $x = 0$.

(V2) $v(xy) = v(x) + v(y)$.

(V3) $v(x+y) \geq \min\{\,v(x), v(y)\,\}$

[‡‡]This is also what people call ***valuation of rank*** ≤ 1 (cf. [Bou06, §VI.4.5, Prop. 8]). We refer the interested readers to [Bou06] or [EP05] for the general valuation theory.

For any exponent valuation v on K, the subset

$$\mathcal{O}_v := \{x \in K \,:\, v(x) \geq 0\}$$

is a local ring, called the ***valuation ring*** of v. Its maximal ideal is given by

$$\mathfrak{p}_v := \{x \in K \,:\, v(x) > 0\}\,.$$

We call $\mathfrak{p}_v$ the ***valuation ideal*** of v. The quotient $\kappa(v) := \mathcal{O}_v/\mathfrak{p}_v$ is thus a field, called the ***residue field*** of v. It is easy to see that $v(K^*)$ is a subgroup of the additive group $\mathbb{R}$. It is called the ***value group*** of v. If $v(K^*) = 0$ (the trivial group), we say v is ***trivial***.

An exponential valuation v is called ***discrete*** if it is nontrivial and if its value group $v(K^*)$ is a discrete subspace of $\mathbb{R}$ (in the usual Euclidean topology). In this case, $v(K^*) = r\mathbb{Z}$ for some real number $r > 0$. It is called ***normalized*** if $r = 1$. The reader checks easily that our definition of normalized discrete valuation here coincides with the one given in Definition 2.3.8.

When v is discrete, dividing by r we may always pass to a normalized valuation without changing the valuation ring. ■

(3.1.7) Let v be an exponential valuation on a field K. Let $q > 1$ be a real number. Then the map

$$K \longrightarrow \mathbb{R}_{\geq 0}\,, \quad x \longmapsto |x| := q^{-v(x)}$$

is a non-archimedean absolute value on K.

Conversely, if $|\cdot|$ is a non-trivial non-archimedean absolute value on a field K, then the map

$$v(x) = -\log_q |x|\,, \quad \forall\, x \in K$$

is an exponential valuation on K. So exponential valuations are in bijection with non-archimedean absolute values.

We may thus define the *equivalence of exponential valuations* by means of the equivalence of the corresponding absolute values. If an absolute value $|\cdot|$ corresponds to an exponential valuation v, then

$$\mathcal{O}_v = \{x \in K \,:\, |x| \leq 1\} \quad \text{and} \quad \mathfrak{p}_v = \{x \in K \,:\, |x| < 1\}\,.$$

According to Prop. 3.1.5, two exponential valuations on K are equivalent if and only if their valuation rings are the same. In particular, multiplying an exponential valuation by a positive real number gives an equivalent valuation. ■

Recall that for each prime number p, we have a p-adic valuation v_p on $\mathbb{Q}$ (Example 2.3.13 (1)).

Theorem 3.1.8. *Let $|\cdot|$ be a nontrivial absolute value on $\mathbb{Q}$.*

If $|\cdot|$ is archimedean, then it is equivalent to the usual absolute value.

If $|\cdot|$ is non-archimedean, then it is equivalent to the absolute value associated to the p-adic valuation defined by a prime number p.

Proof. See [Neu99, Prop. II.3.7] or [EP05, Prop. 1.2.1 and Thm. 2.1.4]. □

For any field k, any irreducible polynomial $p \in k[t]$ determines a p-adic valuation v_p on the rational function field $k(t)$. On the other hand, we have a degree valuation v_∞ on $k(t)$, which is determined by the formula $v_\infty(f) = -\deg(f)$ for all $f \in k[t]$ (Example 2.3.13 (2)).

Theorem 3.1.9. *Let $K = k(t)$ be a one-variable rational function field. Let v be an exponential valuation on K which is trivial on k.*

Then v is equivalent either to the degree valuation v_∞ or to the p-adic valuation v_p defined by an irreducible polynomial $p \in k[t]$.

Proof. See e.g. [EP05, Thm. 2.1.4]. □

Theorem 3.1.10 (Artin–Whaples, Weak approximation theorem)**.** *Let K be a field and $|\cdot|_1, \ldots, |\cdot|_n$ a finite number of nontrivial independent absolute values on K. Let $x_1, \ldots, x_n \in K$ and $\varepsilon > 0$ a real number.*

Then there exists $x \in K$ such that $|x - x_i|_i < \varepsilon$ for every $i = 1, \ldots, n$.

Proof. Choose $M > 0$ such that $\max\{|x_i|_j \,:\, 1 \le i,\, j \le n\} \le M$. It suffices to find an element $z_i \in K$ for each i such that

$$|z_i - 1|_i < \frac{\varepsilon}{nM} \quad \text{and} \quad |z_i|_j < \frac{\varepsilon}{nM} \ \text{ for all } j \neq i\,,$$

because this implies that the element $x := x_1 z_1 + \cdots + x_n z_n$ has the required property. The problem can be transformed to the problem of finding an element y_i for each i, such that $|y_i|_i > 1 > \max_{j \neq i} |y_i|_j$. Indeed, with y_i in hand, the sequence $\frac{y_i^m}{1+y_i^m}$, $m \in \mathbb{N}$ converges to 1 with respect to $|\cdot|_i$ and to 0 with respect to $|\cdot|_j$ for $j \neq i$.

Without loss of generality, we may assume $i = 1$ and we need to show that there exists $y \in K$ such that

$$|y|_1 > 1 > \max_{2 \le j \le n} |y|_j\,.$$

By Prop. 3.1.5 (ii), we can find $\alpha,\, \beta \in K$ such that

$$|\alpha|_1 < 1 \le |\alpha|_n \quad \text{and} \quad |\beta|_n < 1 \le |\beta|_1\,.$$

Now the element β/α satisfies

$$|\beta/\alpha|_n < 1 < |\beta/\alpha|_1\,.$$

This finishes the proof in the case $n = 2$.

For $n > 2$, by induction we can find $z \in K$ such that

$$|z|_1 > 1 > \max_{2 \le j \le n-1} |z|_j\,.$$

Raising to a sufficient large power if necessary, we may assume that $|z\beta/\alpha|_j < 1$ for $2 \le j \le n-1$. If $|z|_n \le 1$, then we can choose $y = z\beta/\alpha$. Let us suppose $|z|_n > 1$. Then the sequence $t_m := \frac{z^m}{1+z^m}$ tends to 1 with respect to $|\cdot|_1$ and $|\cdot|_n$, and to 0 with respect to $|\cdot|_2, \cdots, |\cdot|_{n-1}$. Hence for m large, the element $t_m\beta/\alpha$ satisfies the required property. □

3.1.2 Completions

Definition 3.1.11. A ***valued field*** is a field K together with an absolute value $|\cdot|$ on K. If $|\cdot|$ is non-archimedean, i.e., associated to an exponential valuation, we also say "***valuation field***" instead of "valued field".

Given two valued fields $(K, |\cdot|)$ and $(K', |\cdot|')$, an ***embedding of valued fields*** from $(K, |\cdot|)$ to $(K', |\cdot|')$ is an injective ring homomorphism $\iota : K \to K'$ such that $|\iota(x)|' = |x|$ for all $x \in K$. When such an embedding is given, we also say that $(K', |\cdot|')/(K, |\cdot|)$, or simply K'/K, is an ***extension of valued fields.***

Note that an embedding of valued fields is always continuous for the topologies defined the absolute values.

A valued field $(K, |\cdot|)$ is called ***complete*** if the metric space it defines is complete, i.e., every Cauchy sequence with respect to the metric defined by $|\cdot|$ is convergent. ■

Definition 3.1.12. Let $(K, |\cdot|)$ be a valued field, V a vector space over K. A ***norm*** on V (with respect to $|\cdot|$) is a map $\|\cdot\| : V \longrightarrow \mathbb{R}$ satisfying the following axioms for all $u, v \in V$ and $\lambda \in K$:

(1) $\|0\| = 0$ and $\|u\| > 0$ if $u \neq 0$.

(2) $\|\lambda u\| = |\lambda| \cdot \|u\|$.

(3) $\|u + v\| \leq \|u\| + \|v\|$.

A norm on V defines a metric on V by taking $\|u - v\|$ as distance.

Two norms $\|\cdot\|_1$ and $\|\cdot\|_2$ on V are called ***equivalent*** if there exist real numbers $C_1, C_2 > 0$ such that $C_1\|u\|_1 \leq \|u\|_2 \leq C_2\|u\|_1$ for all $u \in V$. ■

Proposition 3.1.13. *Let $(K, |\cdot|)$ be a complete valued field and let V be a finite-dimensional vector space over K. Let $v_1, \ldots, v_n$ be a basis of V.*

Then every norm on V (with respect to $|\cdot|$) is equivalent to the maximum norm defined by

$$\|x_1v_1 + \cdots + x_nv_n\| := \max\{\,|x_i|\,\}, \quad \text{for all } x_i \in K\,.$$

In particular, V is complete with respect to any norm and the natural map

$$V \longrightarrow K^n\,; \quad x_1v_1 + \cdots + x_nv_n \longmapsto (x_1, \ldots, x_n)$$

is a homeomorphism.

Proof. See e.g. [Neu99, Prop. II.4.9]. □

Theorem 3.1.14 ([EP05, Thm. 1.1.4])**.** *Let $(K, |\cdot|)$ be a valued field. There exist a complete valued field $(\hat{K}, |\cdot|^\wedge)$ and an embedding of valued fields $\iota : (K, |\cdot|) \to (\hat{K}, |\cdot|^\wedge)$ having the following properties:*

1. *$\iota(K)$ is dense in $\hat{K}$.*
2. *(Universal property) If $\iota' : (K, |\cdot|) \to (K', |\cdot|')$ is another embedding of valued fields with $(K', |\cdot|')$ complete, then there is a unique embedding of valued fields*

$$\varphi : (\hat{K}, |\cdot|^\wedge) \to (K', |\cdot|')$$

such that $\varphi \circ \iota = \iota'$.

Sketch of proof. The construction of $\hat{K}$ is done by the usual process of completion. Namely, we take the ring R consisting of Cauchy sequences of $(K, |\cdot|)$ and let $\mathfrak{m}$ be the maximal ideal consisting of sequences that are convergent to 0. Then we define $\hat{K} = R/\mathfrak{m}$. For any $a = (a_n) \in R$, the extended absolute value is defined by $|a|^\wedge := \lim |a_n|$. The embedding $K \to \hat{K}$ is defined by sending each $x \in K$ to the class of the constant sequence $(x, x, \dots)$. □

The valued field $(\hat{K}, |\cdot|^\wedge)$ in the above theorem is unique up to isomorphism, by the universal property. It is called the ***completion*** of the valued field $(K, |\cdot|)$.

Theorem 3.1.15 (Ostrowski)**.** *Let $(K, |\cdot|)$ be a complete archimedean valued field. Then there is a real number $s \in (0, 1]$ and an isomorphism of valued fields from K onto $(\mathbb{R}, |\cdot|^s)$ or $(\mathbb{C}, |\cdot|^s)$.*

Proof. See e.g. [Neu99, Thm. II.4.2]. □

Remark 3.1.16. By Ostrowski's theorem a complete archimedean valued field $(K, |\cdot|)$ can be identified with $\mathbb{R}$ or $\mathbb{C}$ equipped with the usual absolute value. In particular, for an algebraic extension L of K, there is a unique absolute valuation $|\cdot|_L$ on L that extends the given absolute value of K, it is given by the formula

$$\forall\, \alpha \in L\ ,\ |\alpha|_L := \big(|N_{L/K}(\alpha)|\big)^{1/n} \quad \text{where } n = [L : K]$$

and L is complete with respect to $|\cdot|_L$.

Indeed, the only nontrivial case is $L = \mathbb{C}$ and $K = \mathbb{R}$. Let $|\cdot|_{\mathbb{C}}$ and $|\cdot|_{\mathbb{R}}$ denote the usual absolute values of $\mathbb{C}$ and $\mathbb{R}$. It is well known that $(L, |\cdot|_{\mathbb{C}})$ is complete and that $|z|_{\mathbb{C}} = \sqrt{|z\bar{z}|_{\mathbb{R}}} = \sqrt{|N_{\mathbb{C}/\mathbb{R}}(z)|_{\mathbb{R}}}$. To show the uniqueness of the extension, let $|\cdot|'$ be another absolute value on $\mathbb{C}$ that extends $|\cdot|_{\mathbb{R}}$. Then $\mathbb{C}$ is also complete with respect to $|\cdot|'$ by Prop. 3.1.13. Thus, by Thm. 3.1.15, there is a positive real number $s > 0$ and a field isomorphism $\sigma : \mathbb{C} \to \mathbb{C}$ such that $|z|' = |\sigma(z)|_{\mathbb{C}}^s$ for all $z \in \mathbb{C}$. Notice that σ must be continuous, so it is the identity on $\mathbb{R}$. Thus, either σ is the identity or the complex conjugation. In any case we have $|\sigma(z)|_{\mathbb{C}} = |z|_{\mathbb{C}}$. So we get $|z|' = |z|_{\mathbb{C}}^s$ for all $z \in \mathbb{C}$. Restricting the formula to real numbers shows immediately that $s = 1$. This proves the desired uniqueness.

As we will see later (cf. Thm. 3.2.4), the above unique extension property is also true for a complete non-archimedean absolute value. ■

(3.1.17) We already know (from (3.1.7)) that non-archimedean absolute values correspond naturally to exponential valuations. So we may speak of ***completion*** of an exponential valuation. Let K be a field and let v be an exponential valuation on K with valuation ring A. Let $(\hat{K}, \hat{v})$ be the completion of the valued field (K, v).

The reader checks easily the following facts:

1. Let $\hat{A}$ denote the valuation ring of $\hat{v}$ in $\hat{K}$. Then $\hat{A}$ equals the topological closure of A in $\hat{K}$. We say $\hat{A}$ is the ***completion*** of the discrete valuation ring A. When $A = \hat{A}$ (or equivalently $K = \hat{K}$), we say that A (or v) is ***complete***.

2. The value group and the residue field remain unchanged after completion, i.e., $\hat{v}(\hat{K}^*) = v(K^*)$ and the natural map $A \to \hat{A}$ induces an isomorphism on their residue fields. In particular, if v is discrete (resp. discrete and normalized), then so is $\hat{v}$.

Two most important examples are worth mentioning here. For a prime number p, the completion of $\mathbb{Q}$ with respect to the p-adic valuation is denoted $\mathbb{Q}_p$ and referred to as the field of ***p-adic numbers***. Its valuation ring is denoted $\mathbb{Z}_p$ and called the ***ring of p-adic integers***.

If $K = k(t)$ is a rational function field, the completion of K with respect to the t-adic valuation v_t is the field $k(\!(t)\!)$ of Laurent series in t:

$$k(\!(t)\!) = \left\{ \sum_{n\in\mathbb{Z}} a_n t^n \,\middle|\, a_n \in k \text{ and } a_n = 0 \text{ for all } n \ll 0 \right\}.$$

The corresponding valuation ring is the ring $k[\![t]\!]$ of formal power series. ■

3.2 Henselian valued fields

3.2.1 Hensel's lemma and Newton polygon

Definition 3.2.1. Let $(K, |\cdot|)$ be a non-archimedean valued field with valuation ring $\mathcal{O}_K = \{x \in K : |x| \le 1\}$. Let $\mathfrak{p}$ be the maximal ideal of $\mathcal{O}_K$ and let κ be the residue field.

(1) Let $f(t) = a_0 + a_1 t + \cdots + a_n t^n \in K[t]$ be a polynomial of degree n. We define the ***absolute value*** $|f|$ of f to be the maximum of the absolute values of its coefficients, i.e.,

$$|f| := \max\{\, |a_0|, |a_1|, \ldots, |a_n| \,\}.$$

The polynomial $f(t) \in \mathcal{O}_K[t]$ is called ***primitive*** if $|f| = 1$, or equivalently, if $f(t) \not\equiv 0 \pmod{\mathfrak{p}}$.

(2) We say that K (or $\mathcal{O}_K$) is ***henselian***, if it has the following property: For every primitive polynomial $f(t) \in \mathcal{O}_K[t]$, if the reduction $\bar{f} := f \pmod{\mathfrak{p}}$ admits a factorisation $\bar{f} = \bar{g}\bar{h}$ in $\kappa[t]$ with $\bar{g}$, $\bar{h}$ relatively prime to each other, then f admits a factorisation $f = gh$ in $\mathcal{O}_K[t]$ such that $\bar{g}$, $\bar{h}$ coincide with the reductions of g and h mod $\mathfrak{p}$ respectively and $\deg(g) = \deg(\bar{g})$. ■

Proposition 3.2.2. *Let $(K, |\cdot|)$ be a henselian (non-archimedean) valued field with valuation ring $\mathcal{O}_K$, and let $f(t) = a_0 + a_1 t + \cdots + a_n t^n \in K[t]$ be an irreducible polynomial of degree n.*

Then $|f| = \max\{\, |a_0|, |a_n| \,\}$. In particular, if $a_n = 1$ and $a_0 \in \mathcal{O}_K$, then $f \in \mathcal{O}_K[t]$.

Proof. After multiplying by a suitable element of K^* we may assume that $f \in \mathcal{O}_K[t]$ and $|f| = 1$. Let a_r be the first one among the coefficients $a_0, \cdots, a_n$ such that $|a_r| = 1$. In other words, we have

$$f(t) \equiv t^r (a_r + a_{r+1} t + \cdots + a_n t^{n-r}) \pmod{\mathfrak{p}}.$$

If one had $\max\{|a_0|, |a_n|\} < 1$, then $0 < r < n$ and the above congruence would contradicts the irreducibility of f, according to the henselian hypothesis. □

Proposition 3.2.3. *A complete non-archimedean valued field is henselian.*

Proof. We use the same notation as in Definition 3.2.1. Let $d = \deg(f)$, $m = \deg(\bar{g})$, so that $d - m \geq \deg(\bar{f}) - \deg(\bar{g}) = \deg(\bar{h})$. Let g_0, $h_0 \in \mathcal{O}_K[t]$ be polynomials lifting $\bar{g}$, $\bar{h}$ (i.e. such that $\bar{g} = g_0 \pmod{\mathfrak{p}}$, $\bar{h} = h_0 \pmod{\mathfrak{p}}$), such that $\deg(g_0) = m$ and $\deg(h_0) \leq d - m$. Since $\gcd(\bar{g}, \bar{h}) = 1$ by assumption, we can find polynomials $a(t)$, $b(t) \in \mathcal{O}_K[t]$ such that $ag_0 + bh_0 \equiv 1 \pmod{\mathfrak{p}}$. Among the coefficients of the two polynomials $f - g_0h_0$ and $ag_0 + bh_0 - 1$ whose coefficients all lie in $\mathfrak{p}$, we can pick one with minimal valuation and call it π. Then

$$\{\text{coefficients of } f - g_0h_0\} \cup \{\text{coefficients of } ag_0 + bh_0 - 1\} \subseteq \pi\mathcal{O}_K\,.$$

Now for each $n \geq 1$ we construct two polynomials of the form

$$g_{n-1} = g_0 + p_1\pi + \cdots + p_{n-1}\pi^{n-1}\,,\ h_{n-1} = h_0 + q_1\pi + \cdots + q_{n-1}\pi^{n-1}$$

where p_i, $q_i \in \mathcal{O}_K[t]$ satisfy $\deg(p_i) < m = \deg(g_0)$ and $\deg(q_i) \leq d - m$, such that

$$f \equiv g_{n-1}h_{n-1} \pmod{\pi^n\mathcal{O}_K}\,.$$

Once the sequences $(g_{n-1})_{n\geq 1}$ and $(h_{n-1})_{n\geq 1}$ are constructed, taking $g := \lim_{n\to\infty} g_{n-1}$ and $h := \lim_{n\to\infty} h_{n-1}$ finishes the proof. (Here g_{n-1} and h_{n-1} lie in the finite-dimensional space $K[t]_{\leq d}$ of polynomials of degree $\leq d$. So limits of polynomials sequences can be defined by taking limits of the finitely many sequences of coefficients.)

To fulfill the construction, we assume by induction that g_{n-1} and h_{n-1} have been constructed for some $n \geq 1$. We need to find polynomials p_n, $q_n \in \mathcal{O}_K[t]$ with degree bounded by $m - 1$ and $d - m$ respectively, such that $g_n := g_{n-1} + p_n\pi^n$ and $h_n := h_{n-1} + q_n\pi^n$ satisfy the congruence relation $f \equiv g_nh_n \pmod{\pi^{n+1}\mathcal{O}_K}$, which is equivalent to

$$f - g_{h-1}h_{n-1} \equiv (g_{n-1}q_n + h_{n-1}p_n)\pi^n \pmod{\pi^{n+1}\mathcal{O}_K}\,.$$

Dividing by π^n, this means

$$g_{n-q}q_n + h_{n-1}p_n \equiv g_0q_n + h_0p_n \equiv f_n \pmod{\pi\mathcal{O}_K}\,,$$

where $f_n := \pi^{-n}(f - g_{n-1}h_{n-1}) \in \mathcal{O}_K[t]$. Since $ag_0 + bh_0 \equiv 1 \pmod{\pi\mathcal{O}_K}$, one has $g_0(af_n) + h_0(bf_n) \equiv f_n \pmod{\pi\mathcal{O}_K}$. At this point we would like to put $p_n = af_n$ and $q_n = bf_n$, but the degrees might be too big. The remedy is to notice that the leading coefficient of g_0 is a unit since $\deg(g_0) = m = \deg(\bar{g}_0)$ by the choice. Thus, by the Euclidean division algorithm, we can write

$$bf_n = qg_0 + p_n \quad \text{with } q,\ p_n \in \mathcal{O}_K \text{ and } \deg(p_n) < m = \deg(g_0)\,.$$

We have $g_0(af_n + h_0q) + h_0p_n = g_0af_n + h_0bf_n \equiv f_n \pmod{\pi\mathcal{O}_K}$. Now removing monomials with coefficients divisible by π from the polynomial $af_n + h_0q$, we get a polynomial q_n such that $g_0q_n + h_0p_n \equiv f_n \pmod{\pi\mathcal{O}_K}$, and by the choice, q_n has no coefficients divisible by π. In particular, $\deg(q_n) = \deg(\tilde{q}_n)$, where $a \mapsto \tilde{a}$ denotes the reduction mod π.

Note that $\deg(\tilde{f}_n) \leq \deg(f_n) \leq d = \deg(f)$, $\deg(\tilde{g}_0) = m$ (since the leading coefficient of g_0 is a unit) and

$$\deg(\tilde{h}_0\tilde{p}_n) \leq \deg(h_0 p_n) \leq d - m + \deg(p_n) < d - m + m = d\,.$$

So we have

$$\deg(q_n) = \deg(\tilde{q}_n) = \deg(\tilde{g}_0\tilde{q}_n) - m = \deg(\tilde{f}_n - \tilde{h}_0\tilde{p}_n) - m \leq d - m\,.$$

This completes the proof. □

Theorem 3.2.4. *Let $(K, |\cdot|)$ be a henselian (non-archimedean) valued field and let L/K be an algebraic field extension.*

1. *The absolute value $|\cdot|$ of K may be extended in a unique way to an absolute value $|\cdot|_L$ on L.*

   Moreover, if L/K is a finite extension, then the extended absolute value is given by the formula

   $$\forall\, \alpha \in L\,, \quad |\alpha|_L = \big(|N_{L/K}(\alpha)|\big)^{1/n} \quad \text{where } n = [L:K]\,.$$

   If L/K is finite and $(K, |\cdot|)$ is complete, then $(L, |\cdot|_L)$ is also complete.

2. *Two elements of L with the same minimal polynomial over K have the same absolute value.*

3. *If $\mathcal{O}_K$ and $\mathcal{O}_L$ denote the valuation ring of $|\cdot|$ in K and the valuation ring of $|\cdot|_L$ in L respectively, then $\mathcal{O}_L$ is the integral closure of $\mathcal{O}_K$ in L.*

Proof. For (1), see [Neu99, Thms. II.4.8 and II.6.2].

(2) Suppose α, $\alpha' \in L$ have the same minimal polynomial over K. Then there exists a K-automorphism $\sigma : \overline{K} \to \overline{K}$ such that $\alpha' = \sigma\alpha$. If $|\cdot|_{\overline{K}}$ denotes the unique extension to $\overline{K}$, then it is equal to $|\sigma(\cdot)|_{\overline{K}}$ because the latter is also an extension of $|\cdot|_K$. So we have

$$|\alpha'|_L = |\alpha'|_{\overline{K}} = |\sigma(\alpha)|_{\overline{K}} = |\alpha|_{\overline{K}} = |\alpha|_L\,.$$

(3) Let $\alpha \in L$. We need to show that $|\alpha|_L \leq 1$ if and only if α is integral over $\mathcal{O}_K$. Replacing L with $K(\alpha)$ if necessary, we may assume that $L = K(\alpha)$. In particular, L/K is finite.

If $\alpha \in L$ is integral over $\mathcal{O}_K$, then $N_{L/K}(\alpha) \in \mathcal{O}_K$ by Prop. 2.1.11 (as an easy exercise, the reader proves that $\mathcal{O}_K$ is integrally closed). Hence $|\alpha|_L \leq 1$ by the formula in (1), showing that $\alpha \in \mathcal{O}_L$. Conversely, suppose $\alpha \in \mathcal{O}_L$ and let $f(t) \in K[t]$ be the monic minimal polynomial of α over K. Then

$$|f(0)|_K = \big|\pm N_{L/K}(\alpha)\big|_K = |\alpha|_L^{[L:K]} \leq 1\,.$$

By Prop. 3.2.2, we have $f \in \mathcal{O}_K[t]$. Hence α is integral over $\mathcal{O}_K$. □

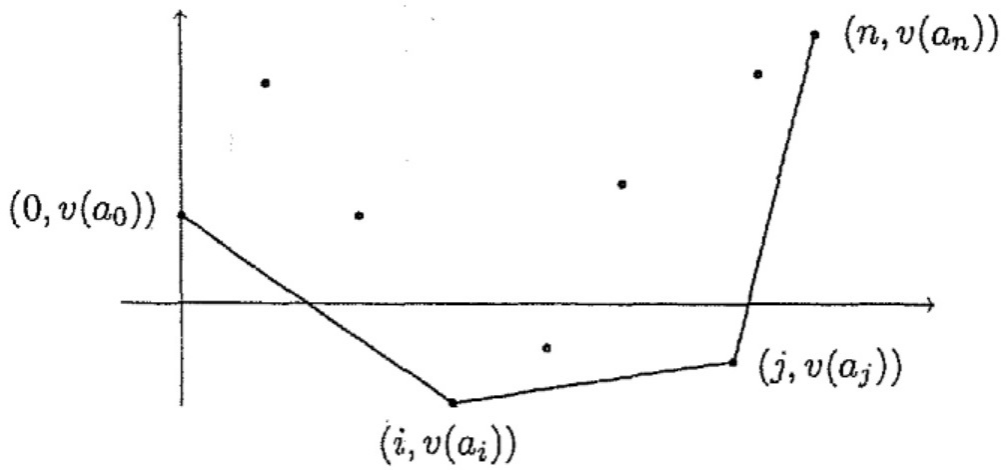
(3.2.5) In fact, the unique extendability to algebraic extensions characterizes henselian valuation fields. In order to prove this, we appeal to a method which allows us to express the valuations of the roots of a polynomial in terms of the valuations of the coefficients. It relies on the notion of *Newton polygon* which arises as follows. Let v be an exponential valuation on a field K. Let

$$f(t) = a_0 + a_1 t + \cdots + a_n t^n \in K[t]$$

be a polynomial such that $a_0 a_n \neq 0$. To each term $a_i t^i$ we associate a point $(i,\, v(a_i)) \in \mathbb{R}^2$, ignoring however the point $(i,\, +\infty)$ if $a_i = 0$. We now take the lower convex envelope of the set of points

$$\{\, (0,\, v(a_0)),\, (1,\, v(a_1)) \,, \ldots, (n,\, v(a_n)) \,\}\,.$$

This produces a polygonal chain which is called the ***Newton polygon*** of f.



The polygon consists of a sequence of line segments whose slopes are strictly increasing. ■

Example 3.2.6. Let $K = \mathbb{F}_p(\!(x)\!)$ and let $f(t) = t^p - x$. By definition, the Newton polygon of f consists of one single segment, joining the point $(0,\, 1)$ to $(p,\, 0)$.

Note that the splitting field of f is $L = K(\sqrt[p]{x})$. Counted with multiplicities, f has p roots $\alpha_1 = \cdots = \alpha_p = \sqrt[p]{x}$ in L, and $w(\alpha_i) = w(\sqrt[p]{x}) = \frac{1}{p} v(N_{L/K}(\sqrt[p]{x})) = \frac{1}{p}$, where w denotes the unique extension to L of the t-adic valuation of K. ■

Proposition 3.2.7. *Let v be an exponential valuation on a field K and let*

$$f(t) = a_0 + a_1 t + \cdots + a_n t^n \in K[t]$$

be a polynomial such that $a_0 a_n \neq 0$. Let w be an extension of v to the splitting field L of f over K.

Suppose that two points $P(r,\, v(a_r))$, $Q(s,\, v(a_s))$, where $0 \leq r \leq s \leq n$, are the endpoints of a line segment of slope $-k \in \mathbb{R}$ occurring in the Newton polygon of f.

Then f has precisely $s-r$ roots $\alpha_1, \ldots, \alpha_{s-r}$ satisfying

$$w(\alpha_1) = \cdots = w(\alpha_{s-r}) = k\,.$$

Here the multiplicities of roots are counted so that $\alpha_1, \ldots, \alpha_{s-r}$ may not be distinct one to another.

Proof. Dividing by a_n only shifts the polygon up or down. We may thus assume $a_n = 1$. We number the roots $\alpha_1, \ldots, \alpha_n \in L$ of f in such a way that

$$\begin{aligned} w(\alpha_1) = \cdots = w(\alpha_{s_1}) &= m_1 \\ w(\alpha_{s_1+1}) = \cdots = w(\alpha_{s_2}) &= m_2 \\ \cdots \quad \cdots \quad \cdots \quad \cdots & \\ w(\alpha_{s_d+1}) = \cdots = w(\alpha_n) &= m_{d+1} \end{aligned}$$

where $m_1 < m_2 < \cdots < m_{d+1}$. Viewing the coefficients a_i as elementary symmetric functions of the roots α_j, we immediately find that

$$\begin{aligned} v(a_n) &= v(1) = 0 \\ v(a_{n-1}) &\geq \min_i \{\, w(\alpha_i) \,\} = m_1 \\ v(a_{n-2}) &\geq \min_{i,\,j} \{\, w(\alpha_i \alpha_j) \,\} = 2m_1 \\ \cdots \quad \cdots \quad \cdots \quad \cdots & \\ v(a_{n-s_1}) &= \min_{i_1,\ldots,i_{s_1}} \{\, w(\alpha_{i_1} \cdots \alpha_{i_{s_1}}) \,\} = s_1 m_1\,, \end{aligned}$$

the latter because the valuation of the term $\alpha_1 \cdots \alpha_{s_1}$ is smaller than that of all the others,

$$\begin{aligned} v(a_{n-s_1-1}) &\geq \min_{i_1,\ldots,i_{s_1+1}} \{\, w(\alpha_{i_1} \cdots \alpha_{i_{s_1+1}}) \,\} = s_1 m_1 + m_2 \\ v(a_{n-s_1-2}) &\geq \min_{i_1,\ldots,i_{s_1+2}} \{\, w(\alpha_{i_1} \cdots \alpha_{i_{s_1+2}}) \,\} = s_1 m_1 + 2m_2 \\ v(a_{n-s_1-3}) &\geq \min_{i_1,\ldots,i_{s_1+3}} \{\, w(\alpha_{i_1} \cdots \alpha_{i_{s_1+3}}) \,\} = s_1 m_1 + 3m_2 \\ \cdots \quad \cdots \quad \cdots \quad \cdots & \\ v(a_{n-s_2}) &= \min_{i_1,\ldots,i_{s_1}} \{\, w(\alpha_{i_1} \cdots \alpha_{i_{s_2}}) \,\} = s_1 m_1 + (s_2 - s_1) m_2\,, \end{aligned}$$

and so on. From this result one concludes that the vertices of the Newton polygon, from right to left, are given by

$$(n,\, 0)\,,\ (n - s_1,\, s_1 m_1)\,,\ (n - s_2,\, s_1 m_1 + (s_2 - s_1) m_2)\,, \ldots$$

The slope of the extreme right-hand line segment is

$$\frac{0 - s_1 m_1}{n - (n - s_1)} = -m_1\,,$$

and proceeding further to the left,

$$\frac{(s_1m_1 + \cdots + (s_j - s_{j-1})m_j) - (s_1m_1 + \cdots + (s_{j+1} - s_j)m_{j+1})}{(n - s_j) - (n - s_{j+1})} = -m_{j+1}\,.$$

This completes the proof. □

Corollary 3.2.8. *Let K, v, f and so on be as in Proposition 3.2.7. Suppose that the Newton polygon of f consists of precisely r segments of slopes*

$$-m_r < \cdots < -m_1\,.$$

Then the factorisation of f over the splitting L is given by

$$f(t) = a_n \prod_{i=1}^{r} f_i(t)\,, \quad \text{where} \quad f_i(t) = \prod_{w(\alpha_j)=m_i} (t - \alpha_j)\,.$$

Here the factor $f_i(t)$ corresponds to the $(r - i + 1)$-th segment, whose slope is $-m_i$.

In particular, the Newton polygon of f consists of exactly one segment if and only if the roots of f all have the same valuation.

Proposition 3.2.9. *With notation as in Prop. 3.2.7, suppose that the valuation v admits a unique extension w to the splitting field L of f (e.g. K is henselian).*

Then in the factorization

$$f(t) = a_n \prod_{i=1}^{r} f_i(t)\,, \quad \text{where} \quad f_i(t) = \prod_{w(\alpha_j)=m_i} (t - \alpha_j)\,,$$

we have $f_i(t) \in K[t]$ for every $i \in [\![1, r]\!]$.

In particular, if f is irreducible over K, then its Newton polygon consists of a single segment.

Proof. We may clearly assume $a_n = 1$.

First assume that f is irreducible over K. Then for every $i \in [\![1, r]\!]$, there is an automorphism σ_i of the normal extension L/K such that $\sigma_i\alpha_1 = \alpha_i$. So as in the proof of Thm. 3.2.4 (2), we get $w(\alpha_i) = w(\alpha_1)$. Thus, by Cor. 3.2.8, we have $r = 1$ and hence $f_1 = f \in K[t]$.

The general case follows by induction on $n = \deg(f)$. Let $p(t) \in K[t]$ be the monic minimal polynomial of α_1 over K and $g := f/p \in K[t]$. All the roots of $p(t)$ have the same valuation m_1 by the previous paragraph. So $p(t)$ is a divisor of $f_1(t)$. Let $g_1 := f_1/p \in K[t]$. The factorization of g according to the slopes of line segments in its Newton polygon is

$$g(t) = g_1(t) \prod_{i=2}^{r} f_i(t)\,.$$

Since $\deg(g) < \deg(f)$, it follows from the induction hypothesis that $f_j(t) \in K[t]$ for all $j = 1, \cdots, r$. □

Theorem 3.2.10. *A non-archimedean valued field (K, v) is henselian if and only if the valuation v can be extended uniquely to every algebraic extension of K.*

Therefore, any algebraic extension of a henselian valued field is again henselian.

Proof. See e.g. [Neu99, Thm. II.6.6]. □

Remark 3.2.11. In contrast to the henselian property, completeness of valued fields does not pass to infinite algebraic extensions.

In fact, it can be shown that if (K, v) is complete nontrivially valued field, then every infinite separable algebraic extension L/K is not complete, and the algebraic closure $\overline{K}$ is not complete if it is an infinite extension over K. ■

We have introduced henselian fields by a condition of which the reader will find weaker versions in the literature, restricted to *monic polynomials* only. Both are equivalent as is shown by the following result.

Proposition 3.2.12. *Let v be an exponential valuation on a field K, $\mathcal{O}_v$ its valuation ring, and $\kappa = \kappa(v)$ the residue field.*

Then (K, v) is henselian if and only if **Hensel's lemma** *holds for $\mathcal{O}_v$, namely, for every* **monic** *polynomial $f \in \mathcal{O}_v[t]$, if*

$$\bar{f} = \bar{g} \cdot \bar{h} \ \in \ \kappa[t]$$

for some relatively prime monic polynomials $\bar{g}\,, \bar{h} \in \kappa[t]$, then there are monic polynomials g, $h \in \mathcal{O}_v[t]$ such that

$$f = gh \in \mathcal{O}_v[t] \quad \text{and } g,\ h \text{ are liftings of } \bar{g},\ \bar{h} \text{ respectively}.$$

Proof. See e.g. [Neu99, Prop. II.6.7]. □

3.2.2 Krasner's lemma

Throughout this subsection, let $(K, |\cdot|)$ be a henselian (non-archimedean) valued field. Let $\overline{K}$ be an algebraic closure of K and denote the naturally extended absolute on $\overline{K}$ again by $|\cdot|$.

Lemma 3.2.13. *Let f, $g \in K[t]$ be* **monic** *polynomials of the same degree $n \geq 1$. Let $\alpha \in \overline{K}$ be a root of f.*

Then for any real number $\varepsilon > 0$, there exits a real number $\delta > 0$ such that

$$(|g - f| < \delta) \implies (g \text{ has a root } \beta \in \overline{K} \text{ satisfying } |\alpha - \beta| < \varepsilon\,).$$

Proof. Put $h = g - f$. Then $\deg(h) \leq n - 1$ and $|h(\alpha)| \leq |h| \max_{0 \leq i \leq n-1} |\alpha|^i$. Choose $\delta > 0$ such that

$$\delta \cdot \max_{0 \leq i \leq n-1} |\alpha|^i < \varepsilon^n\,.$$

Then $|h| < \delta$ implies $|g(\alpha)| = |g(\alpha) - f(\alpha)| = |h(\alpha)| < \varepsilon^n$. Let $g(t) = \prod_{i=1}^{n}(t - \beta_i)$ be the decomposition of g in $\overline{K}$ (with β_i not necessarily distinct). Then

$$\prod_{i=1}^{n} |\alpha - \beta_i| = |g(\alpha)| < \varepsilon^n\,.$$

This implies $|\alpha - \beta_i| < \varepsilon$ for some i. □

Proposition 3.2.14. *Let $(K, |\cdot|)$ be a henselian non-archimedean valued field and let $f \in K[t]$ be a monic polynomial. Assume that f is separable.*

Then there exists a real number $\delta > 0$ having the following property: For every monic polynomial $g \in K[t]$ with $\deg(g) = \deg(f)$, if $|g - f| < \delta$, then g is separable and for any root α of f, the polynomial g has a root β satisfying

$$|\beta - \alpha| < \min_{\alpha'} |\alpha' - \alpha| ,$$

where α' runs over the roots of f distinct from α.

One says that β **belongs to** *α and observes that $|\beta - \alpha'| = |\alpha - \alpha'|$ for every α'.*

Proof. Put

$$\varepsilon := \min\{\, |\alpha - \alpha'| \,:\, (\alpha, \alpha') \text{ is a pair of distinct roots of } f \,\} .$$

By Lemma 3.2.13, there exists $\delta > 0$ such that whenever g is monic of the same degree as f and $|g - f| < \delta$, g has a root belonging to α for every root of f. In particular, putting $n = \deg(g) = \deg(f)$, we obtain n roots of g which must be distinct in view of the choice of ε. This implies that g is separable. □

Theorem 3.2.15 (Krasner's lemma)**.** *Let $\alpha, \beta \in \overline{K}$ and assume that α is separable over $K(\beta)$ (e.g. α is separable over K) and let $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ be the conjugates of α over K.*

If $|\beta - \alpha| < \min_{2 \le i \le n} |\alpha_i - \alpha|$, then $K(\alpha) \subseteq K(\beta)$.

Proof. Suppose that $|\beta - \alpha| < \min_{2 \le i \le n} |\alpha_i - \alpha|$. Consider the separable extension $K(\alpha, \beta)/K(\beta)$. It suffices to show that for every $\sigma \in \mathrm{Gal}(\overline{K}/K(\beta))$, $\sigma(\alpha) = \alpha$. By the uniqueness of the extension of the absolute value, we have

$$|\beta - \sigma\alpha| = |\sigma(\beta - \alpha)| = |\beta - \alpha| < |\alpha_i - \alpha| , \quad \forall\, i \ge 2 .$$

Therefore,

$$|\alpha - \sigma\alpha| < \max\{\, |\alpha - \beta| , |\beta - \sigma| \,\} < |\alpha_i - \alpha| , \quad \forall\, i \ge 2 .$$

Since $\sigma(\alpha) \in \{\alpha_1, \cdots, \alpha_n\}$, it follows that $\sigma(\alpha) = \alpha$ as desired. □

The following is a strengthening of Prop. 3.2.14 for irreducible polynomials.

Corollary 3.2.16. *Let $f \in K[t]$ be a monic irreducible separable polynomial.*

Then there exists a real number $\delta > 0$ having the following property: For every monic polynomial $g \in K[t]$ with $\deg(g) = \deg(f)$, if $|g - f| < \delta$, then g is irreducible and separable and for any root α of f, the polynomial g has a root β belonging to α and $K(\alpha) = K(\beta)$.

Proof. First, g admits a root β belonging to α by Prop. 3.2.14. We have $K(\alpha) \subseteq K(\beta)$ by Krasner's lemma. Thus,

$$\deg(f) = [K(\alpha) : K] \le [K(\beta) : K] \le \deg(g) = \deg(f) .$$

It follows that $[K(\beta) : K] = \deg(g)$, hence g is irreducible. □

3.2.3 Extensions of absolute values

Having seen that henselian absolute values extend uniquely to algebraic extensions, we will now study the question of how an arbitrary absolute value of a field extends to an algebraic extension in general.

(3.2.17) Let K be a field and let v be an arbitrary archimedean or non-archimedean absolute value on K. There is a little discrepancy in notation here, because the letter v has hitherto been used for non-archimedean exponential valuations. In spit of this, it will prove advantageous, and agrees with current usage, to employ the letter v simultaneously for both notions to denote the corresponding multiplicative absolute value in both cases by $|\cdot|_v$. Where confusion lurks, we will supply clarifying remarks.

The completion of K with respect to $|\cdot|_v$ will be denoted by K_v, and we fix an algebraic closure $\overline{K_v}$ of K_v. (Warning: $\overline{K_v}$ is not complete if v is non-archimedean!) The canonical extension of v to K_v is again denoted by v and the unique extension of this latter to $\overline{K_v}$ by $\bar{v}$. ■

(3.2.18) With notation as in (3.2.17), let L/K be an algebraic extension. Choosing a K-embedding $\tau : L \to \overline{K_v}$, we obtain by restriction of $\bar{v}$ to τL an extension $w = \bar{v} \circ \tau$ of the valuation v to L. In other words, if v, resp. $\bar{v}$, are given by the absolute values $|\cdot|_v$, resp. $|\cdot|_{\bar{v}}$, on K, K_v, resp. $\overline{K_v}$, where $|\cdot|_{\bar{v}}$ extends precisely the absolute value $|\cdot|_v$ of K_v, then we obtain on L the absolute value

$$|x|_w := |\tau x|_{\bar{v}}\,.$$

The mapping $\tau : L \to \overline{K_v}$ is thus an embedding of valued fields.

We define

$$L_{(w)} := \bigcup_M M_w \tag{3.2.18.1}$$

where M runs over finite subextensions M/K of L/K and M_w denotes the w-adic completion of M. This union will be henceforth called the ***localization*** of L with respect to w. We claim that the given K-embedding $\tau : L \to \overline{K_v}$ extends in a unique way to a continuous K_v-embedding

$$\tau \;:\; L_{(w)} \longrightarrow \overline{K_v}\,.$$

In particular, this shows that $L_{(w)}/K_v$ is an algebraic extension.

Indeed, when M/K is a finite extension, we can define the extended map $\tau : M_w \to \overline{K_v}$ by the rule

$$x \longmapsto \bar{v}\text{-adic limit of } \big(\tau(x_n)\big) \qquad \text{if } x \text{ is the } w\text{-adic limit of } (x_n)\,.$$

Here, when (x_n) is a w-adic Cauchy sequence in M, (τx_n) is clearly a $\bar{v}$-adic Cauchy sequence in the finite complete extension $\tau M.K_v$ of K_v. As the latter field is complete by Thm. 3.2.4 (3), the $\bar{v}$-adic limit of τx_n does exist in $\tau M.K_v$ (hence also in $\overline{K_v}$). So the above definition is meaningful.

We consider the diagram of fields

(3.2.18.2)
$$\begin{array}{ccc} L & \longrightarrow & L_{(w)} \\ | & & | \\ K & \longrightarrow & K_v \end{array}$$

The canonical extension of w from L to $L_{(w)}$ is precisely the unique extension of v from K_v to the algebraic extension $L_{(w)}/K_v$. We have

$$L_{(w)} = L.K_v \text{ or more precisely } \tau L_{(w)} = \tau L.K_v \quad \text{inside } \overline{K_v},$$

because if M/K is a finite subextension of L/K, then $M.K_v$ is a complete subfield of M_w containing M, so it has to be equal to the completion M_w.

If $[L_{(w)} : K_v] =: n_v < +\infty$, then the absolute values corresponding to v and w satisfy the relation

$$|x|_w = \left(N_{L_{(w)}/K_v}(x)\right)^{1/n_v}.$$

The field diagram (3.2.18.2) is of cental importance for algebraic number theory. It shows the passage from the "global extension" L/K to the "local extension" $L_{(w)}/K_v$ and thus represents one of the most important methods of algebraic number theory, the so-called "***local-global principle***". This terminology arises from the case of a function field K, for example $K = \mathbb{C}(t)$, where the elements of the extension L are algebraic functions on a Riemann surface, hence on a *global* object, whereas passing to K_v and $L_{(w)}$ signifies looking at power series expansions, i.e., the study of *local* behaviours of functions. ■

Corollary 3.2.19. *With notation as in (3.2.18), if L/K is a separable algebraic (resp. Galois, resp. finite) extension, then so is $L_{(w)}/K_v$.*

Proof. We have seen that $L_{(w)}$ is a compositum of L and K_v inside $\overline{K_v}$. □

Definition 3.2.20. By a *p-**adic field*** (or *p-**adic number field***), where p is a prime number, we mean a finite extension of the field $\mathbb{Q}_p$. If F is a p-adic field, the natural extension of the p-adic valuation of $\mathbb{Q}_p$ to F will be referred to as the *p-**adic valuation*** on F. With this valuation F is a complete non-archimedean valued field. ■

Proposition 3.2.21. *Let F be a p-adic field. There exists a number field K contained in F such that $[K : \mathbb{Q}] = [F : \mathbb{Q}_p]$, $F = K.\mathbb{Q}_p$ and F is the completion of K with respect to the p-adic valuation.*

Proof. Let $F = \mathbb{Q}_p(\alpha)$, let $f \in \mathbb{Q}_p[t]$ be the minimal polynomial of α over $\mathbb{Q}_p$ and take a monic polynomial $g \in \mathbb{Q}[t]$ very close to f as in Cor. 3.2.16. Then g is irreducible over $\mathbb{Q}_p$ and a fortiori over $\mathbb{Q}$. Let $\beta \in \overline{\mathbb{Q}_p}$ be a root of g belonging to α. Then $\mathbb{Q}_p(\beta) = \mathbb{Q}_p(\alpha)$. Since g has coefficients in $\mathbb{Q}$, $K := \mathbb{Q}(\beta)$ is a number field with $[K : \mathbb{Q}] = \deg(g) = \deg(f) = [F : \mathbb{Q}_p]$. The other assertions follow from the discussions in (3.2.18). □

Remark 3.2.22. An analog of Prop. 3.2.21 holds for a finite *separable* extension of $\mathbb{F}_p((t))$, as the same argument shows. More precisely, if F is a finite separable extension of $\mathbb{F}_p((t))$, there exists a finite separable extension K of $\mathbb{F}_p(t)$ such that $[K : \mathbb{F}_p(t)] = [F : \mathbb{F}_p((t))]$, $F = K.\mathbb{F}_p((t))$ and F is the t-adic completion of K. ■

(3.2.23) With notation as in (3.2.17), let L/K be an algebraic extension. We saw that every K-embedding $\tau : L \to \overline{K_v}$ gave us an extension $w = \bar{v} \circ \tau$ of v. For every field automorphism $\sigma \in \mathrm{Gal}(\overline{K_v}/K_v)$, the composition

$$L \xrightarrow{\tau} \overline{K_v} \xrightarrow{\sigma} \overline{K_v}$$

yields a new K-embedding $\tau' = \sigma \circ \tau$ of L. We say that τ' is ***conjugate to*** τ over K_v.

Note that the composite $\bar{v} \circ \tau'$ also extends the extension v of K. But it does not provide a new extension, because $\bar{v} \circ \sigma = \bar{v}$ by the uniqueness of the extension of v from K_v to $\overline{K_v}$. ■

The following result gives us a complete description of the possible extensions of v to L (noticing that v may denote an archimedean absolute value here).

Theorem 3.2.24. *With notation as in* (3.2.23)*, one has:*

1. *Every extension w of the valuation v to L arises as the composite $w = \bar{v} \circ \tau$ for some K-embedding $\tau : L \to \overline{K_v}$.*
2. *Two extensions $\bar{v} \circ \tau$ and $\bar{v} \circ \tau'$ are equal if and only if τ and τ' are conjugate over K_v.*

Proof. See e.g. [Neu99, p.161, Thm. II.8.1]. □

For a simple algebraic extension, we have the following concrete variant of Theorem 3.2.24.

Proposition 3.2.25. *Let K, v and so on be as in* (3.2.17)*, and let $L = K(\alpha)$ be a finite extension generated by a root α of a monic irreducible polynomial $f \in K[t]$. Let*

$$f(t) = \prod_{i=1}^{r} f_i(t)^{m_i}$$

be the irreducible decomposition of f over the completion K_v.

Then v has precisely r extensions $w_1, \ldots, w_r$ to L, with w_i explicitly obtained from the factor f_i as follows: Let $\alpha_i \in \overline{K_v}$ be a root of f_i and let

$$\tau_i \ : \ L \to \overline{K_v}\,, \quad \alpha \longmapsto \alpha_i$$

be the corresponding K-embedding of L into $\overline{K_v}$. Then one has $w_i = \bar{v} \circ \tau_i$.

Moreover, τ_i extends to an isomorphism $\tau_i : L_{w_i} \xrightarrow{\sim} K_v(\alpha_i)$ on the completion L_{w_i} of L with respect to w_i.

Proof. This is easily deduced from Theorem 3.2.24 because two embeddings τ, τ' of L into $\overline{K_v}$ are K_v-conjugate if and only if $\tau(\alpha)$ and $\tau'(\alpha)$ are conjugate over K_v, i.e., if they are zeroes of the same irreducible factor f_i. □

(3.2.26) With notation as before, let L/K be a finite extension. We will write $w \,|\, v$ to indicate that w is an extension of v to L. For a fixed v, there are only finitely many extensions w of v by Thm. 3.2.24.

For each $w \,|\, v$, the inclusion of L into its w-adic completion L_w induces a natural map

$$L \otimes_K K_v \longrightarrow L_w\,; \quad a \otimes b \longmapsto ab\,.$$

It is easy to see that this map is a homomorphism both as K_v-algebras and as L-algebras. We have thus a natural map

$$\varphi \,:\, L \otimes_K K_v \longrightarrow \prod_{w \,|\, v} L_w\ ,$$

which is a homomorphism of K_v-algebras and a homomorphisms of L-algebras. ■

The following result is immediate.

Proposition 3.2.27. *Let (K, v) be a valued field and let L/K be a finite extension. Assume that the canonical homomorphism φ in (3.2.26) is an isomorphism.*

Then

$$[L : K] = \sum_{w|v} [L_w : K_v]\,, \tag{3.2.27.1}$$

and for every $x \in L$, the characteristic polynomial of the multiplication-by-x map on L is the product of the characteristic polynomials of the same map on the L_w. In particular,

$$N_{L/K}(x) = \prod_{w|v} N_{L_w/K_v}(x) \quad \textit{and} \quad \mathrm{Tr}_{L/K}(x) = \sum_{w|v} \mathrm{Tr}_{L_w/K_v}(x) \tag{3.2.27.2}$$

as elements in K_v.

Proposition 3.2.28. *Let (K, v) be a valued field and let L/K be a finite separable extension.*

Then the natural homomorphism

$$\varphi \,:\, L \otimes_K K_v \longrightarrow \prod_{w \,|\, v} L_w$$

is an isomorphism. In particular, (3.2.27.1) and (3.2.27.2) hold.

Proof. By the primitive element theorem, $L = K(\alpha)$ for some $\alpha \in L$. Let $f \in K[t]$ be the minimal polynomial of α over K. By Prop. 3.2.25, to each $w \,|\, v$ there corresponds an irreducible factor f_w of f in $K_v[t]$, and thanks to the separability, we have $f = \prod_{w \,|\, v} f_w$ in $K_v[t]$. Consider all the L_w as embedded into $\overline{K_v}$ and denote by α_w the image of α

under the embedding $L \to \overline{K_v}$. Then we have $L_w = K_v(\alpha_w)$ and f_w is the minimal polynomial of α_w over K_v. So we have the following commutative diagram

$$\begin{array}{ccc} K_v[t]/(f(t)) & \longrightarrow & \prod_{w\,|\,v} K_v[t]/(f_w(t)) \\ \downarrow & & \downarrow \\ L \otimes_K K_v & \xrightarrow[\varphi]{} & \prod_{w\,|\,v} L_w \end{array}$$

where the top row is an isomorphism by the Chinese remainder theorem. The left vertical map is induced by $t \mapsto \alpha \otimes 1$ and is an isomorphism since $K[t]/(f) \cong L = K(\alpha)$. The vertical arrow on the right is induced by $t \mapsto \alpha_w$ and is an isomorphism for similar reasons. Hence the bottom arrow in the diagram is also an isomorphism. □

Remark 3.2.29. In the context of (3.2.26), the map φ is not necessarily bijective in general. However, it can be shown that it is always surjective and that $\mathrm{Ker}(\varphi)$ is the Jacobson radical of the ring $L \otimes_K K_v$ (see e.g. [Bou06, § VI.8.2, Prop. 2]). Notice also that since $L \otimes_K K_v$ is a finite dimensional algebra over a field, its Jacobson radical is the same as its nilpotent radical. Hence, φ is an isomorphism if and only if the ring $L \otimes_K K_v$ is reduced. ■

(3.2.30) Now suppose (K, v) is non-archimedean with valuation ring $\mathcal{O}_v \subseteq K$ and residue field $\kappa(v)$. Let L/K be an algebraic extension. Let w be a valuation of L extending v, with valuation ring $\mathcal{O}_w \subseteq L$ and residue field $\kappa(w)$. The ***ramification index*** $e(w|v)$ of $w|v$ is defined as the index of the subgroup $v(K^*)$ in $w(L^*)$, i.e.,

$$e(w|v) := [w(L^*) : v(K^*)] \in \mathbb{N}^* \cup \{+\infty\}\,.$$

The ***residue degree*** or the ***inertia degree*** $f(w|v)$ of $w \,|\, v$ is defined as the degree of the residue field extension $\kappa(w)/\kappa(v)$, i.e.,

$$f(w|v) := [\kappa(w) : \kappa(v)] \in \mathbb{N}^* \cup \{+\infty\}\,.$$

Since the value group and the residue field do not change when passing to completions (as we have mentioned in (3.1.17)), if $\hat{v}$ (reps. $\hat{w}$) denotes the natural extension of v (resp. w) to the completion K_v (resp. L_w), then

$$e(\hat{w}|\hat{v}) = e(w|v)\,, \quad f(\hat{w}|\hat{v}) = f(w|v)\,. \tag{3.2.30.1}$$

When L/K is an infinite algebraic extension, letting $L_{(w)}$ be the localization defined in (3.2.18.1) and $\tilde{w}$ be the natural extension of w to $L_{(w)}$, the same is true for $\tilde{w}$ instead of $\hat{w}$.

When L/K is a finite extension, it will follow from Prop. 3.2.31 below that $e(w|v)$ and $f(w|v)$ are both finite. In fact, even more is true:

$$\sum_{w\,|\,v} e(w|v) f(w|v) \le [L : K]\,. \tag{3.2.30.2}$$

This result is usually referred to as the ***fundamental inequality*** of valuation theory[†]. By (3.2.30.1) and Prop. 3.2.31, we have $e(w|v)f(w|v) \leq [L_w : K_v]$ for each $w \,|\, v$. So (3.2.30.2) is a consequence of the surjectivity of φ (Remark 3.2.29).

In Cor. 3.3.3 we will discuss a strengthened version of (3.2.30.2) for discrete valuations. ■

Proposition 3.2.31. *With notation as in (3.2.30), suppose that L/K is a finite extension. Let $\omega_1, \dots, \omega_f \in \mathcal{O}_w$ be representatives of a system of elements in $\kappa(w)$ which are linearly independent over $\kappa(v)$, and let $\pi_0, \dots, \pi_{e-1} \in L^*$ be elements whose valuations represent distinct elements of $w(L^*)/v(K^*)$.*

Then the family

$$\pi_i \omega_j \,, \quad 0 \leq i \leq e-1 \,,\ 1 \leq j \leq f$$

is linearly independent over K.

In particular, $[L : K] \geq e(w|v)f(w|v)$.

Proof. Suppose

$$\sum_{i=0}^{e-1} \sum_{j=1}^{f} a_{ij} \pi_i \omega_j = 0 \,, \quad \text{with } a_{ij} \in K \,. \tag{3.2.31.1}$$

Assume that not all a_{ij} are zero.

Note that the canonical images of ω_j in the residue field $\kappa(w)$ should be nonzero. So $w(\omega_j) = 0$ for every $j \in [\![1,\, f]\!]$. Choose indices $0 \leq s \leq e-1$ and $1 \leq t \leq f$ such that

$$w(a_{st}\pi_s) = \min\{w(a_{ij}\pi_i) \,|\, 0 \leq i \leq e-1 \,,\ 1 \leq j \leq f\} \,.$$

(Since not all a_{ij} are zero, this of course implies $a_{st}\pi_s\omega_t \neq 0$, or equivalently $a_{st} \neq 0$.) We claim that for all possible indices i, j,

$$w(a_{ij}\pi_i) \neq w(a_{st}\pi_s) \quad \text{whenever } i \neq s \,. \tag{3.2.31.2}$$

Indeed, if $w(a_{ij}\pi_i) = w(a_{st}\pi_s)$, we would get $a_{ij} \neq 0$ and

$$w(\pi_i) - w(\pi_s) = w(a_{st}) - w(a_{ij}) = v(a_{st}a_{ij}^{-1}) \in v(K^*) \,.$$

But this contradicts our assumption on the valuations of the π_i. So (3.2.31.2) holds.

Now, dividing (3.2.31.1) by $a_{st}\pi_s$, we obtain a relation

$$\sum_{j=1}^{f} b_j \omega_j + z = 0 \quad \text{where } b_j = \frac{a_{sj}\pi_s}{a_{st}\pi_s} \quad \text{and} \quad z = \sum_{i \neq s} \sum_{j=1}^{f} \frac{a_{ij}\pi_i}{a_{st}\pi_s} \omega_j \,.$$

By the choice of $(s,\, t)$ and (3.2.31.2), we have $b_j \in \mathcal{O}_w$, $b_t = 1$ and $w(z) > 0$. So in the residue field $\kappa(w)$ we find

$$\bar{\omega}_t + \sum_{j \neq t} \bar{b}_j \bar{\omega}_j = 0 \,.$$

This contradicts the linearly independence of the system $\bar{\omega}_1, \cdots, \bar{\omega}_f$. We have thus proved the linear independence of $\pi_i\omega_j$ over K, and this implies the inequality $[L : K] \geq e(w|v)f(w|v)$. □

[†]The fundamental inequality is true for valuations more general than exponential valuations (which we defined in Definition 3.1.6). A complete proof of that more general version can be found in [EP05, p.75, Thm. 3.3.4] or [Bou06, § VI.8.3, Thm. 1].

3.3 Extensions and ramification of discrete valuations

Throughout this section, let K be a field equipped with a (non-archimedean) valuation $v = v_K$. Let $\mathcal{O}_v \subseteq K$ denote the valuation ring of v, and let k denote the residue field of $\mathcal{O}_v$.

3.3.1 The fundamental equality

By a ***discrete valuation field*** or a ***discretely valued field*** we mean a field equipped with a discrete valuation. In this subsection, we assume K is a discrete valuation field with normalized discrete valuation $v = v_K$.

(3.3.1) Let L/K be a finite extension and let w be an extension of v to L. Let $e = e(w|v)$. Consider the extension L_w/K_v of the completion fields. Then we have $e(\hat{w}|\hat{v}) = e$ by (3.2.30.1), where $\hat{w}$ denotes the natural extensions of w to L_w and similarly for $\hat{v}$. Therefore,

$$w(L^*) = \hat{w}(L_w^*) = \frac{1}{e}\mathbb{Z} = \frac{1}{e}\hat{v}(K_v^*) = \frac{1}{e}v(K^*)\,.$$

In particular, w is also a discrete valuation and $v_L := e.w = e(w|v)w$ is a normalized discrete valuation of L.

Let $\mathcal{O}_w$ be the valuation ring of w in L, and let $\Pi \in \mathcal{O}_w$ resp. $\pi \in \mathcal{O}_v$ be uniformizers of the discrete valuation rings $\mathcal{O}_w$ and $\mathcal{O}_v$. Then $w(\Pi^e) = e.w(\Pi) = v_L(\Pi) = 1 = w(\pi)$. So we find

$$\pi = \varepsilon.\Pi^e \quad \text{for some } \varepsilon \in \mathcal{O}_w^* \quad \text{and} \quad e = v_L(\pi)\,.$$

In particular, the ramification index $e = e(w|v)$ can be determined by using the normalized discrete valuation v_L that is equivalent to w. ■

Theorem 3.3.2 (Compare [Neu99, p.150, Prop. II.6.8])**.** *With notation as in* (3.3.1)*, suppose that* (K, v) *is* **complete** *(so* v *extends uniquely to* L*).*

1. *The valuation ring* $\mathcal{O}_w$ *coincides with the integral closure of* $\mathcal{O}_v$ *in* L*.*
2. *Let* $\omega_1, \ldots, \omega_f \in \mathcal{O}_w$ *be representatives of a basis of* ℓ *over* k*. Let* $\Pi_0, \ldots, \Pi_{e-1} \in \mathcal{O}_w$ *be chosen such that* $v_L(\Pi_i) = i$ *(where* v_L *denotes the normalized discrete valuation of* L*).*

   Then $\{\pi_i\omega_j \,|\, 0 \le i \le e-1,\ 1 \le j \le f\}$ *is a free basis of* $\mathcal{O}_w$ *as an* $\mathcal{O}_v$*-module.*

   In particular, $\mathcal{O}_w$ *is a free* $\mathcal{O}_v$*-module of rank* ef*, the equality*

   $$[L : K] = e(w|v)f(w|v)$$

   holds, and the normalized discrete valuation of L *is given by*

   $$v_L = e.w = \frac{1}{f}v_K \circ N_{L/K}\,.$$

Proof. (1) This has been proved Thm. 3.2.4 (3).

(2) Let Π be a uniformizer for v_L and let $u_0, \dots, u_{e-1} \in \mathcal{O}_w^*$ be such that $\Pi_i = u_i \Pi^i$ for each $0 \leq i \leq e-1$. Note that $\Pi^e \mathcal{O}_w = \pi \mathcal{O}_w$ for any uniformizer π of $\mathcal{O}_v$. In Prop. 3.2.31 we have seen that the family $\Pi_i \omega_j$ is linearly independent. Now we show that $\mathcal{O}_w$ is equal to the $\mathcal{O}_v$-submodule

$$M := \sum_{i=0}^{e-1} \sum_{j=1}^{f} \mathcal{O}_v . \Pi_i \omega_j \,.$$

Extending $\Pi_i \omega_j$ to a K-basis of L and then using that basis to identify L with K^n (for $n = [L:K]$) as topological vector spaces, we see that M is a closed subspace of L.

We put $N = \sum_{j=1}^{f} \mathcal{O}_v . \omega_j$ so that

$$M = u_0 N + u_1 \Pi N + u_2 \Pi^2 N + \cdots + u_{e-1} \Pi^{e-1} N \,.$$

Note that $\mathcal{O}_w = u \mathcal{O}_w = uN + u\Pi \mathcal{O}_w$ for any unit $u \in \mathcal{O}_w^*$. This implies

$$\begin{aligned} \mathcal{O}_w &= u_0 N + u_0 \Pi \mathcal{O}_w = u_0 N + \Pi \mathcal{O}_w = u_0 N + \Pi(u_1 N + u_1 \Pi \mathcal{O}_w) = \cdots = \\ &= u_0 N + u_1 \Pi N + u_2 \Pi^2 N + \cdots + u_{e-1} \Pi^{e-1} N + \Pi^e \mathcal{O}_w \\ &= M + \Pi^e \mathcal{O}_w = M + \pi \mathcal{O}_w = M + \pi(M + \pi \mathcal{O}_w) = M + \pi M + \pi^2 \mathcal{O}_w = \cdots \end{aligned}$$

Since $M = M + \pi M = M + \pi M + \pi^2 M = \cdots$, it follows that for every $\alpha \in \mathcal{O}_w$, we can find inductively a sequence $x_n \in M$ such that

$$\alpha - x_n \in \pi^{n+1} \mathcal{O}_w \quad \text{for all } n \in \mathbb{N} \,.$$

Taking the limit as $n \to \infty$ and using the fact that M is closed in L, we find $\alpha = \lim x_n \in M$. The first assertion is thus proved.

Since the rank of $\mathcal{O}_w$ over $\mathcal{O}_v$ is equal to $[L:K]$, the equality $[L:K] = ef$ follows. This combined with the formula $w = \frac{1}{[L:K]} v_K \circ N_{L/K}$ proves the desired formula for $v_L = e.w$. □

Corollary 3.3.3. *With notation as in* (3.3.1)*, suppose that L/K is separable. Then we have the* **fundamental equality**

$$[L:K] = \sum_{w \,|\, v} e(w|v) f(w|v) \,.$$

Proof. By Thm. 3.3.2 and (3.2.31.1), we have $[L_w : K_v] = e(w|v) f(w|v)$ for each $w \,|\, v$. So the result follows from Prop. 3.2.28. □

(3.3.4) Let L/K be a finite extension of degree n, $A = \mathcal{O}_v$ and B the integral closure of A in L. Suppose that B is a finitely generated A-module (which is the case if L/K is separable, by Prop. 2.1.12). Since the discrete valuation ring A is a PID, B is free of rank n over A.

Let $\pi \in A$ be a uniformizer, so $\mathfrak{p} := \pi A$ is the maximal ideal of A. Let

$$\mathfrak{p} B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$$

be the prime factorization of $\mathfrak{p}B$ in the Dedekind domain B. Each localization $B_i := B_{\mathfrak{P}_i}$ is a discrete valuation ring with fraction field L, and determines a normalized discrete valuation $v_i = v_{\mathfrak{P}_i}$ on L. Clearly, $\pi B_i = (\mathfrak{P}_i B_i)^{e_i}$. So $e_i = v_i(\pi)$, and $w_i := \frac{1}{e_i} v_i$ is an extension of v to L, with ramification index $e(w_i|v) = e_i = e(\mathfrak{P}_i|\mathfrak{p})$. (Recall that the ramification index of $\mathfrak{P}_i$ over $\mathfrak{p}$ is defined in (2.4.4).)

We claim that $w_1, \cdots, w_r$ are exactly all the extensions of v to L, and that their residue fields $\kappa(w_i)$ are precisely $B/\mathfrak{P}_i$.

To prove the claim, consider any extension w of v and let $\mathfrak{P}_w$ be the maximal ideal of the valuation ring $\mathcal{O}_w \subseteq L$. By Thm. 3.3.2, the completion $\hat{\mathcal{O}}_w$ is the integral closue of $\hat{A}$ in L_w. So $B \subseteq \hat{\mathcal{O}}_w \cap L = \mathcal{O}_w$. The prime ideal $\mathfrak{P}_w \cap B$ is a prime ideal lying over $\mathfrak{p}$. So $\mathfrak{P}_w \cap B = \mathfrak{P}_i$ for some $i \in [\![1, r]\!]$. This implies $B_{\mathfrak{P}_i} \subseteq \mathcal{O}_w$ and hence $\mathcal{O}_w = B_{\mathfrak{P}_i}$ by Lemma 2.3.24. By the correspondence between discrete valuation rings and the associated valuations (cf. Prop. 2.3.10), we conclude that $w = w_i$ and that $\kappa(w_i)$ is the residue field of $B_{\mathfrak{P}_i}$, which is the same as $B/\mathfrak{P}_i$. Our claim is thus proved.

The above discussions show in particular that the fundamental equality

$$[L : K] = \sum_{w|v} e(w|v) f(w|v) \,.$$

repeats what we have already seen in Prop. 2.4.6, working with the prime decomposition. The *raison d'être* of valuation theory, however, is not to reformulate ideal-theoretic knowledge, but rather, to provide the possibility of passing from the extension L/K to the various completions L_w/K_v where much simpler arithmetic laws apply. ■

Corollary 3.3.5. *With notation as in (3.3.1), suppose that L/K is separable. Let $A = \mathcal{O}_v$ and let B be the integral closure of A in L. Let $\hat{A}$ and $\hat{\mathcal{O}}_w$ denote the completions of the corresponding discrete valuation rings.*

Then the natural homomorphism

$$\varphi \,:\, B \otimes_A \hat{A} \longrightarrow \prod_{w\,|\,v} \hat{\mathcal{O}}_w$$

is an isomorphism.

Proof. Since L/K is separable, B is a free A-module of rank $n := [L : K]$. So $B \otimes_A \hat{A}$ is free of rank n over $\hat{A}$. On the other hand, each $\hat{\mathcal{O}}_w$ is free of rank $e(w|v)f(w|v)$ over $\hat{A}$ by Thm. 3.3.2, and hence by Cor. 3.3.3, the right hand side is also free of rank n over $\hat{A}$. Thus, by Nakayama's lemma, it is sufficient to show that the map

$$\overline{\varphi} \,:\, \big(B \otimes_A \hat{A}\big) \otimes_{\hat{A}} (\hat{A}/\pi\hat{A}) \longrightarrow \prod_{w\,|\,v} \hat{\mathcal{O}}_w \otimes_{\hat{A}} (\hat{A}/\pi\hat{A})$$

is an isomorphism, where $\pi \in A$ is a uniformizer.

With notation as in (3.3.4), we have seen that the rings $\hat{\mathcal{O}}_w$ can be identified with the completions of the localizations $B_i = B_{\mathfrak{P}_i}$. Hence

$$\prod_{w\,|\,v} \hat{\mathcal{O}}_w \otimes_{\hat{A}} (\hat{A}/\pi\hat{A}) = \prod_{w\,|\,v} \hat{\mathcal{O}}_w/\pi\hat{\mathcal{O}}_w = \prod B_i/\mathfrak{P}_i^{e_i} B_i = \prod B/\mathfrak{P}_i^{e_i} \,.$$

So the map $\overline{\varphi}$ coincides with the natural isomorphism

$$B/\pi B \xrightarrow{\sim} \prod B/\mathfrak{P}_i^{e_i}$$

obtained by applying the Chinese remainder theorem. □

3.3.2 Unramified and tamely ramified extensions

In this subsection, we assume that (K, v) is a *henselian* (e.g. complete) valuation field, and we write $k = \kappa(v)$ for the residue field of v. We fix an algebraic closure $\overline{K}$ of K and consider all algebraic extensions of K as embedded in $\overline{K}$.

If M/K is an algebraic extension, let w_M be the unique extension of v to M, $\mathcal{O}_M$ the valuation ring of w_M, $\mathfrak{p}_M$ the maximal ideal of $\mathcal{O}_M$, and $\kappa_M = \kappa(w_M)$ the residue field. (Warning: When v is discrete, w_M may not be a discrete valuation if M/K is an infinite extension!) As we have seen in Thm. 3.2.4 (3), $\mathcal{O}_M$ is the integral closure of $\mathcal{O}_K$ in M. Moreover, M is henselian by Thm. 3.2.10.

The following result will be used frequently.

Lemma 3.3.6. *Let M/K be an algebraic extension, and let $f \in \mathcal{O}_K[t]$ be a monic polynomial whose reduction $\bar{f} \in k[t]$ is separable.*

Then f is separable, and the reduction map $\mathcal{O}_M \to \kappa_M$; $x \mapsto \bar{x}$ induces a bijection

$$\{\textit{roots of } f \textit{ in } M\} \xrightarrow{\sim} \{\textit{roots of } \bar{f} \textit{ in } \kappa_M\} \; ; \quad \alpha \mapsto \overline{\alpha} \, .$$

Moreover, $\bar{f}$ is irreducible over k if and only if f is irreducible over K.

Proof. Since f is monic, its roots in in $\overline{K}$ all lie in $\mathcal{O}_{\overline{K}}$. If f has multiple roots in $\overline{K}$, then $\bar{f}$ has multiple roots in the residue field of $\overline{K}$, contradicting the separability of $\bar{f}$.

Since f is moinc and $\mathcal{O}_K$ is integrally closed, f is irreducible over K if and only if it is irreducible in $\mathcal{O}_K[t]$. The irreducibility of $\bar{f}$ over k clearly implies the irreducibility of f in $\mathcal{O}_K[t]$. Conversely, by Hensel's lemma, f is reducible if $\bar{f}$ is.

It remains to prove the bijection between the roots of f and those of $\bar{f}$. If $\bar{f}$ has no roots in κ_M, then both sets of roots are empty, so there is nothing to prove in this case. We may thus assume $\bar{f}$ has some roots in κ_M. We can factorize the separable polynomial $\bar{f}$ in $\kappa_M[t]$ such that

$$\bar{f}(t) = \bar{g}(t) \cdot \prod_{i=1}^{r} (t - \bar{\alpha}_i) \, ,$$

where $\bar{\alpha}_i \in \kappa_M$ are distinct roots of $\bar{f}$ and $\bar{g}$ has no roots in κ_M. Applying Hensel's lemma (Prop. 3.2.12) repeatedly, we can find a factorization $f = g \cdot \prod_{i=1}^{r}(t - \alpha_i)$ in $\mathcal{O}_M[t]$, where $\alpha_i \in \mathcal{O}_M$ lifts $\bar{\alpha}_i$ and $g \in \mathcal{O}_M[t]$ is a monic lifting of $\bar{g}$. Since $\bar{g}$ has no roots in κ_M, g has no roots in M. So $\{\alpha_1, \cdots, \alpha_r\}$ is precisely the set of roots of f in M. The lemma is thus proved. □

(3.3.7) Let L/K be a finite extension with residue field extension ℓ/k, and let $w = w_L$. We say that L/K is ***unramified*** if ℓ/k is separable and $[\ell : k] = [L : K]$. Notice that the equality $[\ell : k] = [L : K]$ implies $e(w|v) = 1$, by the fundamental inequality (3.2.30.2). If the fundamental equality holds (e.g., if v is discrete and either L/K is separable or K is complete, by Thm. 3.3.2 and Cor. 3.3.3), then $[\ell : k] = [L : K]$ is equivalent to $e(w|v) = 1$.

If (K, v) is a discrete valuation field, then $\mathcal{O}_L$ is a discrete valuation ring. Let $\pi \in \mathcal{O}_K$ be a uniformizer of K, and $\Pi \in \mathcal{O}_L$ a uniformizer of L. Then $\pi\mathcal{O}_L = \Pi^e\mathcal{O}_L$, where $e = e(w|v)$ is the ramification index of $w|v$, by (3.3.1). Since $\mathfrak{p}_K = \pi\mathcal{O}_K$, $\mathfrak{p}_L = \Pi\mathcal{O}_L$ and $\ell = \mathcal{O}_L/\mathfrak{p}_L$, $e(w|v)$ (resp. $f(w|v)$) is the same as the ramification index $e(\mathfrak{p}_L|\mathfrak{p}_K)$ (resp. the residue degree $f(\mathfrak{p}_L|\mathfrak{p}_K)$) of $\mathfrak{p}_L|\mathfrak{p}_K$. So in this case, assuming the fundamental equality holds, L/K is unramified if and only if L/K is unramified at $\mathfrak{p}_K$ (in the sense of Definition 2.4.5).

We say that L/K is ***totally ramified***[‡] if $\ell = k$, i.e., $f(w|v) = 1$. (Here $f(w|v) = 1$ holds if $e(w|v) = [L : K]$, by the fundamental inequality (Prop. 3.2.31), and if the fundamental equality holds, the reverse implication is also true.) When (K, v) is a discrete valuation field, L/K is totally ramified if and only if it is totally ramified at $\mathfrak{p}_K$ (in the sense of Definition 2.4.5).

If F/K is a subextension of L/K, then L/K is totally ramified if and only if L/F and F/K are both totally ramified. ■

Lemma 3.3.8. *Let L/K be a finite extension with residue field extension ℓ/k.*

1. *Suppose that there is a monic polynomial $f \in \mathcal{O}_K[t]$ and a root $\alpha \in \mathcal{O}_L$ of f such that the reduction $\bar{f} \in k[t]$ is separable and irreducible, and $L = K(\alpha)$.*

   Then f is separable and irreducible over K, L/K is separable and unramified, $\ell = k(\bar{\alpha})$ and $[L : K] = [\ell : k]$.

2. *Conversely, suppose that L/K is unramified and write $\ell = k(\bar{\alpha})$ for some $\bar{\alpha} \in \ell$. Let $\bar{f} \in k[t]$ be the monic minimal polynomial of $\bar{\alpha}$ over k and lift it to a monic polynomial $f \in \mathcal{O}_K[t]$.*

   Then f is separable and irreducible over K, $\bar{\alpha}$ has a lifting $\alpha \in \mathcal{O}_L$ such that $f(\alpha) = 0$ and $L = K(\alpha)$. In particular, L/K is separable.

Proof. (1) First, f is irreducible and separable by Lemma 3.3.6, so $L = K(\alpha)$ is separable over K. Moreover,

$$[\ell : k] \geq [k(\bar{\alpha}) : k] = \deg(\bar{f}) = \deg(f) = [L : K]\,.$$

By the fundamental inequality (3.2.30.2), we have $[\ell : k] = [L : K]$ and $\ell = k(\bar{\alpha})$. So ℓ/k is separable by the separability of $\bar{f}$ and L/K is thus unramified.

(2) Again by Lemma 3.3.6, f is irreducible and separable over K and there is a lifting $\alpha \in \mathcal{O}_L$ of $\bar{\alpha}$ such that $f(\alpha) = 0$. The subfield $K(\alpha) \subseteq L$ has degree $[K(\alpha) : K] =$

[‡]Our definition of total ramifiedness agrees with that of [TW15, Appendix A] (for discrete valuations). It is slightly different from the one given in [Neu99, p.158], when the residue field $\kappa(v)$ is imperfect.

$\deg(f) = \deg(\bar{f}) = [\ell : k]$. Since L/K is unramified, we have $[\ell : k] = [L : K]$. It follows that $L = K(\alpha)$. □

Proposition 3.3.9. *Let L/K and K'/K be finite extensions (contained in $\overline{K}/K$) and let $L' = L.K'$ be the composite.*

1. *Let F be an intermediate field of $K \subseteq L$. Then L/K is unramified if and only if F/K and L/F are unramified.*
2. *If L/K is unramified, then L'/K' is also unramified.*
3. *If both L/K and K'/K are unramified, then L'/K is unramified.*

Proof. (1) The residue field extension κ_L/k is separable if and only if κ_L/κ_F and κ_F/k are both separable. The result is thus a consequence of the fundamental inequality (3.2.30.2) and the obvious formula $f(w_L|w_F) \cdot f(w_F|v) = f(w_L|v)$.

(2) By Lemma 3.3.8 (2), we can find an element $\alpha \in \mathcal{O}_L$ with minimal polynomial f such that $L = K(\alpha)$, $\bar{f} \in k[t]$ irreducible separable and $\ell = k(\bar{\alpha})$. Let k' be the residue field of K' and let $g \in \mathcal{O}_{K'}[t]$ be the minimal polynomial of α over K'. Then g divides f in $\mathcal{O}_{K'}[t]$, so the reduction $\bar{g} \in k'[t]$ is a factor of $\bar{f}$ in $k'[t]$. Since $\bar{f}$ is separable, so is $\bar{g}$. By Lemma 3.3.6, we also know that $\bar{g}$ is irreducible over k'. Since $L' = K'(\alpha)$, it follows from Lemma 3.3.8 (1) that L'/K' is unramified.

(3) By (2), L'/K' is unramified. Then L'/K is unramified by (1). □

(3.3.10) Let M/K be an arbitrary algebraic extension. We say that M/K is ***unramified*** if every finite subextension of it is unramified. Note that

$$M = \bigcup_E E\,, \quad w_M(M^*) = \bigcup_E w_E(E^*) \quad \text{and} \quad \kappa_M = \bigcup_E \kappa_E\,,$$

where E/K runs over finite subextensions of M/K. In particular, κ_M/k is an algebraic extension, since each κ_E/k is a finite (hence algebraic) extension.

The following properties are easily verified (using Prop. 3.3.9 if necessary):

1. Any unramified extension is separable.
2. An algebraic extension M/K is unramified if and only if M is a union of finite unramified extensions of K.
3. If M/K is unramified, then the residue field extension $\kappa(w_M)/\kappa(v)$ is separable and $w_M(M^*) = v(K^*)$. The converse is also true if M/K is separable or K is complete. ■

Proposition 3.3.11. *For any algebraic extensions L/K and K'/K, the statements in Prop. 3.3.9 are still true.*

Proof. Exercise. □

Definition 3.3.12. Let L/K be an algebraic extension. The composite of all unramified subextensions in L/K is called the ***maximal unramified subextension*** of L/K.

The maximal unramifield subextension of $\overline{K}/K$ is simply called the ***maximal unramified extension*** of K, and will be denoted by K^{ur}. ■

Proposition 3.3.13. *Let L/K be an algebraic extension and T/K its maximal unramified extension.*

Then the residue field of T is the separable closure of $k = \kappa(v)$ in the residue field extension ℓ/k of L/K.

In particular, the residue field of K^{ur} is a separable closure of k.

Proof. Let $\bar{\alpha} \in \ell$ be an element that is separable over k. We want to show that $\bar{\alpha}$ lies in the residue field of T.

Let $\bar{f} \in k[t]$ be the monic minimal polynomial of $\bar{\alpha}$ over k, and lift it to a monic polynomial $f \in A[t]$. Since $\bar{f}$ is separable and irreducible over k, by Lemma 3.3.6, f is irreducible over K and has a root $\alpha \in \mathcal{O}_L$ whose image in ℓ is $\bar{\alpha}$. The subfield $K(\alpha) \subseteq L$ satisfies $[K(\alpha) : K] = \deg(f) = \deg(\bar{f}) = [k(\bar{\alpha}) : k]$. So $K(\alpha)/K$ is unramified with residue field extension $k(\bar{\alpha})/k$. Hence $K(\alpha) \subseteq T$ and $\bar{\alpha}$ lies in the residue field of T. This proves the first assertion.

It is easy to see that the residue field of $\overline{K}$ is an algebraic closure of k. So the second assertion is immediate from the first one. □

Theorem 3.3.14. *Let K^{ur}/K be the maximal unramified extension of K (inside $\overline{K}$) and let k_s/k be the residue field extension. (Note that k_s is a separable closure of k, by Prop. 3.3.13.)*

Then, by taking residue fields, we obtain an inclusion-preserving bijection

$$\{\textit{finite subextensions of } K^{ur}/K\} \xrightarrow{\sim} \{\textit{finite subextensions of } k_s/k\}\,;$$

Moreover, if L/K corresponds to ℓ/k via this bijection, then the natural homomorphism (cf. Prop. 2.1.21)

$$\mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(\ell/k)\,; \quad \sigma \longmapsto \overline{\sigma}$$

is an isomorphism, and L/K is Galois if and only if ℓ/k is Galois.

Proof. Given a finite subextension ℓ/k of k_s/k, as in the proof of Prop. 3.3.13 we can construct a finite subextension L/K in K^{ur}/K with residue field ℓ/k. This proves the surjectivity of the map under consideration. From the construction it is also clear that if ℓ_0 is a subextension of ℓ, then we can construction the extension L_0/K corresponding to ℓ_0/k in such a way that $L_0 \subseteq L$.

Suppose that L_1, L_2 are finite subextensions of K^{ur}/K with the same residue field ℓ. Writing $\ell = k(\bar{\alpha})$, letting $\bar{f} \in k[t]$ be the minimal polynomial of $\bar{\alpha}$ and lifting $\bar{f}$ to a monic $f \in \mathcal{O}_K[t]$, we can deduce from Lemma 3.3.8 (2) that f has a root $\alpha_1 \in L_1$ and a root $\alpha_2 \in L_2$, both lifting $\bar{\alpha} \in \ell$, such that $L_1 = K(\alpha_1)$ and $L_2 = K(\alpha_2)$. Since α_1, α_2 have the same image in the residue field of K^{ur}, Lemma 3.3.6 shows that $\alpha_1 = \alpha_2$, whence $L_1 = L_2$. This proves the claimed bijection.

Now suppose L/K is a finite subextension of K^{ur}/K, with residue field extension ℓ/k. As above, we can write $L = K(\alpha)$ and $\ell = k(\bar{\alpha})$, with α lifting $\bar{\alpha}$ and the minimal polynomial f of α lifting the minimal polynomial $\bar{f}$ of $\bar{\alpha}$. Elements of $\mathrm{Gal}(L/K)$ correspond bijectively to the roots of f in L and similarly for $\mathrm{Gal}(\ell/k)$. Let $n = [L : K] = [\ell : k]$. Then L/K is Galois if and only if f has n (distinct) roots in L, and ℓ/k is Galois if and only if $\bar{f}$ has n (distinct) roots in ℓ. So the second assertion of theorem is an immediate consequence of the bijection in Lemma 3.3.6. □

Definition 3.3.15. Let L/K be an algebraic extension and T/K be the maximal unramified subextension of L/K. We say that L/K is ***tamely ramified*** if the residue field extension ℓ/k is separable and $\mathrm{char}(k) \nmid [L : T]$. If L/T is an infinite extension, this latter condition is taken to mean that the degree of every finite subextension of L/T is not divisible by $\mathrm{char}(k)$.

If L/K is not tamely ramified, we say that it is ***wildly ramified***.

Clearly, If the residue field k has characteristic 0, then evidently any algebraic extension of K is tamely ramified. ■

Lemma 3.3.16. *With notation as in (3.3.15), the following assertions hold:*

1. *L/K is tamely ramified if and only if L/T is tamely ramified.*
2. *Suppose that L/K is a finite extension with residue field extension ℓ/k and let $e(L/K)$, $f(L/K)$ be its ramification index and residue degree.*
   (a) *L/T is totally ramified if and only if ℓ/k is separable.*
   (b) *Suppose that the fundamental equality $[L : K] = e(L/K)f(L/K)$ holds (e.g. if K is complete or L/K is separable). Then, L/K is tamely ramified if and only if $\mathrm{char}(k) \nmid e(L/K)$ and the extension ℓ/k is separable.*

Proof. Exercise. □

Proposition 3.3.17. *Let (K, v) be a henselian discrete valuation field. Let L/K be a totally and tamely ramified extension of degree e.*

Then there is a uniformizer Π of L such that $\pi := \Pi^e$ is is a uniformizer of K and $L = K(\Pi)$. In particular, L/K is a separable extension.

Moreover, L/K is Galois if and only if K contains a primitive e-th root of unity.

Proof. Since L/K is totally ramified, the ramification index of $w_L|v$ is e, the residue field of L is k, and the maximal unramified extension of K in L is K itself. In particular, the tameness assumption implies that $\mathrm{char}(k) \nmid e = [L : K]$.

Let β be a uniformizer of L and π_0 be a uniformizer of K. Then $\pi_0 u = \beta^e$ for some $u \in \mathcal{O}_L^*$ (cf. (3.3.1)). We can choose $u_0 \in \mathcal{O}_K^*$ such that $\bar{u} = \bar{u}_0$ in k, i.e., $u \equiv u_0 \pmod{\mathfrak{p}_L}$. Put $\pi = \pi_0 u_0 \in \mathcal{O}_K$. Then $\beta^e = \pi + \pi x$ for some $x \in \mathfrak{p}_L$. Letting $|\cdot|$ denote the absolute value associated to the extension of v to $\overline{K}$, we have

$$|\beta|^e = |\pi| \quad \text{and} \quad |\beta^e - \pi| < |\pi|\,.$$

Now consider the polynomial $f(t) := t^e - \pi$. By Eisenstein's criterion, f is irreducible over K. Let $\alpha_1, \cdots, \alpha_e$ be all the (distinct) roots of f in $\overline{K}$. Then $|\alpha_i|^e = |\pi| = |\beta|^e$, so $|\alpha_i| = |\beta|$ for each i. Since

$$\prod_{i=1}^{e} |\beta - \alpha_i| = |f(\beta)| = |\beta^e - \pi| < |\pi| = |\beta|^e ,$$

we may assume without loss of generality that $|\beta - \alpha_1| < |\beta| = |\alpha_1|$. On the other hand, for each $j \geq 2$, $|\alpha_1 - \alpha_j| \leq \max\{|\alpha_1|, |\alpha_j|\} = |\alpha_1|$, and

$$\prod_{j=2}^{e} |\alpha_1 - \alpha_j| = |f'(\alpha_1)| = |\alpha_1|^{e-1} .$$

Therefore, $|\alpha_1 - \alpha_j| = |\alpha_1|$ for every $j \in [\![2, e]\!]$. Now we have

$$|\beta - \alpha_1| < |\alpha_1| = \min_{2 \leq j \leq e} |\alpha_j - \alpha_1| .$$

So by Krasner's lemma (Thm. 3.2.15), $K(\alpha_1) \subseteq K(\beta) \subseteq L$. Since $[K(\alpha_1) : K] = \deg(f) = e = [L : K]$, we get $L = K(\alpha_1)$. Taking $\Pi = \alpha_1$ proves the first assertion.

Let $\xi \in \overline{K}$ be a primitive e-th root of unity. If $\xi \in K$, then L contains all the roots of $t^e - \pi$, which are $\Pi, \xi\Pi, \cdots, \xi^{e-1}\Pi$. So in this case, the extension $L = K(\Pi) = K(\sqrt[e]{\pi})$ is Galois. Conversely, suppose that L/K is Galois, then $\xi\Pi \in L$ and hence $\xi \in L$. This implies that the residue field of L contains a primitive e-th root of unity. But the residue field of L is the same as that of K. So by Lemma 3.3.6, K also contains a primitive e-th root of unity. □

3.4 Different and discriminant

Throughout this section, let A denote a Dedekind domain with fraction field K, L/K a finite separable extension and B the integral closure of A in L. By Prop. 2.1.12, B is a finitely generated module over A. Also, the separability implies that the symmetric bilinear form

$$\mathrm{Tr} : \ L \times L \longrightarrow K ; \quad (x, y) \longmapsto \mathrm{Tr}_{L/K}(xy)$$

induced by trace map $\mathrm{Tr}_{L/K} : L \to K$ is nondegenerate.

3.4.1 Definitions and basic properties

(3.4.1) For any A-submodule M of L, we define its ***dual*** over A with respect to the trace form to be

$$M^{\#} := \{x \in L \mid \mathrm{Tr}(xM) \subseteq A\} .$$

This is an A-submodule of L. If M is a B-submodule of L, then so is $M^{\#}$.

The notion of duality is justified as follows: Since the trace form is nondegenerate, it induces an isomorphism of K-vector spaces

$$\theta : \ L \xrightarrow{\sim} \mathrm{Hom}_K(L, K) := \{K\text{-linear maps } L \to K\} ; \ \alpha \mapsto (z \mapsto \mathrm{Tr}(\alpha z)) .$$

When M contains a K-basis, any A-linear map $f : M \to A$ extends uniquely to a K-linear map $f : L \to K$, so we may consider

$$\mathrm{Hom}_A(M,\, A) := \{A\text{-linear maps } M \to A\}$$

as an A-submodule of $\mathrm{Hom}_K(L,\, K)$. Then the above map θ induces an isomorphism of A-modules

$$M^{\#} \xrightarrow{\sim} \mathrm{Hom}_A(M,\, A)\,; \quad \alpha \mapsto (z \mapsto \mathrm{Tr}(\alpha z))\,.$$

As we have seen in the proof of Prop. 2.1.12, if $\{e_i\}$ is a K-basis of L contained in M and $V := \oplus Ae_i$, then $M^{\#} \subseteq V^{\#}$ and $V^{\#} = \oplus Af_i$, where $\{f_i\} \subseteq L$ is the dual basis of $\{e_i\}$ with respect to the trace form, i.e., $\mathrm{Tr}(e_i f_j) = \delta_{ij}$. In particular $M^{\#}$ is a finitely generated A-module in this case. If M is a fractional ideal of B, then $M^{\#}$ is a finitely generated B-submodule of L, hence a fractional ideal of B. ■

Definition 3.4.2. The fractional ideal

$$\mathfrak{C}_{B/A} := B^{\#} = \{\, x \in L \mid \mathrm{Tr}(xB) \subseteq A \,\}$$

is called ***Dedekind's complementary module*** or the ***inverse different*** of B/A (or of L/K). Its inverse (in the group of fractional ideals of B)

$$\mathfrak{D}_{B/A} := \mathfrak{C}_{B/A}^{-1}$$

is called the ***different*** of B/A (or of L/K). Since $\mathrm{Tr}(B) \subseteq A$, we have $\mathfrak{C}_{B/A} \supseteq B$ and $\mathfrak{D}_{B/A}$ is an integral ideal of B.

When the intended rings A, B are evident from the context, we will often write $\mathfrak{C}_{L/K}$ and $\mathfrak{D}_{L/K}$ instead of $\mathfrak{C}_{B/A}$ and $\mathfrak{D}_{B/A}$. ■

Proposition 3.4.3. *If S is a multiplicative subset of A, then*

$$S^{-1}\mathfrak{C}_{B/A} = \mathfrak{C}_{S^{-1}B/S^{-1}A} \quad \textit{and} \quad S^{-1}\mathfrak{D}_{B/A} = \mathfrak{D}_{S^{-1}B/S^{-1}A}\,.$$

Proof. Immediate from the definition. □

Recall (from (2.4.20)) that the ***discriminant*** (***ideal***) $\mathfrak{d}_{B/A} = \mathfrak{d}_{L/K}$ of B/A or L/K is defined to be the fractional ideal of A generated by the elements

$$\mathrm{disc}_{L/K}(\alpha_1, \cdots, \alpha_n) \quad \text{where } n = [L : K] \text{ and all } \alpha_i \in B\,.$$

We will need the following result to relate the discriminant to the different.

Lemma 3.4.4. *Let $\alpha_1, \cdots, \alpha_n$ be a K-basis of L and let $\alpha_1', \cdots, \alpha_n'$ be its dual basis with respect to the trace form. Then*

$$\mathrm{disc}_{L/K}(\alpha_1, \cdots, \alpha_n) \cdot \mathrm{disc}_{L/K}(\alpha_1', \cdots, \alpha_n') = 1\,.$$

Proof. Let $\sigma_1, \cdots, \sigma_n$ be all the K-embeddings of L into $\overline{K}$. Then by Thm. 2.4.19 (1), we have

$$\mathrm{disc}(\alpha_1, \cdots, \alpha_n) = \det(M)^2 = \det(M^T)^2\,,\ \mathrm{disc}(\alpha'_1, \cdots, \alpha'_n) = \det(M')^2$$

where $M = (\sigma_i \alpha_j)$ and $M' = (\sigma_i \alpha'_j)$. Note that for all $i, j \in [\![1, n]\!]$, the (i, j)-th entry of the product matrix $M^T M'$ is

$$\sum_{l=1}^{n} \sigma_l(\alpha_i)\sigma_l(\alpha'_j) = \mathrm{Tr}(\alpha_i \alpha'_j) = \delta_{ij}\,.$$

That is, $M' = (M^T)^{-1}$. So the result follows immediately. □

Proposition 3.4.5. *We have* $\mathfrak{d}_{L/K} = N_{L/K}(\mathfrak{D}_{L/K})$.

(Here the right hand side means the ideal norm defined as in (2.4.12), not the set $\{N_{L/K}(x) \mid x \in \mathfrak{D}_{L/K}\}$*.)*

Proof. By localization (using Props. 2.4.21 and 3.4.3), we may assume that A is a discrete valuation ring. Then B is a PID (Exercise) and a free A-module of rank $n = [L : K]$. Let $\alpha_1, \cdots, \alpha_n$ be a basis of B over A. Then

$$\mathfrak{d}_{L/K} = \mathrm{disc}_{L/K}(\alpha_1, \cdots, \alpha_n)A$$

by Prop. 2.4.25. Let α'_j be the dual basis of α_i. Then, on the one hand, $\mathfrak{C}_{L/K} = B^{\#} = (\oplus \alpha_i)^{\#} = \oplus A\alpha'_i$. On the other hand, as a fractional ideal of B, $\mathfrak{C}_{L/K}$ can be written as $\mathfrak{C}_{L/K} = xB = \oplus Ax\alpha_i$ for some $x \in B$. Thus, by (2.4.18.2) and Thm. 2.4.19 (1),

$$\begin{aligned}\mathrm{disc}(\alpha'_1, \cdots, \alpha'_n)A &= \mathrm{disc}(x\alpha_1, \cdots, x\alpha_n)A = (\det(\sigma_i(x\alpha_j)))^2 A \\ &= N_{L/K}(x)^2(\det(\sigma_i\alpha_j))^2 A = N_{L/K}(x)^2 \mathrm{disc}(\alpha_1, \cdots, \alpha_n)A\,.\end{aligned}$$

Together with Lemma 3.4.4, this shows that

$$N_{L/K}(x)A = \mathrm{disc}(\alpha_1, \cdots, \alpha_n)^{-1}A = \mathfrak{d}_{L/K}^{-1}\,.$$

Finally, by Prop. 2.4.14 we have

$$N_{L/K}(\mathfrak{D}_{L/K})^{-1} = N_{L/K}(\mathfrak{C}_{L/K}) = N_{L/K}(xB) = N_{L/K}(x)A = \mathfrak{d}_{L/K}^{-1}\,.$$

So the desired result follows by taking inverse. □

Proposition 3.4.6. *Let* $\mathfrak{a}$ *(resp.* $\mathfrak{b}$*) be a fractional ideal of* A *(resp.* B*).*

Then $\mathrm{Tr}(\mathfrak{b}) \subseteq \mathfrak{a} \iff \mathfrak{b} \subseteq \mathfrak{a}.\mathfrak{D}_{L/K}^{-1}$.

Proof. Note that $\mathrm{Tr}(\mathfrak{b})$ is a fractional ideal of A, i.e., a finitely generated A-submodule of K (since $\mathfrak{b}$ is finitely generated over A). We have

$$\begin{aligned}\mathrm{Tr}(\mathfrak{b}) \subseteq \mathfrak{a} &\iff \mathfrak{a}^{-1}\,\mathrm{Tr}(\mathfrak{b}) \subseteq A \iff \mathrm{Tr}(\mathfrak{a}^{-1}\mathfrak{b}) \subseteq A \\ &\iff \mathfrak{a}^{-1}\mathfrak{b} \subseteq \mathfrak{C}_{B/A} = \mathfrak{D}_{L/K}^{-1} \iff \mathfrak{b} \subseteq \mathfrak{a}.\mathfrak{D}_{L/K}^{-1}\end{aligned}$$

whence the proposition. □

Proposition 3.4.7. *Let M/L and L/K be finite separable extensions. Then*

$$\mathfrak{D}_{M/K} = \mathfrak{D}_{M/L} \cdot \mathfrak{D}_{L/K} \quad \textit{and} \qquad \mathfrak{d}_{M/K} = N_{L/K}(\mathfrak{d}_{M/L})(\mathfrak{d}_{L/K})^{[M:L]} .$$

Proof. Let C be the integral closure of A in M. For any fractional ideal $\mathfrak{c}$ of C, we obtain from Prop. 3.4.6

$$\begin{aligned}
\mathfrak{c} \subseteq \mathfrak{D}_{M/L}^{-1} &\iff \mathrm{Tr}_{M/L}(\mathfrak{c}) \subseteq B \iff \mathfrak{D}_{L/K}^{-1}\,\mathrm{Tr}_{M/L}(\mathfrak{c}) \subseteq \mathfrak{D}_{L/K}^{-1} \\
&\iff \mathrm{Tr}_{L/K}\left(\mathfrak{D}_{L/K}^{-1}\,\mathrm{Tr}_{M/L}(\mathfrak{c})\right) \subseteq A \iff \mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L}\left(\mathfrak{D}_{L/K}^{-1} \cdot \mathfrak{c}\right) \subseteq A \\
&\iff \mathrm{Tr}_{M/K}(\mathfrak{D}_{L/K}^{-1} \cdot \mathfrak{c}) \subseteq A \iff \mathfrak{D}_{L/K}^{-1} \cdot \mathfrak{c} \subseteq \mathfrak{D}_{M/K}^{-1} \\
&\iff \mathfrak{c} \subseteq \mathfrak{D}_{L/K} \cdot \mathfrak{D}_{M/K}^{-1} .
\end{aligned}$$

Comparing the first and last inclusions we find

$$\mathfrak{D}_{M/L}^{-1} = \mathfrak{D}_{L/K} \cdot \mathfrak{D}_{M/K}^{-1} ,$$

whence the first equality of the proposition. The second formula then follows by applying the norm $N_{M/K}$, thanks to Prop. 3.4.5. □

Proposition 3.4.8. *Let $\mathfrak{p}$ be a maximal ideal of A, $\hat{A}_\mathfrak{p}$ the completion of the localization $A_\mathfrak{p}$. For every $\mathfrak{P} \in \mathrm{Spm}(B)$ lying over $\mathfrak{p}$, let $\hat{B}_\mathfrak{P}$ be the completion of the localization $B_\mathfrak{P}$.*

Then

$$\mathfrak{D}_{B/A}\hat{B}_\mathfrak{P} = \mathfrak{D}_{\hat{B}_\mathfrak{P}/\hat{A}_\mathfrak{p}} \quad \textit{and} \quad \mathfrak{d}_{B/A}\hat{A}_\mathfrak{p} = \prod_{\mathfrak{P}\,|\,\mathfrak{p}} \mathfrak{d}_{\hat{B}_\mathfrak{P}/\hat{A}_\mathfrak{p}} .$$

Proof. By localization at $\mathfrak{p}$ and using Prop. 3.4.3, we may assume $A = A_\mathfrak{p}$ is a DVR. Putting $L_\mathfrak{P} = \mathrm{Frac}(\hat{B}_\mathfrak{P})$ and $K_\mathfrak{p} = \mathrm{Frac}(\hat{A}_\mathfrak{p})$, we have

$$\mathrm{Tr}_{L/K}(z) = \sum_{\mathfrak{P}\,|\,\mathfrak{p}} \mathrm{Tr}_{L_\mathfrak{P}/K_\mathfrak{p}}(z) \quad \text{for all } z \in L ,$$

by Prop. 3.2.28. Using this formula, we first prove $\mathfrak{C}_{B/A} \subseteq \mathfrak{C}_{\hat{B}_\mathfrak{P}/\hat{A}_\mathfrak{p}}$ for any fixed $\mathfrak{P}\,|\,\mathfrak{p}$.

Let $x \in \mathfrak{C}_{B/A}$. For any $y \in \hat{B}_\mathfrak{P}$, the weak approximation theorem (Thm. 3.1.10) guarantees the existence of an element $\eta \in B$ which is close to y with respect to the $\mathfrak{P}$-adic topology, and close to 0 with respect to the $\mathfrak{P}'$-adic topology for all $\mathfrak{P}'|\mathfrak{p}$, $\mathfrak{P}' \neq \mathfrak{P}$. Then

$$\mathrm{Tr}_{L/K}(x\eta) = \mathrm{Tr}_{L_\mathfrak{P}/K_\mathfrak{p}}(x\eta) + \sum_{\mathfrak{P}' \neq \mathfrak{P}} \mathrm{Tr}_{L_{\mathfrak{P}'}/K_\mathfrak{p}}(x\eta) .$$

The left hand side belongs to $A = A_\mathfrak{p} \subseteq \hat{A}_\mathfrak{p}$ by the definition of $\mathfrak{C}_{B/A}$, and the same is true of the elements $\mathrm{Tr}_{L_{\mathfrak{P}'}/K_\mathfrak{p}}(x\eta)$ because they are close to 0 in the $\mathfrak{p}$-adic topology. Therefore, $\mathrm{Tr}_{L_\mathfrak{P}/K_\mathfrak{p}}(x\eta)$, and hence also $\mathrm{Tr}_{L_\mathfrak{P}/K_\mathfrak{p}}(xy)$, lies in $\hat{A}_\mathfrak{p}$. This proves $\mathfrak{C}_{B/A} \subseteq \mathfrak{C}_{\hat{B}_\mathfrak{P}/\hat{A}_\mathfrak{p}}$.

Now we show that $\mathfrak{C}_{B/A}$ is dense in $\mathfrak{C}_{\hat{B}_\mathfrak{P}/\hat{A}_\mathfrak{p}}$. Let $z \in \mathfrak{C}_{\hat{B}_\mathfrak{P}/\hat{A}_\mathfrak{p}}$. If $\xi \in L$ is sufficiently close to z in the $\mathfrak{P}$-adic topology, and sufficiently close to 0 in the $\mathfrak{P}'$-adic topology for all $\mathfrak{P}' \neq \mathfrak{P}$, then $\xi \in \mathfrak{C}_{B/A}$. In fact, if $\beta \in B$, then $\mathrm{Tr}_{L_\mathfrak{P}/K_\mathfrak{p}}(\xi\beta)$ lies in $\hat{A}_\mathfrak{p}$ since it is close

to $\mathrm{Tr}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(z\beta) \in \hat{A}_{\mathfrak{p}}$. For $\mathfrak{P}' \neq \mathfrak{P}$, $\mathrm{Tr}_{L_{\mathfrak{P}'}/K_{\mathfrak{p}}}(\xi\beta)$ belongs to $\hat{A}_{\mathfrak{p}}$ because it is close to 0. Therefore,

$$\mathrm{Tr}_{L/K}(\xi\beta) = \mathrm{Tr}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(\xi\beta) + \sum_{\mathfrak{P}' \neq \mathfrak{P}} \mathrm{Tr}_{L_{\mathfrak{P}'}/K_{\mathfrak{p}}}(\xi\beta) \ \in \hat{A}_{\mathfrak{p}}\,.$$

Hence $\mathrm{Tr}_{L/K}(\xi\beta) \in \hat{A}_{\mathfrak{p}} \cap K = A_{\mathfrak{p}} = A$. This being established for all $\beta \in B$, we get $\xi \in \mathfrak{C}_{B/A}$ as desired.

This proves the density of $\mathfrak{C}_{B/A}$ in $\mathfrak{C}_{\hat{B}_{\mathfrak{P}}/\hat{A}_{\mathfrak{p}}}$. It follows that $\mathfrak{C}_{B/A}\hat{B}_{\mathfrak{P}} = \mathfrak{C}_{\hat{B}_{\mathfrak{P}}/\hat{A}_{\mathfrak{p}}}$, and taking inverse yields the first formula in the proposition.

The second one can be obtained from the first one by taking the norm and using Prop. 3.4.5. In fact, noticing that the $\mathfrak{P}$ over $\mathfrak{p}$ are all the maximal ideal of B (since A is now a DVR), if we write

$$\mathfrak{D}_{B/A} = \prod_{\mathfrak{P}\,|\,\mathfrak{p}} \mathfrak{P}^{c(\mathfrak{P})} \quad \text{where} \quad c(\mathfrak{P}) \in \mathbb{Z}\,,$$

then

$$\mathfrak{d}_{B/A} \cdot \hat{A}_{\mathfrak{p}} = N_{L/K}(\mathfrak{D}_{B/A})\hat{A}_{\mathfrak{p}} = (\mathfrak{p}\hat{A}_{\mathfrak{p}})^{n_{\mathfrak{p}}} \quad \text{with } n_{\mathfrak{p}} = \sum_{\mathfrak{P}\,|\,\mathfrak{p}} c(\mathfrak{P}) f(\mathfrak{P}|\mathfrak{p})\,.$$

On the other hand,

$$\begin{aligned}\prod_{\mathfrak{P}\,|\,\mathfrak{p}} \mathfrak{d}_{\hat{B}_{\mathfrak{P}}/\hat{A}_{\mathfrak{p}}} &= \prod_{\mathfrak{P}\,|\,\mathfrak{p}} N_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}\big(\mathfrak{D}_{\hat{B}_{\mathfrak{P}}/\hat{A}_{\mathfrak{p}}}\big) = \prod_{\mathfrak{P}\,|\,\mathfrak{p}} N_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}\big(\mathfrak{D}_{B/A}\hat{B}_{\mathfrak{P}}\big) \\ &= \prod_{\mathfrak{P}\,|\,\mathfrak{p}} N_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}\big(\mathfrak{P}^{c(\mathfrak{P})}\hat{B}_{\mathfrak{P}}\big) = \prod_{\mathfrak{P}\,|\,\mathfrak{p}} (\mathfrak{p}\hat{A}_{\mathfrak{p}})^{c(\mathfrak{P})f(\mathfrak{P}\,|\,\mathfrak{p})} = (\mathfrak{p}\hat{A}_{\mathfrak{p}})^{n_{\mathfrak{p}}}\,.\end{aligned}$$

This completes the proof. □

3.4.2 Different and ramification

Theorem 3.4.9. *Let $\mathfrak{P}$ be a maximal ideal of B lying over a maximal ideal $\mathfrak{p}$ of A.*

Then the extension L/K is unramified at $\mathfrak{P}$ if and only if $\mathfrak{P}$ does not divide the different $\mathfrak{D}_{B/A}$.

Proof. Since localization and completion do not alter the ramification index and the residue field extension, Prop. 3.4.8 allows us to reduce to the case where A is a complete DVR. In this case B is also a complete DVR and is a free A-module.

Let $k = A/\mathfrak{p}$ and $\overline{B} := B/\mathfrak{p}B = B \otimes_A k$. Let $\{e_i\}$ be a basis of B over A. By Prop. 2.4.25, the discriminant $\mathfrak{d}_{B/A}$ is the principal ideal generated by $d := \det(\mathrm{Tr}(e_i e_j))$. The images $\bar{e}_i$ of the e_i in $\overline{B}$ form a basis of $\overline{B}$ as a k-vector space. The discriminant of this basis, i.e., the determinant $\det(\mathrm{Tr}_{\overline{B}/k}(\bar{e}_i\bar{e}_j))$, is equal to the canonical image $\bar{d}$ of d in $\overline{B}$, by the compatibility of trace maps with base change (cf. (2.6.16.2)). By Prop. 3.4.5, $\mathfrak{P} \nmid \mathfrak{D}_{B/A}$ if and only if $\mathfrak{p} \nmid dA = \mathfrak{d}_{B/A}$, or equivalently, $\bar{d} \neq 0$ in k. This last condition means precisely that the k-bilinear form

$$\mathrm{Tr}_{\overline{B}/k} \,:\, \overline{B} \times \overline{B} \longrightarrow k \,;\, (x,\, y) \longmapsto \mathrm{Tr}_{\overline{B}/k}(xy)$$

is nondegenerate, since the Gram matrix of this bilinear form is $(\mathrm{Tr}_{\overline{B}/k}(\bar{e}_i\bar{e}_j))$. So, we are left to prove that the above trace form is nondegenerate if and only if L/K is unramified.

Let $\Pi \in B$ be a uniformizer and let $e = e(\mathfrak{P}|\mathfrak{p})$ be the ramification index. Then $\overline{B} = B/\Pi^e B$. If L/K is unramified, then $e = 1$ and $\overline{B} = B/\Pi B$ is a finite separable field extension of k. So $\mathrm{Tr}_{\overline{B}/k}$ is nondegenerate. Now suppose that L/K is ramified. Then either $e > 1$, or $\overline{B}$ is a field but not separable over k. In the latter case we already know that $\mathrm{Tr}_{\overline{B}/k}$ is degenerate (Cor. 1.2.6). So let us consider the case $e > 1$. In this case, the canonical image α of Π in $\overline{B} = B/\Pi^e B$ is a nonzero nilpotent element. For every $\beta \in \overline{B}$, the product $\alpha\beta$ is again nilpotent. Hence the k-linear map $\overline{B} \to \overline{B}\,;\ z \mapsto \alpha\beta z$ is a nilpotent linear transformation. Hence $\mathrm{Tr}_{\overline{B}/k}(\alpha\beta) = 0$ for all $\beta \in \overline{B}$. This shows that the trace form $\mathrm{Tr}_{\overline{B}/k}$ is degenerate. This completes the proof of the theorem. □

Corollary 3.4.10. *For a maximal ideal $\mathfrak{p}$ of A, the following assertions are equivalent:*

(i) *The extension L/K is unramified at $\mathfrak{p}$.*

(ii) *$\mathfrak{p}$ does not divide the discriminant $\mathfrak{d}_{L/K} = \mathfrak{d}_{B/A}$.*

Proof. This follows from Thm. 3.4.9 and Prop. 3.4.5. □

Theorem 3.4.11. *Let K be a number field. If every prime number p is unramified in K, then $K = \mathbb{Q}$.*

Proof. By Cor. 3.4.10, a prime number p ramifies in K if and only if p divides the discriminant d_K of K. By Thm. 2.6.12, if $K \neq \mathbb{Q}$, then $|d_K|$ has a prime divisor. So the result follows. □

4 Introduction to Class Field Theory

4.1 Local and global fields

4.1.1 Local Fields

Definition 4.1.1. A ***local field*** is a valued field K of one of the following types:
(1) $K = \mathbb{R}$ or $K = \mathbb{C}$ with the usual absolute value;
(2) K is complete with respect to a discrete valuation whose valuation ring has *finite* residue field.

The fields $\mathbb{R}$ and $\mathbb{C}$ are called ***archimedean local fields***. A local field of the second type is called ***non-archimedean***. ■

We say that a topological space X is ***locally compact*** if every point $x \in X$ has a compact neighborhood (i.e., a compact subset containing an open neighborhood of x). Clearly, an archimedean local field is locally compact. This is also true for a non-archimedean local field.

Theorem 4.1.2. *Let K be a non-archimedean local field. Then K is locally compact and its valuation ring $\mathcal{O}_K$ is compact. Moreover, every compact subring of K is contained in $\mathcal{O}_K$.*

Proof. Let $\pi \in \mathcal{O}_K$ be a uniformizer. Then the open subsets $\pi^n\mathcal{O}_K$, $n \geq 1$ form a basis of open neighborhoods of 0 in K, and each of these open subsets are homeomorphic to $\mathcal{O}_K$. So the compactness of $\mathcal{O}_K$ implies the local compactness of K.

To prove that $\mathcal{O}_K$ is compact, we use the following two facts:

(1) In a metric space, a subspace X is compact if and only if it is sequentially compact (i.e., every sequence $(x_n)_{n\geq 0}$ in X has a convergent subsequence whose limit lies in X). (See e.g. [Mun00, Thm. 28.2].)

(2) A series $\sum_{n\geq 0} a_n$ in K converges if and only if the sequence (a_n) converges to 0 (Exercise).

Now consider a sequence $(x_n)_{n\geq 0}$ in $\mathcal{O}_K$. We want to show that it has a subsequence converging to a limit in $\mathcal{O}_K$. Since $\mathcal{O}_K$ is closed, it suffices to find a convergent subsequence. If the set $\{x_n \,|\, n \geq 0\}$ is finite, the result is clear. By extracting a subsequence if necessary, we may assume that the sequence (x_n) consists of pairwise distinct elements.

We claim that there is a strictly increasing sequence of integers $0 \leq n_0 < n_1 < n_2 < \cdots$ such that

$$x_{n_r} \equiv x_{n_{r-1}} \pmod{\pi^r\mathcal{O}_K} \quad \text{for all } r \geq 1\,.$$

Indeed, since the residue field $\mathcal{O}_K/\pi\mathcal{O}_K$ is finite, we can first choose $n_0 \geq 0$ such that the coset $x_{n_0} + \pi\mathcal{O}_K$ contains infinitely many elements of $\{x_n\}$. Similarly, $x_{n_0} + \pi\mathcal{O}_K$ is a union of finitely many cosets of $\mathcal{O}_K$ mod $\pi^2\mathcal{O}_K$. At least one of them contains infinitely many x_n. So we can find $n_1 > n_0$ such that $x_{n_1} + \pi^2\mathcal{O}_K \subseteq x_{n_0} + \pi\mathcal{O}_K$ and that $x_{n_1} + \pi^2\mathcal{O}_K$ contains infinitely many x_n. Continuing this way we obtain a subsequence (x_{n_r}) of (x_n) such that

$$x_{n_r} + \pi^{r+1}\mathcal{O}_K \subseteq x_{n_{r-1}} + \pi^r\mathcal{O}_K\,.$$

This proves our claim.

Define $a_r = x_{n_r}$ for each $r \in \mathbb{N}$. Then the series $\sum_{r\geq 1}(a_r - a_{r-1})$ converges, i.e., the sequence $a_r - a_0$ converges. So (a_r) is a convergent subsequence of (x_n). This proves the sequential compactness of $\mathcal{O}_K$ and hence also its compactness.

Finally, let $R \subseteq K$ be a compact subring. If there exists $x \in R \setminus \mathcal{O}_K$, then the sequence $(x^n) \subseteq R$ does not have a convergent subsequence, contradicting the sequential compactness of R. □

Remark 4.1.3. In fact, for any topological field K (i.e. a field equipped with a topology for which the usual 4 algebraic operations $+$, $-$, $\times$ and $\div$ are all continuous), if K is locally compact, Hausdorff and non-discrete, then K is a local field. A proof can be found in [Bou06, §VI.9.3, Thm. 1]. ■

Proposition 4.1.4. *Let K be a non-archimedean local field and let p be the characteristic of its residue field.*

Then either K is a p-adic field (i.e., a finite extension of $\mathbb{Q}_p$) or $K \cong \mathbb{F}(\!(t)\!)$ for some finite extension $\mathbb{F}$ of $\mathbb{F}_p$. (In the former case $\mathrm{char}(K) = 0$ and in the latter case K is a finite separable extension of $\mathbb{F}_p(\!(t)\!)$.)

Proof. See (the proof of) [Neu99, Prop. II.5.2]. □

(4.1.5) Let K be a local field. The ***normalized absolute value*** on F, denoted $\|\cdot\|_K$, is defined as follows:

(1) If F is non-archimedean, then

$$\|x\|_K := |\kappa|^{-v_K(x)} \quad \text{for all} \quad x \in K$$

where v_K is the normalized discrete valuation on K and κ denotes its residue field.

(2) If $K = \mathbb{R}$, $\|\cdot\|_K$ is the usual absolute value $|\cdot|_{\mathbb{R}}$ on $\mathbb{R}$.

(3) If $K = \mathbb{C}$, $\|\cdot\|_K$ is the square $|\cdot|_{\mathbb{C}}^2$ of the standard absolute value on $\mathbb{C}$ (so that $\|1+\mathrm{i}\|_{\mathbb{C}} = \|\sqrt{2}\|_{\mathbb{C}} = 2 \neq \|\sqrt{2}\|_{\mathbb{R}}$). ■

Lemma 4.1.6. *Let L/K be a finite extension of local fields. Then*

$$\forall\, x \in L\,,\ \|x\|_L = \|N_{L/K}(x)\|_K\,.$$

Proof. Exercise. □

4.1.2 Global fields and their places

(4.1.7) A field K is called a ***global function field*** if it is isomorphic to a finite extension of the rational function field $\mathbb{F}_p(t) = \mathrm{Frac}(\mathbb{F}_p[t])$ for some prime number p. By standard facts about transcendental field extensions (cf. [Mor96, § 19]), a global function field is the same as a finitely generated extension of transcendence degree 1 over a finite field.[§] Moreover, it can be shown that if K is a global function field of characteristic p, then there exists an element $u \in K$ which is transcendental over its prime field $\mathbb{F}_p$, such that K is a finite separable extension of $\mathbb{F}_p(u)$ (cf. [Mor96, Cor. 20.22]). Therefore, we may also have defined a global function field as a finite *separable* extension of a rational function field $\mathbb{F}_p(u)$.

A ***global field*** is either a number field (as already defined in (2.2.1)) or a global function field. ■

(4.1.8) Let K be a global field. A ***place*** (or a ***prime***) of K is an equivalence class of nontrivial absolute values on K. We denote by Ω_K the set of places of K. For each $v \in \Omega_K$, we shall denote by K_v the completion of K with respect to any absolute value in the class v. A place $v \in \Omega_K$ is called ***finite*** or ***non-archimedean*** (resp. ***infinite*** or ***archimedean***) if the associated absolute value is non-archimedean (resp. archimedean). In case v is infinite, the completion K_v is either $\mathbb{R}$ or $\mathbb{C}$ by Ostrowski's theorem (Thm. 3.1.15). We say v is ***real*** (resp. ***complex***) if $K_v \cong \mathbb{R}$ (resp. $K_v \cong \mathbb{C}$).

Since a field of positive characteristic has no archimedean absolute values (Prop. 3.1.4), a global function field has no archimedean places.

Let L/K be a finite extension of global fields. Clearly, equivalent absolute values of L when restricted to K yield equivalent absolute values on K. So we have a well defined restriction map

$$\Omega_L \longrightarrow \Omega_K\,; \quad w \longmapsto w|_K\,. \tag{4.1.8.1}$$

[§] In algebro-geometric languages, a global function field is the function field of an irreducible algebraic curve over a finite field.

For any $w \in \Omega_L$ and $v \in \Omega_K$, we say w ***lies over*** v and we write $w \,|\, v$ if $v = w|_L$, that is, the restriction to K of any absolute value in the class w is equivalent to any absolute value in the class v. When $w \,|\, v$, the completion L_w is a finite extension of K_v, which is separable (resp. Galois) if L/K is separable (resp. Galois) by Cor. 3.2.19.

As we have discussed in (3.2.18) and (3.2.26), every absolute value of K has a finite nonempty set of extensions to L, so the map (4.1.8.1) is surjective with finite fibers. The following statements are easy consequences of this surjectivity:

1. Let K be a number field. Then K has a finite nonempty set of archimedean places. More precisely, Thm. 3.2.24 tells us that a real place is uniquely determined by a real embedding $\tau : K \hookrightarrow \mathbb{R}$ and a complex place corresponds to a pair of conjugate imaginary embeddings $\sigma, \overline{\sigma} : K \hookrightarrow \mathbb{C}$.

   A non-archimedean place of K lies over (the equivalence class of) the p-adic valuation for some prime number p (by Thm. 3.1.8). It is therefore (the equivalence class of) the discrete valuation associated to a maximal ideal $\mathfrak{p} \in \mathrm{Spm}(\mathcal{O}_K)$ lying over p (by (3.3.4)).

2. Let K be a global function field of characteristic p. We can regard K as a finite separable extension of $\mathbb{F}_p(t)$ (as has been said in (4.1.7)). Then, by Thm. 3.1.9, every place $v \in \Omega_K$ lies either over the degree valuation v_∞ of $\mathbb{F}_p(t)$ or over the f-adic valuation v_f associated to an irreducible polynomial $f \in \mathbb{F}_p[t]$.

From the above description of Ω_K, we see that for every $v \in \Omega_K$ the completion K_v is a local field. Conversely, if F is a local field, then $F \cong K_v$ for some global field K and some $v \in \Omega_K$ by Props. 3.2.21 and 4.1.4. ■

If K is a global field and $v \in \Omega_K$, we shall write $\|\cdot\|_v$ for the normalized absolute value on the local field K_v. It can be viewed as a function on K via the natural embedding $K \hookrightarrow K_v$.

Lemma 4.1.9. *Let K be a global field and $\alpha \in K^*$.*
Then $\|\alpha\|_v = 1$ for all but finitely many places $v \in \Omega_K$.

Proof. In view of Lemma 4.1.6, it suffices to prove the assertion for $K = \mathbb{Q}$ and $K = \mathbb{F}_p(t)$. In these two special cases, one can easily check the lemma by using the description of Ω_K given in (4.1.8). □

Theorem 4.1.10 (Product formula)**.** *Let K be a global field and $\alpha \in K^*$. Then*

$$\prod_{v \in \Omega_K} \|\alpha\|_v = 1\,.$$

Proof. Again, we may assume $K = \mathbb{Q}$ or $K = \mathbb{F}_p(t)$ and then deduce easily the result using the description of Ω_K. The details are left to the reader. □

4.1.3 Adèles and idèles

Historically the *idèles* were introduced by Chevalley in [Che36] under the name "élément idéal", which he then abbreviated to "idèle" in [Che40] following a suggestion of Hasse. This was to formulate class field theory for infinite extensions in terms of topological groups. Weil [Wei38] defined (but did not name) the ring of adèles in the function field case and pointed out that Chevalley's group of *Idealelemente* was the group of invertible elements of this ring. Tate in his thesis [Tat50] (reproduced in [Tat67]) defined the ring of adèles as a restricted product, though he called its elements "valuation vectors" rather than adèles. Chevalley [Che51] defined the ring of adèles in the function field case, under the name "repartitions". The term *adèle* (short for additive idèles, and also a French woman's name) was in use shortly afterwards ([Jaf56]) and may have been introduced by André Weil.

Throughout this subsection, let K be a global field. For each finite place $v \in \Omega_K$, let $\widehat{\mathcal{O}}_v$ denote the valuation ring of the local field K_v.

Definition 4.1.11. For any finite subset $S \subseteq \Omega_K$ containing all archimedean places, the ring of S-***adèles*** of K is defined as

$$\mathbf{A}_{K,S} := \prod_{v \in S} K_v \times \prod_{v \notin S} \widehat{\mathcal{O}}_v \, .$$

We shall endow $\mathbf{A}_{K,S}$ with the product topology and view it as a topological ring. By Thm. 4.1.2, K_v is locally compact and Hausdorff for every (finite or infinite) place $v \in \Omega_K$ and $\widehat{\mathcal{O}}_v$ is compact and Hausdorff for every finite place v. By standard facts in topology, $\mathbf{A}_{K,S}$ is locally compact and Hausdorff.

The ***adèle ring*** $\mathbf{A}_K$ of K is defined by

$$\mathbf{A}_K := \bigcup_S \mathbf{A}_{K,S} \, ,$$

where S runs over all finite subsets of Ω_K containing all archimedean places. We topologize $\mathbf{A}_K$ by defining a subset $V \subseteq \mathbf{A}_K$ to be open if $V \cap \mathbf{A}_{K,S}$ is open in $\mathbf{A}_{K,S}$ for all S as above. This topology on $\mathbf{A}_K$ is called the ***adelic topology***. With this topology $\mathbf{A}_K$ is a locally compact Hausdorff topological group.

The image of the diagonal embedding $K \to \prod_{v \in \Omega_K} K_v$ is contained in $\mathbf{A}_K$ (Lemma 4.1.9). It consists of adèles every one of whose components is equal to a same element of K. Such an adèle is referred to as a ***principal adèle***. We shall often identify K with the subring of principal adèles in $\mathbf{A}_K$. ■

Theorem 4.1.12. *The topology on K induced by the inclusion $K \subseteq \mathbf{A}_K$ is discrete, the image of K in $\mathbf{A}_K$ is closed and the quotient space $\mathbf{A}_K/K$ is compact Hausdorff.*

Proof. See [RV99, Thm. 5.11]. □

Theorem 4.1.13 (Strong approximation theorem)**.** *Let K be a global field and fix a place $v_0 \in \Omega_K$. Suppose we are given an adèle $\alpha = (a_v) \in \mathbf{A}_K$, a finite subset S of $\Omega_K \setminus \{v_0\}$ and a real number $\varepsilon > 0$.*

Then there is an element $x \in K$ such that

$$\begin{cases} \|a_v - x\|_v < \varepsilon & \text{for all } v \in S \\ \|a_v - x\|_v \leq 1 & \text{for all finite places } v \notin S \cup \{v_0\}\,. \end{cases}$$

Proof. See e.g. [CF67, p.67, § II.15, Theorem]. □

Briefly speaking, strong approximation allows one to choose $x \in K$ approximating $\alpha = (a_v)$ at all places in a given finite set S such that $a_v - x$ is integral at all finite places not in S except potentially one. The weak approximation theorem (Thm. 3.1.10) is the weaker statement that, for any finite subset $S \subseteq \Omega_K$, any $\alpha = (a_v) \in \mathbf{A}_K$ and any real number $\varepsilon > 0$, there exists $x \in K$ such that $\|a_v - x\|_v < \varepsilon$ for all $v \in S$.

Definition 4.1.14. Let $S \subseteq \Omega_K$ be a finite subset containing the archimedean places. This is clearly an open subring of $\mathbf{A}_K$. We define the group of S-***idèles*** by

$$\mathbf{I}_{K,S} := \prod_{v \in S} K_v^* \times \prod_{v \notin S} \widehat{\mathcal{O}}_v^*\,. \tag{4.1.14.1}$$

It is endowed with the product topology, which makes it into a locally compact Hausdorff topological group.

The group of ***idèles*** of K is defined by

$$\mathbf{I}_K := \bigcup_S \mathbf{I}_{K,S}\,,$$

where S runs over all finite subsets of Ω_K containing the archimedean places. As in the case of adèles, we define the ***idelic topology*** by declaring a subset of $\mathbf{I}_K$ to be open if its intersection with every $\mathbf{I}_{K,S}$ is open. In this way $\mathbf{I}_K$ becomes a locally compact Hausdorff topological group.

Elements in the image of the diagonal map $K^* \to \mathbf{I}_K$ are called ***principal idèles***. The quotient

$$\mathbf{C}_K := \mathbf{I}_K / K^*$$

is called the ***idèle class group*** of K. With the quotient topology of the idelic topology, $\mathbf{C}_K$ is a locally compact topological group. ■

Remark 4.1.15. It is obvious that in the purely algebraic sense (i.e. disregarding the topologies), $\mathbf{I}_K$ is the group of units in the ring $\mathbf{A}_K$. The natural inclusion map $\iota : \mathbf{I}_K \hookrightarrow \mathbf{A}_K$ is continuous with respect to the idelic and adelic topologies, but its image is not open in $\mathbf{A}_K$. Hence, the idelic topology of $\mathbf{I}_K$ is not the subspace topology of the adelic topology induced from the inclusion $\iota : \mathbf{I}_K \hookrightarrow \mathbf{A}_K$. ■

Lemma 4.1.16. *The image of the diagonal inclusion $K^* \to \mathbf{I}_K$ is a discrete, closed subgroup of $\mathbf{I}_K$.*

Proof. By Thm. 4.1.12, K^* is closed and discrete in $\mathbf{I}_K$ already in the adelic topology, which is weaker than the idelic topology. □

Corollary 4.1.17. *The idèle class group* $\mathbf{C}_K$ *of any global field* K *is a locally compact Hausdorff group.*

Proof. We already know that $\mathbf{C}_K$ is locally compact. Since K^* is closed in $\mathbf{I}_K$ (Lemma 4.1.16), $\mathbf{C}_K$ is Hausdorff. (In general, if H is a normal subgroup of a topological group G, the quotient G/H is Hausdorff if H is closed in G by [RV99, p.6, Prop. 1.4]). □

Definition 4.1.18. The ***idelic norm*** of K is the function

$$\|\cdot\|_K : \mathbf{I}_K \longrightarrow \mathbb{R}_+^* = \{\, x \in \mathbb{R} \,|\, x > 0 \,\}$$

given by

$$\|(a_v)\|_K := \prod_{v \in \Omega_K} \|a_v\|_v \,.$$

This is clearly a continuous group homomorphism. Its kernel is denoted by $\mathbf{I}_K^1$ and called the group of ***unit idèles*** or ***norm one idèles***. ■

Theorem 4.1.19. *The topological quotient* $\mathbf{I}_K^1/K^*$ *is a compact Hausdorff group.*

Proof. See e.g. [CF67, p.70, § II.16, Theorem]. □

4.1.4 What is class field theory

In [Che40, p.394], Chevalley wrote:

"*L'objet de la théorie du corps de classes est de montrer comment les extensions abéliennes d'un corps de nombres algébriques* K *peuvent être déterminées par des éléments tirés de la connaissance de* K *lui-même; ou, si l'on veut présenter les choses en termes dialectiques, comment un corps possèede en soi les éléments de son propre dépassement (et ce, san aucune contradiction interne!).*"‖

This paragraph nicely describes what class field theory is in a narrow, classical sense. In a more general sense, class field theory includes the study of all Galois extensions of local and global fields. The notion of *class field* is often attributed to Hilbert. But it was already familiar for Kronecker and the term was actually coined by Weber before Hilbert's fundamental papers (between 1896 and 1900, including his *Zahlbericht* published in 1897) came out ([Has67, p.266]).

The origins of class field theory lie in the quadratic reciprocity law proved by Gauss, the generalization of which took place as a long-term historical project. Another source of ideas of class field theory is the Kronecker–Weber theorem about abelian extensions of the rational numbers. This theorem was first announced by Kronecker in 1853 and proved (with a minor gap) by Weber in 1886. Roughly between 1896 and 1898, Hilbert gives a simpler (and complete) proof of the Kronecker–Weber theorem, rewrites the law of quadratic reciprocity as a product formula for the *Hilbert symbol*, conjectures the

‖A Chinese translation: "类域论的目标是解释一个代数数域 K 的 Abel 扩张如何由这个域自身的信息决定; 或者, 如果我们想用更加辩证的术语来说, 一个域如何将超越自身的要素蕴含在自身之内(并且不产生任何内在矛盾)." For an English translation, see e.g. the introduction in [Mil20].

existence and basic properties of the narrow *Hilbert class field* and proves them in the special case of class number 2.

At least two of Hilbert's famous 23 problems, some of which appearing in his Paris ICM lecture in 1900, stimulated further developments of class field theory. These are:

Hilbert's 9th problem: *Find the most general law of the reciprocity theorem in any algebraic number field.*

Hilbert's 12th problem: *Extend the Kronecker–Weber theorem on abelian extensions of the rational numbers to any algebraic number field.*

By works of Takagi (高木貞治), Furtwängler, Artin, Hasse and many others, all the main results in the classical (abelian) class field theory were established by about 1930. For nonabelian extensions, the first indication of the shape the theory should take is in a letter from Langlands to Weil in 1967. The Langlands program, which presents a wealth of far-reaching and influential conjectures, is often viewed as a nonabelian class field theory. In recent years there has been much progress in the nonabelian local and function field cases, but less in the number field case. Beginning about 1980, abelian class field theory has been successfully extended to higher dimensional fields.

For more details about the history of class field theory, we refer the reader to the well written surveys [Has67], [Con] and [Roq01].

4.2 Local class field theory

In this section, let K denote a non-archimedean local field with residue field k, and let $p = \mathrm{char}(k)$. We denote by $\overline{K}$ a fixed algebraic closure of K and consider all the algebraic extensions of K as subfields of $\overline{K}$.

4.2.1 The reciprocity map

(4.2.1) We use the following notation for any finite extension L/K:

- Let v_L denote the normalized discrete valuation on L.
- Let $\mathcal{O}_L$ be the valuation ring of L, $\mathfrak{p}_L$ the maximal ideal of $\mathcal{O}_L$, and $U_L = \mathcal{O}_L^*$ the group of units in $\mathcal{O}_L$.
- If ℓ/k is the residue field extension of L/K and $q = |k|$, denote by

$$\mathfrak{F}_{\ell/k} : \ell \longrightarrow \ell \ ; \ x \longmapsto x^q$$

the ***Frobenius*** automorphism of ℓ/k. It is a generator of the Galois group $\mathrm{Gal}(\ell/k)$.

If L/K is an unramified extension, then by Thm. 3.3.14, L/K is a Galois extension and $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(\ell/k)$. In this case, we denote by $\mathfrak{F}_L = \mathfrak{F}_{L/K} \in \mathrm{Gal}(L/K)$ the element corresponding to the Frobenius automorphism of ℓ/k. ■

(4.2.2) We also need some group-theoretic concepts.

Let G be a group. We denote by $[G, G]$ the ***commutator subgroup*** of G, i.e., the subgroup of G generated by elements of form $\sigma\tau\sigma^{-1}\tau^{-1}$, $\sigma, \tau \in G$. The quotient group $G/[G, G]$ is called the ***abelianization*** of G. When G is a finite group, we write $G^{ab} := G/[G, G]$.

For a subgroup of finite index H in G, we have a ***transfer*** (***Verlagerung*** in German) map $\mathrm{Ver} : G/[G, G] \to H/[H, H]$ defined as follows (cf. [Ser79, § VII.8]): Let S be a complete system of representatives of the right cosets of H in G. For each $\sigma \in G$ and $s \in S$, let $h_{\sigma, s} \in H$ be the element such that

$$\sigma s = h_{\sigma, s} s' \quad \text{for some } s' \in S\,.$$

We define

$$\mathrm{Ver}(\sigma.[G, G]) := \prod_{s \in S} h_{\sigma, s}.[H, H]\,.$$

One can also interpret Ver as the restriction map $H_1(G, \mathbb{Z}) \to H_1(H, \mathbb{Z})$ in group homology. (When G is finite, the map Ver is also the Pontryagin dual of the corestriction map $H^1(H, \mathbb{Q}/\mathbb{Z}) \to H^1(G, \mathbb{Q}/\mathbb{Z})$. See e.g. [NSW00, Prop. 1.5.9]. ■

We now state the mains results in local class field theory. The proofs can be found in standard references such as [Neu99], [Neu86], [AT09] and so on.

Recall that a field extension E/F is called ***abelian*** (resp. ***cyclic***) if it is a Galois extension whose Galois group is abelian (resp. cyclic).

Theorem 4.2.3. *For every finite Galois extension L/K, there is a canonical group homomorphism,*

$$\Psi_{L/K} \;:\; K^* \longrightarrow \mathrm{Gal}(L/K)^{ab}$$

satisfying the following properties:

1. *The map $\Psi_{L/K}$ is surjective with kernel $\mathrm{Ker}(\Psi_{L/K}) = N_{L/K}(L^*)$.*
2. *If L/K is unramified, then*

$$\forall\, x \in K^*\,,\ \Psi_{L/K}(x) = \mathfrak{F}_{L/K}^{v_K(x)}\,.$$

3. *For any field automorphism $\sigma : \overline{K} \to \overline{K}$, the following diagram commutes:*

$$\begin{array}{ccc} K^* & \xrightarrow{\ \sigma\ } & (\sigma K)^* \\ {\scriptstyle \Psi_{L/K}}\downarrow & & \downarrow{\scriptstyle \Psi_{\sigma L/\sigma K}} \\ \mathrm{Gal}(L/K)^{ab} & \xrightarrow{\ \mathrm{Int}(\sigma)\ } & \mathrm{Gal}(\sigma L/\sigma K)^{ab} \end{array}$$

Here $\mathrm{Int}(\sigma)$ denotes the isomorphism

$$\mathrm{Gal}(L/K) \xrightarrow{\sim} \mathrm{Gal}(\sigma L/\sigma K)\,; \quad \tau \longmapsto \sigma\tau\sigma^{-1}$$

given by conjugation.

4. *If M/K is a finite Galois extension containing L/K, then the diagram*

$$\begin{array}{ccc} K^* & \xrightarrow{\mathrm{Id}} & K^* \\ {\scriptstyle \Psi_{M/K}}\downarrow & & \downarrow{\scriptstyle \Psi_{L/K}} \\ \mathrm{Gal}(M/K)^{ab} & \xrightarrow{\sigma\mapsto\sigma|_L} & \mathrm{Gal}(L/K)^{ab} \end{array}$$

is commutative.

5. *If F/K is a subextension of L/K, then the following diagrams are commutative:*

$$\begin{array}{ccc} F^* & \xrightarrow{N_{F/K}} & K^* \\ {\scriptstyle \Psi_{L/F}}\downarrow & & \downarrow{\scriptstyle \Psi_{L/K}} \\ \mathrm{Gal}(L/F)^{ab} & \xrightarrow{\iota^{ab}} & \mathrm{Gal}(L/K)^{ab} \end{array} \qquad \begin{array}{ccc} K^* & \xrightarrow{\textit{inclusion}} & F^* \\ {\scriptstyle \Psi_{L/K}}\downarrow & & \downarrow{\scriptstyle \Psi_{L/F}} \\ \mathrm{Gal}(L/K)^{ab} & \xrightarrow{\mathrm{Ver}} & \mathrm{Gal}(L/F)^{ab} \end{array}$$

where ι^{ab} is the natural map induced from the inclusion $\mathrm{Gal}(L/F) \hookrightarrow \mathrm{Gal}(L/K)$ and Ver *denotes the group theoretic transfer map described in* (4.2.2).

Definition 4.2.4. With notation as in Thm. 4.2.3, the map $\Psi_{L/K} : K^* \to \mathrm{Gal}(L/K)^{ab}$ or the induced map $\Psi_{L/K} : K^*/N_{L/K}(L^*)$ is called the ***Artin reciprocity map***, or the ***norm residue symbol*** of L/K. It is also common to denote it by $(\cdot, L/K)$. ■

Remark 4.2.5. In Thm. 4.2.3 (2) we have given an explicit formula for the Artin reciprocity map in the case of unramified extensions. To describe explicitly the map $\Psi_{L/K}$ for an arbitrary finite Galois extension, we may use Thm. 4.2.3 (4) to reduce to the abelian case. Then the Artin map can be determined by using the Lubin–Tate theory (see e.g. [Iwa86, Chap. VI], [Neu99, § V.5] or [Har20, Chap. 11]). ■

We leave it to the reader to check that the statements in Thm. 4.2.3 imply the following[‖]:

Proposition 4.2.6. *Let L/K be a finite abelian extension and let $I(L/K)$ be the inertia subgroup of* $\mathrm{Gal}(L/K)$.

The Artin reciprocity map $\Psi_{L/K} : K^* \to \mathrm{Gal}(L/K)$ maps U_K surjectively onto the inertia subgroup $I(L/K)$ and induces an isomorphism $U_K/N_{L/K}(U_L) \cong I(L/K)$. In particular, L/K is unramified if and only if $U_K = N_{L/K}(U_L)$.

Definition 4.2.7. For each $n \in \mathbb{N}$, put

$$U_K^{(n)} := \{x \in K \,|\, v_K(x-1) \geq n\} \quad (\text{with } U_K^{(0)} = U_K)\,.$$

The ***Artin conductor*** of a finite abelian extension L/K is defined to be the ideal

$$\mathfrak{f}_{L/K} = \mathfrak{p}_K^m \quad \text{where} \quad m = \min\{n \in \mathbb{N} \,|\, U_K^{(n)} \subseteq N_{L/K}(L^*)\}\,.$$

[‖]Here we are claiming that the assertions of Prop. 4.2.6 can be deduced from those of Thm. 4.2.3. However, we don't want to say that to prove these two results, one should prove Thm. 4.2.3 first and then use it to obtain Prop. 4.2.6. In fact, these two results are usually proved in the reverse order.

Note that $\mathfrak{f}_{L/K}$ is well defined (cf. Thm. 4.2.9 (1) below), because every open subgroup of K^* contains $U_K^{(n)}$ for some $n \in \mathbb{N}$, as these form a basis of open neighborhoods of 1 in K^*. (This also shows that if K is a p-adic field, every open subgroup of K^* has finite index.)

When $\mathfrak{f}_{L/K}$ is $\mathfrak{p}_K^0 = \mathcal{O}_K$, we also write $\mathfrak{f}_{L/K} = (1)$. ■

Proposition 4.2.8 (Conductor theorem)**.** *A finite abelian extension L/K is unramified if and only if $\mathfrak{f}_{L/K} = (1)$.*

Proof. This is a restatement of the last assertion in Prop. 4.2.6. □

Theorem 4.2.9. *Let L/K be a finite separable extension.*

1. *The norm subgroup $N_{L/K}(L^*)$ is a finite-index open subgroup of K^*.*
2. *(Norm index inequalities) Let F/K be the maximal abelian subextension of L/K. Then*
$$N_{L/K}(L^*) = N_{F/K}(F^*) \quad \text{and} \quad [K^* : N_{F/K}(F^*)] = [F : K] \leq [L : K]\,.$$
3. *(Existence theorem) The map*
$$\{\text{finite abelian extensions of } K \text{ (in } \overline{K})\} \longrightarrow \{\text{finite-index open subgroups of } K^*\}$$
$$E \longmapsto N_{E/K}(E^*)$$
is an inclusion-reversing bijection.

The extension E/K corresponding to a finite-index open subgroup $N \leq K^*$ is called the **class field** *belonging to N.*

(4.2.10) Let E/F be a finite extension of archimedean local fields. That is, E/F is
$$\mathbb{C}/\mathbb{C}\,,\ \mathbb{C}/\mathbb{R} \quad \text{or} \quad \mathbb{R}/\mathbb{R}\,.$$
If E/F is $\mathbb{C}/\mathbb{R}$, we say that E/F is ***ramified***[**]; in the other two cases, we say that E/F is ***unramified***.

By the ***Frobenius*** of E/F we shall mean the unique generator $\mathfrak{F}_{E/F}$ of the Galois group $\mathrm{Gal}(E/F)$.

There is a unique injective homomorphism $F^*/F^{*2} \hookrightarrow \mathbb{Z}/2\mathbb{Z}$. We define $v_F : F^* \to \mathbb{Z}/2\mathbb{Z}$ to be the composite map
$$v_F \ :\ F^* \longrightarrow F^*/F^{*2} \hookrightarrow \mathbb{Z}/2\mathbb{Z}\,.$$
We define the ***Artin reciprocity map***, or the ***norm residue symbol***, by
$$\Psi_{E/F} \ :\ F^* \longrightarrow \mathrm{Gal}(E/F)\ ; \quad x \longmapsto \mathfrak{F}_{E/F}^{v_F(x)}\,.$$
It is easily verified that with the above definitions, the statements of Theorems 4.2.3 and 4.2.9 remain valid for archimedean local fields. ■

[**]Our convention here is the usual one used in most textbooks (such as [Neu86], [AT09], etc.), but is different from that of [Neu99, p.184, § III.1].

4.2.2 The Hilbert symbol

In this subsection, let F be a (non-archimedean or archimedean) local field with an algebraic closure $\overline{F}$.

We fix a positive integer $n \geq 2$ which is not divisible by the characteristic of F, and we assume that F contains a primitive n-root of unity $\xi = \xi_n \in \overline{F}$. (If $F = \mathbb{R}$, then $n = 2$.) Let $F^{*n} = \{x^n \,|\, x \in F^*\}$.

We define $F(\sqrt[n]{F^*})/F$ to be the subextension of $\overline{F}/F$ generated by all the elements $\sqrt[n]{a}$, $a \in F^*$, i.e., $F(\sqrt[n]{F^*}) := F(\{\sqrt[n]{a} \,|\, a \in F^*\})$.

Proposition 4.2.11. *Let $L = F(\sqrt[n]{F^*})$.*

1. *The extension L/F is a finite abelian extension with n-torsion Galois group and for any finite abelian extension E/F whose Galois group is n-torsion, we have $E \subseteq L$.*

   Furthermore, the map

   $$\mathrm{Gal}(L/F) \times F^*/F^{*n} \longrightarrow \mu_n(F)\,; \quad (\sigma\,,\, \alpha F^{*n}) \longmapsto \frac{\sigma(\sqrt[n]{\alpha})}{\sqrt[n]{\alpha}} \tag{4.2.11.1}$$

   is a nondegenerate bilinear (in the multiplicative sense) pairing, called the **Kummer pairing**, *which induces a canonical isomorphism*

   $$F^*/F^{*n} \cong \mathrm{Hom}\big(\mathrm{Gal}(L/F),\, \mu_n(F)\big) \tag{4.2.11.2}$$

2. *We have $N_{L/F}(L^*) = F^{*n}$.*

Proof. (1) As an exercise, one can show that F^*/F^{*n} is a finite group. So L/F is a finite extension. The other assertions are standard results of the "Kummer theory" (see e.g. [Mor96, § 11]).

(2) The isomorphism (4.2.11.1) shows $|\mathrm{Gal}(L/F)| = [F^* : F^{*n}]$. On the other hand, $[F^* : N_{L/F}(L^*)] = |\mathrm{Gal}(L/K)|$ by Theorem 4.2.3 or Theorem 4.2.9 (together with (4.2.10) in the archimedean case), and

$$F^*/N_{L/F}(L^*) \cong \mathrm{Gal}(L/F)$$

is n-torsion, whence $F^{*n} \subseteq N_{L/F}(L^*)$. So it follows that $F^{*n} = N_{L/F}(L^*)$. □

(4.2.12) Let $c \in F^*$, and let $\sqrt[n]{c} \in \overline{F}$ be a fixed n-th root of c. By Kummer theory, the extension $F(\sqrt[n]{c})/F$ is a finite cyclic extension whose degree is equal to the order of cF^{*n} in F^*/F^{*n}. For any $\sigma \in \mathrm{Gal}(F(\sqrt[n]{c})/F)$, the element $\sigma(\sqrt[n]{c})$ is another n-th root of c, hence $\sigma(\sqrt[n]{c})/\sqrt[n]{c} \in \mu_n(F)$.

We now define the ***Hilbert symbol*** of F as the map

$$(\cdot,\,\cdot)_{n,\,F} \;:\; F^* \times F^* \longrightarrow \mu_n(F)\,; \quad (a,\,b) \mapsto \frac{(a\,,\, F(\sqrt[n]{b})/F)\,\sqrt[n]{b}}{\sqrt[n]{b}}\,,$$

where $(a,\, F(\sqrt[n]{b})/F) \in \mathrm{Gal}(F(\sqrt[n]{b})/F)$ denotes the image of $a \in F^*$ under the norm residue symbol (Definition 4.2.4).

Whenever there is no risk of confusion, we may write $(\cdot,\,\cdot)_F$ or $(\cdot,\,\cdot)_n$ instead of $(\cdot,\,\cdot)_{n,\,F}$. ■

Example 4.2.13. Suppose $F = \mathbb{R}$ and $n = 2$. Then we have the following formula for the Hilbert symbol:

$$\forall\, a,\, b \in \mathbb{R}^*\,, \quad (a,\, b)_{\mathbb{R}} = \begin{cases} 1 & \text{if } a > 0 \text{ or } b > 0\,, \\ -1 & \text{otherwise}\,. \end{cases}$$

This can be checked directly from the definitions. ■

Proposition 4.2.14. *For all $a,\, a',\, b,\, b' \in F^*$, the following statements hold:*

1. *We have*
$$(aa',\, b)_F = (a,\, b)_F \cdot (a',\, b)_F\,,\ (a,\, bb')_F = (a,\, b)_F \cdot (a,\, b')_F\,.$$
2. *$(a,\, b)_F = 1$ if and only if a lies in the norm subgroup of the extension $F(\sqrt[n]{b})/F$.*
3. *If $(a,\, b)_F = 1$ for all $b \in F^*$, then $a \in F^{*n}$.*
4. *$(a,\, b)_F = (b,\, a)_F^{-1}$ and $(a,\, -a)_F = 1$.*
5. *If $a \neq 1$, then $(a,\, 1-a)_F = 1$.*

Proof. See e.g. [Neu99, Prop. V.3.2]. □

Now consider a non-archimedean local field K with residue characteristic p. The following proposition gives an explicit formula for the Hilbert symbol in the case $p \nmid n$. Notice that in this case $\mu_n(K) \cong \mu_n(k)$ by Prop. 2.5.6, and hence n divides $|k^*| = q - 1$.

Proposition 4.2.15. *Suppose $p \nmid n$. Then for all $a,\, b \in K^*$ we have*

$$(a,\, b)_{n,\,K} = (-1)^{v_K(a)v_K(b)} \overline{\left(\frac{b^{v_K(a)}}{a^{v_K(b)}} \right)}^{\frac{q-1}{n}}\,. \tag{4.2.15.1}$$

Here we have identifed $\mu_n(K)$ with $\mu_n(k)$ and we denote by $x \mapsto \bar{x}$ the natural reduction map $\mathcal{O}_K \to k$.

In particular, if $\pi \in K$ is a uniformizer, then

$$(\pi,\, u)_{n,\,K} = \bar{u}^{\frac{q-1}{n}} \ \in\ k^* \quad \text{for all } u \in U_K\,. \tag{4.2.15.2}$$

Proof. See e.g. [Neu99, Prop. V.3.4]. □

Definition 4.2.16. Suppose $p \nmid n$. The ***n-th power residue symbol*** on K is defined to be the function

$$\left(\frac{\cdot}{\mathfrak{p}_K} \right)_n \ :\ U_K \longrightarrow \mu_n(K)\,; \quad u \longmapsto (\pi,\, u)_{n,\,K}\,,$$

where π is a uniformizer of K. The formula (4.2.15.2) ensures that the above definition is independent of the choice of π and that $\left(\frac{u}{\mathfrak{p}_K}\right)_n$ is the n-th root of unity uniquely determined by the congruence

$$\left(\frac{u}{\mathfrak{p}_K} \right)_n \equiv u^{\frac{q-1}{n}} \pmod{\mathfrak{p}_K}\,.$$

Here again we have used the isomorphism $\mu_n(K) \cong \mu_n(k)$. ■

The following result is easily deduced.

Proposition 4.2.17. *Suppose $p \nmid n$ and let $u \in U_K$. Then*

$$\left(\frac{u}{\mathfrak{p}_K}\right)_n = 1 \iff u \text{ is an } n\text{-th power modulo } \mathfrak{p}_K\,.$$

4.3 Global class field theory

In this section, we state the main results in global class field theory. We omit all difficult (though important) proofs, which the interested reader may find in standard references ([CF67], [Neu86], [Neu99], [AT09], etc.).

Unless otherwise stated explicitly, in this section K denotes a global field with an algebraic closure $\overline{K}$. All algebraic extensions of K are considered as subfields of $\overline{K}$. The set of all places of K is denoted by Ω_K. As already said in (4.1.8), a global function field has no archimedean places and a number field has a nonempty finite set of archimedean places.

For each $v \in \Omega_K$, let K_v be the completion of K at v. If v is non-archimedean, let $\widehat{\mathcal{O}}_v$ be the valuation ring of K_v. If v is archimedean, we put $\widehat{\mathcal{O}}_v = K_v$ and hence $\widehat{\mathcal{O}}_v^* = K_v^*$.

Adèles, idèles and idèle classes have been defined in § 4.1.3.

4.3.1 Main theorems in terms of idèles

(4.3.1) Let L/K be a finite separable extension. For each $v \in \Omega_K$ we have a diagonal embedding $K_v \to \prod_{w|v} L_w$; this induces a natural injective ring homomorphism $\mathbf{A}_K \hookrightarrow \mathbf{A}_L$ which is compatible with the inclusions $K \hookrightarrow \mathbf{A}_K$ and $L \hookrightarrow \mathbf{A}_L$. It can be shown that the inclusion $\mathbf{A}_K \hookrightarrow \mathbf{A}_L$ is topologically a closed embedding (i.e., induces a homeomorphism of $\mathbf{A}_K$ onto a closed subspace of $\mathbf{A}_L$), and that it induces an isomorphism

$$\mathbf{A}_K \otimes_K L \xrightarrow{\sim} \mathbf{A}_L\,. \tag{4.3.1.1}$$

If if the tensor product $\mathbf{A}_K \otimes_K L$ is provided with the product topology on $\mathbf{A}_K^{\oplus[L:K]}$ induced by any choice of K-basis of L, the isomorphism (4.3.1.1) is in fact an isomorphism of topological rings.

We see in particular that $\mathbf{A}_L$ is a free $\mathbf{A}_K$-module of rank $[L : K]$. We have thus (cf. (2.6.16)) a norm map $N_{L/K} : \mathbf{A}_L \to \mathbf{A}_K$, which takes $\alpha \in \mathbf{A}_L$ to the determinant of multiplication by x as an $\mathbf{A}_K$-module endomorphism of $\mathbf{A}_L$. This norm is compatible with the norm map $N_{L/K} : L \to K$. More explicitly, we have

$$N_{L/K}\big((z_w)\big) = \left(\prod_{w|v} N_{L_w/K_v}(z_w)\right) \quad \text{for all } (z_w) \in \mathbf{A}_L\,. \tag{4.3.1.2}$$

Similarly, we have a natural inclusion of idèle groups $\mathbf{I}_K \hookrightarrow \mathbf{I}_L$ which is topologically a closed embedding. The norm map on adèles induces a norm map $N_{L/K} : \mathbf{I}_L \to \mathbf{I}_K$

and the formula (4.3.1.2) also holds for idèles. Clearly, by passing to quotients we also obtain a norm map

$$N_{L/K} \,:\, \mathbf{C}_L \longrightarrow \mathbf{C}_K$$

between the idèle class groups. ■

Proposition 4.3.2. *Let L/K be a finite separable extension.*

1. *The natural map $\mathbf{C}_K \to \mathbf{C}_L$ induced by the inclusion $\mathbf{I}_K \hookrightarrow \mathbf{I}_L$ is also a closed embedding (and in particular, injective and continuous).*
2. *The norm map $N_{L/K} : \mathbf{C}_L \to \mathbf{C}_K$ is a continuous open map. In particular, $N_{L/K}(\mathbf{C}_L)$ is an open subgroup of $\mathbf{C}_K$.*

(4.3.3) Let L/K be a finite separable extension and $v \in \Omega_K$.

For a place $w \in \Omega_L$ lyinig over v, we say that L/K is ***unramified*** at w if the extension L_w/K_v is unramified. In the non-archimedean case, this coincides with our earlier definition (Definition 2.4.5), as was discussed in (3.3.7). The definition of unramifiedness for archimedean local fields was given in (4.2.10). If L/K is unramified at every place $w|v$, we say that L/K is unramified at v.

We say that v ***splits completely*** in L/K if $L_w = K_v$ for every $w|v$. Thus, a complex place always splits completely, and a real place v splits completely in L if and only if its extensions to L are all real. From the definition it is clear that an archimedean place is unramified in L/K if and only if it splits completely in L/K. If v is non-archimedean, then by the fundamental equality (Cor. 3.3.3), v splits completely in L/K if and only if it has precisely $[L : K]$ extensions to L, if and only if $e(w|v) = f(w|v) = 1$ for all $w|v$ (so the definition again agrees with our earlier definition in Definition 2.4.5).

Now suppose L/K is a finite Galois extension and let $w|v$. By restriction we get a natural group homomorphism

$$\mathrm{Gal}(L_w/K_v) \longrightarrow \mathrm{Gal}(L/K)\,; \quad \sigma \longmapsto \sigma|_L\,.$$

Since the compositum of L and K_v inside L_w is equal to the whole of L_w, this map is injective. If w' is another place lying over v, then there exists $\tau_v \in \mathrm{Gal}(\overline{K}_v/K_v)$ such that $L_{w'} = \tau_v L_w$ inside $\overline{K}_v$ by Thm. 3.2.24. Thus, $\mathrm{Gal}(L_{w'}/K_v) = \tau_v \,\mathrm{Gal}(L_w/K_v)\tau_v^{-1}$ and the images of $\mathrm{Gal}(L_w/K_v)$ and $\mathrm{Gal}(L_{w'}/K_v)$ in $\mathrm{Gal}(L/K)$ are thus conjugate to each other. In particular, if L/K is an abelian extension, then $\mathrm{Gal}(L_w/K_v)$ and $\mathrm{Gal}(L_{w'}/K_v)$ are the same as subgroups of $\mathrm{Gal}(L/K)$.

When L/K is unramified at $w|v$, we may view the Frobenius $\mathfrak{F}_{w/v} := \mathfrak{F}_{L_w/K_v} \in \mathrm{Gal}(L_w/K_v)$ as an element of $\mathrm{Gal}(L/K)$. If moreover L/K is an abelian, then $\mathfrak{F}_{w/v}$ depends only on v, so in this case we may simply write $\mathfrak{F}_v$ for $\mathfrak{F}_{w/v}$.

When L/K is a finite abelian extension, it is easy to see that v splits completely in L/K if and only if it is unramified in L/K and $\mathfrak{F}_v = \mathrm{Id} \in \mathrm{Gal}(L/K)$. ■

Theorem 4.3.4. *For every finite Galois extension L/K, there is a canonical group homomorphism,*

$$\Psi_{L/K} \,:\, \mathbf{C}_K \longrightarrow \mathrm{Gal}(L/K)^{ab}$$

satisfying the following properties:

1. *The map* $\Psi_{L/K}$ *is surjective with kernel* $\mathrm{Ker}(\Psi_{L/K}) = N_{L/K}(\mathbf{C}_L)$.

2. *(Local-global compatibility) For every* $v \in \Omega_K$ *and every* $w \in \Omega_L$ *lying over* v*, the following diagram commutes*

$$\begin{array}{ccc} K_v^* & \longrightarrow & \mathbf{C}_K \\ {\scriptstyle \Psi_{L_w/K_v}}\downarrow & & \downarrow{\scriptstyle \Psi_{L/K}} \\ \mathrm{Gal}(L_w/K_v)^{ab} & \xrightarrow[\sigma\mapsto\sigma|_L]{} & \mathrm{Gal}(L/K)^{ab} \end{array}$$

where the upper horizontal map is induced from the natural injection

$$K_v^* \longrightarrow \mathbf{I}_K \ ; \ z \longmapsto \alpha = (\alpha_{v'}) \text{ with } \alpha_{v'} = \begin{cases} z & \text{for } v' = v\,, \\ 1 & \text{for } v' \neq v\,. \end{cases}$$

(Note that the induced map $K_v^* \to \mathbf{C}_K$ *is also injective.)*

3. *For any field automorphism* $\sigma : \overline{K} \to \overline{K}$*, the following diagram commutes:*

$$\begin{array}{ccc} \mathbf{C}_K & \xrightarrow{\sigma} & \mathbf{C}_{\sigma K} \\ {\scriptstyle \Psi_{L/K}}\downarrow & & \downarrow{\scriptstyle \Psi_{\sigma L/\sigma K}} \\ \mathrm{Gal}(L/K)^{ab} & \xrightarrow{\tau\longmapsto\sigma\tau\sigma^{-1}} & \mathrm{Gal}(\sigma L/\sigma K)^{ab} \end{array}$$

4. *If* M/K *is a finite Galois extension containing* L/K*, then the diagram*

$$\begin{array}{ccc} \mathbf{C}_K & \xrightarrow{\mathrm{Id}} & \mathbf{C}_K \\ {\scriptstyle \Psi_{M/K}}\downarrow & & \downarrow{\scriptstyle \Psi_{L/K}} \\ \mathrm{Gal}(M/K)^{ab} & \xrightarrow{\sigma\mapsto\sigma|_L} & \mathrm{Gal}(L/K)^{ab} \end{array}$$

is commutative.

5. *If* F/K *is a subextension of* L/K*, then the following diagrams are commutative:*

$$\begin{array}{ccc} \mathbf{C}_F & \xrightarrow{N_{F/K}} & \mathbf{C}_K \\ {\scriptstyle \Psi_{L/F}}\downarrow & & \downarrow{\scriptstyle \Psi_{L/K}} \\ \mathrm{Gal}(L/F)^{ab} & \xrightarrow{\iota^{ab}} & \mathrm{Gal}(L/K)^{ab} \end{array} \qquad \begin{array}{ccc} \mathbf{C}_K & \xrightarrow{\textit{inclusion}} & \mathbf{C}_F \\ {\scriptstyle \Psi_{L/K}}\downarrow & & \downarrow{\scriptstyle \Psi_{L/F}} \\ \mathrm{Gal}(L/K)^{ab} & \xrightarrow{\mathrm{Ver}} & \mathrm{Gal}(L/F)^{ab} \end{array}$$

(4.3.5) As in the local case, the map $\Psi_{L/K} : \mathbf{C}_K \to \mathrm{Gal}(L/K)^{ab}$ in Thm. 4.3.4 is called the ***Artin reciprocity map*** or the ***norm residue symbol***. It is sometimes denoted by $(\cdot, L/K)$. ■

Using the local-global compatibility (Thm. 4.3.4 (2)), one can prove the following:

Corollary 4.3.6. *Let L/K be a finite abelian extension and $v \in \Omega_K$.*

1. *For every $w \in \Omega_L$ lying over v, we have $N_{L/K}(\mathbf{C}_L) \cap K_v^* = N_{L_w/K_v}(L_w^*)$ via the embedding $K_v^* \to \mathbf{C}_K$.*
2. *The place v is unramified in L/K if and only if $\widehat{\mathcal{O}}_v^* \subseteq N_{L/K}(\mathbf{C}_L)$ in $\mathbf{C}_K$, or equivalently, $\widehat{\mathcal{O}}_v^* \subseteq N_{L/K}(\mathbf{I}_L)K^*$ in $\mathbf{I}_K$.*

   (Recall that if v is archimedean, we have set $\widehat{\mathcal{O}}_v^* = K_v^*$.)
3. *The place v splits completely in L/K if and only if $K_v^* \subseteq N_{L/K}(\mathbf{C}_L)$ in $\mathbf{C}_K$, or equivalently, $K_v^* \subseteq N_{L/K}(\mathbf{I}_L)K^*$ in $\mathbf{I}_K$.*

Proof. Exercise. □

Theorem 4.3.7. *Let L/K be a finite separable extension.*

1. *The norm subgroup $N_{L/K}(\mathbf{C}_L)$ is a finite-index open subgroup of $\mathbf{C}_K$.*
2. *(Norm index inequalities) Let F/K be the maximal abelian subextension of L/K. Then*

$$N_{L/K}(\mathbf{C}_L) = N_{F/K}(\mathbf{C}_F) \quad \text{and} \quad [\mathbf{C}_K : N_{F/K}(\mathbf{C}_F)] = [F : K] \leq [L : K]\,.$$

3. *(Existence theorem) The map*

$$\begin{aligned} \{\text{finite abelian extensions of } K \text{ (in } \overline{K})\} &\longrightarrow \{\text{finite-index open subgroups of } \mathbf{C}_K\} \\ E &\longmapsto N_{E/K}(\mathbf{C}_E) \end{aligned}$$

   is an inclusion-reversing bijection.

   In other words, for every finite-index open subgroup N of $\mathbf{I}_K$ containing K^*, there is a unique finite abelian extension E/K such that $K^* N_{E/K}(\mathbf{I}_E) = N$.

   The extension E/K corresponding to a finite-index open subgroup $N \leq \mathbf{C}_K$ (or $N \leq \mathbf{I}_K$ with $K^* \subseteq N$) is called the **class field** *belonging to N.*

Example 4.3.8. Let K be a number field. Then each finite place v of K corresponds to a unique maximal ideal $\mathfrak{p}_v$ of the ring of integers $\mathcal{O}_K$.

Define the map

$$\mathbf{I}_K \longrightarrow \mathcal{C}l(K)\,; \quad \alpha = (\alpha_v) \longmapsto \prod_{v \text{ finite}} \mathfrak{p}_v^{v_K(\alpha_v)}\,,$$

where v_K denotes the normalized discrete valuation on K_v determined by the place v. This is clearly a surjective group homomorphism, whose kernel is

$$K^* \cdot \mathbf{I}_{K,\Omega_\infty} = K^* \cdot \left(\prod_{v \in \Omega_K} \widehat{\mathcal{O}}_v^* \right) = K^* \cdot \left(\prod_{v \text{ infinite}} K_v^* \times \prod_{v \text{ finite}} \widehat{\mathcal{O}}_v^* \right),$$

where Ω_∞ denotes the set of infinite places of K. So we have an isomorphism

$$\mathbf{I}_K/K^*\mathbf{I}_{K,\,\Omega_\infty} \xrightarrow{\sim} \mathcal{C}l(K)\,. \tag{4.3.8.1}$$

We know that its ideal class group $\mathcal{C}l(K)$ is finite. So $K^*\mathbf{I}_{K,\,\Omega_\infty}$ is a finite-index subgroup of $\mathbf{I}_K$. It is also easy to see that this subgroup is open in $\mathbf{I}_K$. Therefore, by the existence theorem (Thm. 4.3.7 (3)), there is a unique finite abelian extension H/K such that

$$N_{H/K}(\mathbf{C}_H) = K^*\mathbf{I}_{K,\,\Omega_\infty}/K^*\,.$$

We call this extension H the ***Hilbert class field*** of K. It has the property that

$$\mathrm{Gal}(H/K) \cong \mathbf{I}_K/K^*\mathbf{I}_{K,\,\Omega_\infty} \xrightarrow{\sim} \mathcal{C}l(K)\,. \tag{4.3.8.2}$$

That is, the Galois group of H/K is isomorphic to the ideal class group $\mathcal{C}l(K)$. Moreover, since by construction $N_{H/K}(\mathbf{I}_H)$ is the smallest finite-index open subgroup of $\mathbf{I}_K$ that contains $\widehat{\mathcal{O}}_v^*$ for all $v \in \Omega_K$, so by Cor. 4.3.6, H/K is the largest finite abelian extension in which all places (including finite and infinite ones) of K are unramified. By considering finite subextensions, we see that this maximality property remains valid when we consider all abelian extension with this property. Therefore, the Hilbert class field H/K is the ***maximal unramified abelian extension*** of K. (Let us emphasis once again that here we are requiring unramifiedness not only for non-archimedean places, but also for archimedean places). ■

4.3.2 Ray class fields and Artin conductors

In this subsection, we shall often write $\mathfrak{p}$ for a place of the global field K. The completion of K at $\mathfrak{p}$ is thus denoted by $K_\mathfrak{p}$. We write $\mathfrak{p} \,|\, \infty$ (resp. $\mathfrak{p} \nmid \infty$) to mean that $\mathfrak{p}$ is an infinite (resp. finite) places. If $\mathfrak{p}$ is finite, let $v_\mathfrak{p}$ be the normalized discrete valuation on $K_\mathfrak{p}$, $\widehat{\mathcal{O}}_\mathfrak{p}$ the valuation ring of $K_\mathfrak{p}$ and $\hat{\mathfrak{p}}$ the maximal ideal of $\widehat{\mathcal{O}}_\mathfrak{p}$.

(4.3.9) Let $n \in \mathbb{N}$. For any finite place $\mathfrak{p} \in \Omega_K$, let $U_\mathfrak{p}^{(n)}$ be the group $U_{K_\mathfrak{p}}^{(n)}$ defined in Definition 4.2.7, that is,

$$U_\mathfrak{p}^{(n)} := 1 + \hat{\mathfrak{p}}^n = \{x \in K_\mathfrak{p} \,|\, v_\mathfrak{p}(x-1) \geq n\}\,.$$

(Note that $U_\mathfrak{p}^{(0)} = \widehat{\mathcal{O}}_\mathfrak{p}^*$.) For $\mathfrak{p} \,|\, \infty$, we define

$$U_\mathfrak{p}^{(0)} = K_\mathfrak{p}^* \quad \text{and} \quad U_\mathfrak{p}^{(1)} = K_\mathfrak{p}^{*2}\,.$$

A ***modulus*** of K is a formal product

$$\mathfrak{m} := \prod_{\mathfrak{p} \in \Omega_K} \mathfrak{p}^{n_\mathfrak{p}}\,, \quad \text{with each } \; n_\mathfrak{p} \; \in \mathbb{N}$$

such that $n_\mathfrak{p} = 0$ for almost all $\mathfrak{p} \in \Omega_K$, $n_\mathfrak{p} \in \{0\,,\,1\}$ if $\mathfrak{p}$ is real and $n_\mathfrak{p} = 0$ if $\mathfrak{p}$ is complex. We often write $v_\mathfrak{p}(\mathfrak{m})$ for the integer $n_\mathfrak{p}$ appearing in the above expression.

The ***trivial modulus*** is the modulus with $v_{\mathfrak{p}}(\mathfrak{m}) = 0$ for all $\mathfrak{p} \in \Omega_K$. In this case we write $\mathfrak{m} = (1)$.

Given two moduli $\mathfrak{m}_1$ and $\mathfrak{m}_2$, we write $\mathfrak{m}_1 \,|\, \mathfrak{m}_2$ if $v_{\mathfrak{p}}(\mathfrak{m}_1) \leq v_{\mathfrak{p}}(\mathfrak{m}_2)$ for every $\mathfrak{p} \in \Omega_K$, and we say that $\mathfrak{m}_1$, $\mathfrak{m}_2$ are ***coprime*** if $v_{\mathfrak{p}}(\mathfrak{m}_1) \cdot v_{\mathfrak{p}}(\mathfrak{m}_2) = 0$ for all $\mathfrak{p} \in \Omega_K$. The ***greatest common divisor*** (gcd) of any collection of moduli are defined in the obvious manner. The ***finite part*** $\mathfrak{m}_0$ and ***infinite part*** $\mathfrak{m}_\infty$ of a modulus $\mathfrak{m}$ are defined respectively by

$$\mathfrak{m}_0 := \prod_{\mathfrak{p} \nmid \infty} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{m})}, \quad \mathfrak{m}_\infty := \prod_{\mathfrak{p} \,|\, \infty} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{m})}.$$

If K is a number field with ring of integers $\mathcal{O}_K$, then moduli without infinite part can be identified with nonzero integral ideals of $\mathcal{O}_K$. A nonzero integral ideal $\mathfrak{a} \subseteq \mathcal{O}_K$ is coprime to a modulus $\mathfrak{m}$ if and only if the ideals $\mathfrak{a}$ and $\mathfrak{m}_0$ are coprime in the usual sense of ideal theory.

Given a modulus $\mathfrak{m} = \prod \mathfrak{p}^{n_{\mathfrak{p}}}$, define[‡‡]

$$\mathbf{I}_K^{\mathfrak{m}} := \prod_{\mathfrak{p} \in \Omega_K} U_{\mathfrak{p}}^{(n_{\mathfrak{p}})} = \prod_{\substack{\mathfrak{p} \,|\, \infty \\ \mathfrak{p} \nmid \mathfrak{m}}} K_{\mathfrak{p}}^* \times \prod_{\substack{\mathfrak{p} \,|\, \infty \\ \mathfrak{p} \,|\, \mathfrak{m}}} K_{\mathfrak{p}}^{*2} \times \prod_{\substack{\mathfrak{p} \nmid \infty \\ \mathfrak{p} \nmid \mathfrak{m}}} \widehat{\mathcal{O}}_{\mathfrak{p}}^* \times \prod_{\substack{\mathfrak{p} \nmid \infty \\ \mathfrak{p} \,|\, \mathfrak{m}}} (1 + \hat{\mathfrak{p}}^{n_{\mathfrak{p}}}) \tag{4.3.9.1}$$

This is an open subgroup of the idèle group $\mathbf{I}_K$. The group

$$\mathbf{C}_K^{\mathfrak{m}} := \mathbf{I}_K^{\mathfrak{m}} K^* \Big/ K^*$$

is called the ***congruence subgroup*** modulo $\mathfrak{m}$ of $\mathbf{C}_K$. The quotient

$$\mathbf{C}_K / \mathbf{C}_K^{\mathfrak{m}} = \mathbf{I}_K \Big/ \mathbf{I}_K^{\mathfrak{m}} K^*$$

is called the ***idelic ray class group*** modulo $\mathfrak{m}$.

Clearly, if $\mathfrak{m}$, $\mathfrak{m}'$ are moduli with $\mathfrak{m} \,|\, \mathfrak{m}'$, then $\mathbf{I}_K^{\mathfrak{m}'} \subseteq \mathbf{I}_K^{\mathfrak{m}}$, $\mathbf{C}_K^{\mathfrak{m}'} \subseteq \mathbf{C}_K^{\mathfrak{m}}$ and there is a natural surjection

$$\mathbf{C}_K / \mathbf{C}_K^{\mathfrak{m}'} = \mathbf{I}_K \Big/ \mathbf{I}_K^{\mathfrak{m}'} K^* \twoheadrightarrow \mathbf{C}_K / \mathbf{C}_K^{\mathfrak{m}} = \mathbf{I}_K \Big/ \mathbf{I}_K^{\mathfrak{m}} K^*.$$

If $\mathfrak{m} = (1)$, we have

$$\mathbf{I}_K^{(1)} = \mathbf{I}_{K,\Omega_\infty} = \prod_{\mathfrak{p} \in \Omega_\infty} K_{\mathfrak{p}}^* \times \prod_{\mathfrak{p} \notin \Omega_\infty} \widehat{\mathcal{O}}_{\mathfrak{p}}^*$$

where Ω_∞ denotes the set of infinite places of K (and $\mathbf{I}_{K,\Omega_\infty}$ is the group of Ω_∞-idèles defined in (4.1.14.1)). (Warning: Do not confuse $\mathbf{I}_K^{(1)}$ with the group $\mathbf{I}_K^1$ of unit idèles defined in Definition 4.1.18.)

If K is a number field, we get from (4.3.8.1) an isomorphism

$$\mathbf{C}_K / \mathbf{C}_K^{(1)} \cong \mathcal{C}l(K). \tag{4.3.9.2}$$

[‡‡]Notice again that the definition in [Neu99] is different.

If K is a global function field of characteristic p, letting $\mathbb{F}_q$ be the algebraic closure of $\mathbb{F}_p$ in K, there is a unique (up to isomorphism) smooth projective irreducible curve C over $\mathbb{F}_q$ whose function field is K. In this case, a similar argument shows that $\mathbf{C}_K/\mathbf{C}_K^{(1)}$ is isomorphic to the ***Picard group*** $\mathrm{Pic}(C)$ of the curve C. Unlike the number field case, the group $\mathrm{Pic}(C)$ is an infinite group. This phenomenon of infiniteness is responsible for most differences between the class field theory of function fields and that of number fields. ■

Proposition 4.3.10. *A subgroup of $\mathbf{I}_K$ is an open subgroup if and only if contains $\mathbf{I}_K^{\mathfrak{m}}$ for some modulus $\mathfrak{m}$ of K. A subgroup of $\mathbf{C}_K$ is an open subgroup if and only if it contains a congruence subgroup.*

If K is a number field, then every open subgroup of $\mathbf{C}_K$ has finite index and the idelic ray class group $\mathbf{C}_K/\mathbf{C}_K^{\mathfrak{m}}$ is finite any modulus $\mathfrak{m}$ of K.

Proof. See e.g. (the proof of) [Neu86, Thm. IV.7.3]. □

(4.3.11) Let K be a number field. For any modulus $\mathfrak{m}$ of K, the class field $K(\mathfrak{m})$ belonging to the congruence subgroup $\mathbf{C}_K^{\mathfrak{m}} \leq \mathbf{C}_K$ is called the ***ray class field*** of K with modulus $\mathfrak{m}$.

We have seen that in the case $\mathfrak{m} = (1)$, the field $K(1) = K(\mathfrak{m})$ is nothing but the Hilbert class field of K (cf. Example 4.3.8). It is often denoted by H_K.

We denote by H_K^+ the ray class field with modulus $\mathfrak{m} = \prod_{\mathfrak{p}\text{ real}} \mathfrak{p}$ and we call it the ***narrow Hilbert class field***[*] of K. Clearly, $H_K \subseteq H_K^+$. Since

$$N_{H_K^+/K}(\mathbf{C}_{H_K^+}) = \left(\prod_{\mathfrak{p}\text{ complex}} K_{\mathfrak{p}}^* \times \prod_{\mathfrak{p}\text{ real}} K_{\mathfrak{p}}^{*2} \times \prod_{\mathfrak{p}\nmid\infty} \widehat{\mathcal{O}}_{\mathfrak{p}}^* \right) K^* \Big/ K^* ,$$

we can also characterize H_K^+ as the maximal abelian extension of K in which all finite places of K are unramified, by Cor. 4.3.6 (2).

For a general modulus $\mathfrak{m}$, we see from (4.3.9.1) that places of K that ramify in $K(\mathfrak{m})$ all divide $\mathfrak{m}$. (But it is possible that a place $\mathfrak{p} \mid \mathfrak{m}$ is unramified in $K(\mathfrak{m})$.) ■

Remark 4.3.12. Let K be a global function field. Then $\mathbf{C}_K$ has some open subgroups of infinite index. For example, the group $\mathbf{C}_K^1 := \mathbf{I}_K^1/K$ in Thm. 4.1.19 is such an example. However, by the class field theory for infinite extensions, there still exists a nice bijective correspondence between a certain collection of abelian (possible infinite) extensions of K and the set of closed subgroups of $\mathbf{C}_K$. In particular, one can define the ray class field $K(\mathfrak{m})$ in the same way, although $K(\mathfrak{m})/K$ need not be a finite extension.

The ray class field $K(1)$ corresponding to the trivial modulus (1) is still the maximal abelian extension of K in which all places of K are unramified. But since $K(1)/K$ is an infinite extension in this case, people prefer not to call this extension the Hilbert class field of K. For a discussion of possible generalizations of Hilbert class fields in the function field case, see e.g. [AT09, pp.61–62]. ■

[*] In [Neu99] the field H_K^+ is called the ***big Hilbert class field*** of K.

Lemma 4.3.13. *Let K be a global field and $\mathfrak{m}$ a modulus of K. Let L/K be a finite abelian extension. Then the following conditions are equivalent:*

(i) $L \subseteq K(\mathfrak{m})$.

(ii) $N_{L/K}(\mathbf{I}_L) \supseteq \mathbf{I}_K^{\mathfrak{m}}$.

(iii) $N_{L/K}(\mathbf{C}_L) \supseteq \mathbf{C}_K^{\mathfrak{m}}$.

Definition 4.3.14. Let L/K be a finite abelian extension of global fields. We know from Prop. 4.3.10 that there exists a modulus $\mathfrak{m}$ satisfying the equivalent conditions in Lemma 4.3.13. We define the ***Artin conductor*** $\mathfrak{f}_{L/K}$ of L/K to be the greatest common divisor of all such moduli $\mathfrak{m}$. ■

(4.3.15) Let L/K be a finite abelian extension of global fields. For each place $\mathfrak{p} \in \Omega_K$, fix a place $\mathfrak{P} \in \Omega_L$ lying over $\mathfrak{p}$. Since L/K is abelian, the Galois group $\mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$, when considered as a subgroup of $\mathrm{Gal}(L/K)$, is independent of the choice of $\mathfrak{P}$ (as was discussed in (4.3.3)). In particular, if $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ is an unramified (resp. trivial) extension for some choice of $\mathfrak{P}$, then the same is true for any other choice of $\mathfrak{P}$.

If $\mathfrak{p} \nmid \infty$, let $\mathfrak{f}_{\mathfrak{p}}$ be the the Artin conductor of $L_{\mathfrak{P}}/K_{\mathfrak{p}}$, which is defined in Definition 4.2.7. For $\mathfrak{p} \mid \infty$, we set

$$\mathfrak{f}_{\mathfrak{p}} := \begin{cases} \mathfrak{p} & \text{if } L_{\mathfrak{P}} \neq K_{\mathfrak{p}}\,, \\ (1) & \text{if } L_{\mathfrak{P}} = K_{\mathfrak{p}}\,. \end{cases}$$

With this definition, $\mathfrak{f}_{\mathfrak{p}} = (1)$ if and only if $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ is unramified. In other words, Prop. 4.2.8 remains true in the archimedean case.

We shall now consider each $\mathfrak{f}_{\mathfrak{p}}$ as a modulus of K. Since only finitely many places $\mathfrak{p} \in \Omega_K$ can ramify in the finite extension L/K, the product $\prod_{\mathfrak{p}\in\Omega_K} \mathfrak{f}_{\mathfrak{p}}$ is a well defined modulus of K. ■

Proposition 4.3.16 (Conductor theorem)**.** *Let L/K be a finite abelian extension of global fields.*

1. *We have $\mathfrak{f}_{L/K} = \prod_{\mathfrak{p}\in\Omega_K} \mathfrak{f}_{\mathfrak{p}}$ as moduli of K.*
2. *A (finite or infinite) place $\mathfrak{p} \in \Omega_K$ ramifies in L/K if and only if $\mathfrak{p} \mid \mathfrak{f}_{L/K}$.*

Proof. (1) See e.g. [Neu86, Prop. IV.7.5].

(2) This is immediate from (1) and Prop. 4.2.8, since $\mathfrak{p}$ ramifies in L/K if and only if $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ is ramified. □

4.3.3 Ideal theoretic formulation of class field theory

Class field theory has found its idelic formulation only after it had been completed in the language of ideals. There are advantages and disadvantages to working with the classical ideal theoretic language of class field theory. In any case, it is useful to be able to pass back and forth between the idelic formulation and the ideal theoretic one.

(4.3.17) Let $\mathfrak{m} = \prod \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{m})}$ be a modulus of a global field K. It is trivially verified that

$$K_{\mathfrak{m},1} := K^* \cap \bigcap_{\mathfrak{p} \,|\, \mathfrak{m}} U_\mathfrak{p}^{(v_\mathfrak{p}(\mathfrak{m}))} \tag{4.3.17.1}$$

is a subgroup of K^*. Explicitly, $K_{\mathfrak{m},1}$ consists of elements $\alpha \in K^*$ satisfying the following two conditions:

- For every $\mathfrak{p} \,|\, \mathfrak{m}_0$, $v_\mathfrak{p}(\alpha - 1) \geq v_\mathfrak{p}(\mathfrak{m})$;
- For every $\mathfrak{p} \,|\, \mathfrak{m}_\infty$, corresponding to a real embedding $\tau_\mathfrak{p} : k \to \mathbb{R}$, one has $\tau_\mathfrak{p}(\alpha) > 0$.

If $\mathfrak{m} = (1)$ is the trivial modulus, then $K_{\mathfrak{m},1} = K^*$.

Denote by $\mathscr{I}_K^\mathfrak{m}$ the free abelian multiplicative group generated by all finite places $\mathfrak{p}$ that are coprime to $\mathfrak{m}$, i.e.,

$$\mathscr{I}_K^\mathfrak{m} = \left\{ \prod_{\substack{\mathfrak{p} \nmid \infty \\ \mathfrak{p} \nmid \mathfrak{m}}} \mathfrak{p}^{r_\mathfrak{p}} \;\middle|\; \text{each } r_\mathfrak{p} \in \mathbb{Z} \text{ and for almost all } \mathfrak{p}\,,\ r_\mathfrak{p} = 0 \right\} \tag{4.3.17.2}$$

We also define the subgroup

$$\mathscr{R}_K^\mathfrak{m} := \left\{ \prod_{\mathfrak{p} \nmid \infty} \mathfrak{p}^{v_\mathfrak{p}(\alpha)} \;\middle|\; \alpha \in K_{\mathfrak{m},1} \right\} \subseteq \mathscr{I}_K^\mathfrak{m}\,.$$

We call $\mathscr{R}_K^\mathfrak{m}$ the ***ray*** modulo $\mathfrak{m}$. This terminology stems from the fact that in the case $K = \mathbb{Q}$ and $\mathfrak{m}$ is the (unique) archimedean place ∞ of $\mathbb{Q}$, $\mathscr{R}_K^\mathfrak{m} = \mathscr{R}_\mathbb{Q}^\infty$ can be identified with the set of positive rational numbers, a "ray" from the origin in $\mathbb{Q}$!

The quotient

$$\mathcal{C}l^\mathfrak{m}(K) := \mathscr{I}_K^\mathfrak{m} / \mathscr{R}_K^\mathfrak{m}$$

is called the (***ideal theoretic***) ***ray class group***.

Clearly, if $\mathfrak{m}$, $\mathfrak{m}'$ are moduli with $\mathfrak{m} \,|\, \mathfrak{m}'$, then $\mathscr{I}_K^{\mathfrak{m}'} \subseteq \mathscr{I}_K^\mathfrak{m}$, $\mathscr{R}_K^{\mathfrak{m}'} \subseteq \mathscr{R}_K^\mathfrak{m}$ and there is a natural homomorphism

$$\mathcal{C}l^{\mathfrak{m}'}(K) = \mathscr{I}_K^{\mathfrak{m}'} / \mathscr{R}_K^{\mathfrak{m}'} \longrightarrow \mathcal{C}l^\mathfrak{m}(K) = \mathscr{I}_K^\mathfrak{m} / \mathscr{R}_K^\mathfrak{m}\,.$$

Notice also that if we define the ***reduced part*** of $\mathfrak{m}$ to be

$$S(\mathfrak{m}) := \prod_{\mathfrak{p} \,|\, \mathfrak{m}} \mathfrak{p}$$

then $\mathscr{I}_K^{\mathfrak{m}} = \mathscr{I}_K^{S(\mathfrak{m})}$. So the group $\mathscr{I}_K^{\mathfrak{m}}$ depends only on the reduced part $S(\mathfrak{m})$. On the other hand, the subgroup $\mathscr{R}_K^{\mathfrak{m}}$ does depend on $\mathfrak{m}$ itself.

Now let K be a number field with ring of integers $\mathcal{O}_K$. Then $\mathscr{I}_K^{\mathfrak{m}}$ is a subgroup of the group $\mathscr{I}_K := \mathscr{I}(\mathcal{O}_K)$ of fractional ideals of K and $\mathscr{R}_K^{\mathfrak{m}}$ is a subgroup of the group $\mathscr{P}_K := \mathscr{P}(\mathcal{O}_K)$ of principal fractional ideals. We have thus a natural homomorphism

$$\mathcal{C}l^{\mathfrak{m}}(K) \longrightarrow \mathcal{C}l(K)\ . \tag{4.3.17.3}$$

For $\mathfrak{m} = (1)$, it is clear that $\mathcal{C}l^{(1)}(K) = \mathcal{C}l(K)$.

If $\mathfrak{m} = \prod_{\mathfrak{p}\ \text{real}} \mathfrak{p}$ is the product of the real places of K, then $\mathcal{C}l^{+}(K) := \mathcal{C}l^{\mathfrak{m}}(K)$ is the quotient of $\mathscr{I}_K$ by the group of principal fractional ideals generated by ***totally positive*** elements of K^*, i.e. elements $x \in K^*$ whose image under every real embedding of K is positive. The group $\mathcal{C}l^{+}(K)$ is called the ***narrow class group*** of K. ■

As a generalization of the isomorphism (4.3.9.2), we have:

Proposition 4.3.18. *For any modulus $\mathfrak{m}$ of a global field K, there is an isomorphism*

$$\mathbf{C}_K/\mathbf{C}_K^{\mathfrak{m}} = \mathbf{I}_K/\mathbf{I}_K^{\mathfrak{m}}K^* \xrightarrow{\sim} \mathcal{C}l^{\mathfrak{m}}(K) = \mathscr{I}_K^{\mathfrak{m}}/\mathscr{R}_K^{\mathfrak{m}}\,.$$

Proof. See e.g. [Neu86, Prop. IV.8.1]. □

In general, the isomorphism in Prop. 4.3.18 is rather hard to write explicitly as it requires an application of weak approximation to define!

Definition 4.3.19. Let $\mathfrak{m}$ be a modulus of the global field K. A ***congruence subgroup*** for $\mathfrak{m}$ is a subgroup of $\mathscr{I}_K^{\mathfrak{m}}$ is a subgroup containing $\mathscr{R}_K^{\mathfrak{m}}$.

If $N \leq \mathscr{I}_K^{\mathfrak{m}}$ is a congruence subgroup, the quotient $\mathscr{I}^{\mathfrak{m}}/N$ is called a ***generalized ideal class group*** for $\mathfrak{m}$. ■

(4.3.20) Let L/K be a finite separable extension. For any modulus $\mathfrak{m}$ of K, let $\mathscr{I}_L^{\mathfrak{m}}$ denote the free abelian multiplicative group generated by finite places $\mathfrak{P} \in \Omega_L$ such that whose restriction to K is coprime to $\mathfrak{m}$.

We have a norm homomorphism

$$N_{L/K}\ :\ \mathscr{I}_L^{\mathfrak{m}} \longrightarrow \mathscr{I}_K^{\mathfrak{m}}\ ;\quad \mathfrak{P} \longmapsto \mathfrak{p}^{f(\mathfrak{P}\,|\,\mathfrak{p})} \quad \text{where } \mathfrak{p} := \mathfrak{P}|_K\,.$$

(Here as usual, $f(\mathfrak{P}\,|\,\mathfrak{p})$ denotes the residue degree of $\mathfrak{P}\,|\,\mathfrak{p}$.) In the case of number fields, this is induced from the usual ideal norm map defined in (2.4.12).

Now suppose L/K is a finite abelian extension. For any (finite or infinite) place $\mathfrak{p} \in \Omega_K$ that is unramified in L/K, the Frobenius element $\mathfrak{F}_{\mathfrak{p}} \in \mathrm{Gal}(L/K)$ is well defined as we have discussed in (4.3.3).

Let $\mathfrak{m}$ be a modulus of K which is divisible by all (finite or infinite) places that ramify in L/K. (This conditions holds if L is contained in the ray class field $K(\mathfrak{m})$ by (4.3.11), or if the Artin conductor $\mathfrak{f}_{L/K}$ divides $\mathfrak{m}$, by Prop. 4.3.16. However, we should not admit these facts if we do not assume that the idelic formulation of class field theory had been established.) Then there is a unique group homomorphism

$$\Phi_{L/K}^{\mathfrak{m}}\ :\ \mathscr{I}_K^{\mathfrak{m}} \longrightarrow \mathrm{Gal}(L/K)$$

such that $\Phi^{\mathfrak{m}}(\mathfrak{p}) = \mathfrak{F}_{\mathfrak{p}}$ for every finite place $\mathfrak{p} \nmid \mathfrak{m}$. This map is called the ***Artin symbol*** for L/K and $\mathfrak{m}$. When the modulus $\mathfrak{m}$ is clear from the context, this Artin symbol is often denoted by $(\cdot\,, L/K)$ or $\left(\frac{L/k}{\cdot}\right)$ in the literature.

Since the Frobenius element $\mathfrak{F}_{\mathfrak{p}}$ has order $f(\mathfrak{P} \,|\, \mathfrak{p})$, it is clear that

$$N_{L/K}(\mathscr{I}_L^{\mathfrak{m}}) \subseteq \mathrm{Ker}(\Phi_{L/K}^{\mathfrak{m}})\,.$$

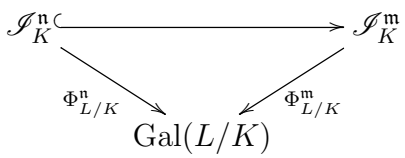
However, the inclusion $\mathscr{R}_K^{\mathfrak{m}} \subseteq \mathrm{Ker}(\Psi_{L/K}^{\mathfrak{m}})$ may not hold. That is, $\mathrm{Ker}(\Phi_{L/K}^{\mathfrak{m}})$ need not be a congruence subgroup. We call the group $\mathscr{R}_K^{\mathfrak{m}} N_{L/K}(\mathscr{I}_L^{\mathfrak{m}})$ the ***Takagi group*** of L/K with modulus $\mathfrak{m}$. Thus, $\mathrm{Ker}(\Phi_{L/K}^{\mathfrak{m}})$ is a congruence subgroup for $\mathfrak{m}$ if and only if it contains the Takagi group $\mathscr{R}_K^{\mathfrak{m}} N_{L/K}(\mathscr{I}_L^{\mathfrak{m}})$. ■

For simplicity, *we assume K is a number field in the remainder of this subsection.* This assumption ensures that every congruence subgroup of $\mathscr{I}_K^{\mathfrak{m}}$ has finite index, or equivalently, every generalized ideal class group is finite.

Theorem 4.3.21. *Let L/K be a finite abelian extension of number fields and let $\mathfrak{m}$ be a modulus divisible by all places of K that ramify in L.*

1. *(Norm index inequality) The Takagi group $\mathscr{R}_K^{\mathfrak{m}} N_{L/K}(\mathscr{I}_L^{\mathfrak{m}})$ has finite index in $\mathscr{I}_K^{\mathfrak{m}}$. In fact,*
$$[\mathscr{I}_K^{\mathfrak{m}} : \mathscr{R}_K^{\mathfrak{m}} N_{L/K}(\mathscr{I}_L^{\mathfrak{m}})] \leq [L : K]\,.$$
2. *The Artin symbol $\Phi_{L/K}^{\mathfrak{m}} : \mathscr{I}_K^{\mathfrak{m}} \to \mathrm{Gal}(L/K)$ is surjective. Hence, by the norm index inequality, $\mathrm{Ker}(\Phi_{L/K}^{\mathfrak{m}})$ is a congruence subgroup for $\mathfrak{m}$ if and only if it equals the Takagi group $\mathscr{R}_K^{\mathfrak{m}} N_{L/K}(\mathscr{I}_L^{\mathfrak{m}})$.*
3. *(Artin reciprocity law) If $v_{\mathfrak{p}}(\mathfrak{m})$ is sufficiently large for every finite place $\mathfrak{p} \,|\, \mathfrak{m}$, then $\mathrm{Ker}(\Phi_{L/K}^{\mathfrak{m}})$ is a congruence subgroup for $\mathfrak{m}$, so that*
$$\mathrm{Ker}(\Phi_{L/K}^{\mathfrak{m}}) = \mathscr{R}_K^{\mathfrak{m}} N_{L/K}(\mathscr{I}_L^{\mathfrak{m}}) \quad \text{and} \quad \mathscr{I}_K^{\mathfrak{m}} \Big/ \mathscr{R}_K^{\mathfrak{m}} N_{L/K}(\mathscr{I}_L^{\mathfrak{m}}) \xrightarrow{\sim} \mathrm{Gal}(L/K)\,.$$
In particular, in this case the Takagi group $\mathscr{R}_K^{\mathfrak{m}} N_{L/K}(\mathscr{I}_L^{\mathfrak{m}})$ depends only on L/K and $S(\mathfrak{m})$, and $\mathrm{Gal}(L/K)$ is isomorphic to a generalized ideal class group of $\mathfrak{m}$.

(4.3.22) One inconvenience in the reciprocity law stated in Thm. 4.3.21 (3) is that the modulus $\mathfrak{m}$ for which $\mathrm{Ker}(\Phi_{L/K}^{\mathfrak{m}})$ is a congruence subgroup is not unique. In fact, if $\mathfrak{m}$, $\mathfrak{n}$ are two moduli divisible by all places of K that ramify in L and $\mathfrak{m} \,|\, \mathfrak{n}$, then $\mathscr{I}_K^{\mathfrak{n}} \subseteq \mathscr{I}_K^{\mathfrak{m}}$, $\mathscr{R}_K^{\mathfrak{n}} \subseteq \mathscr{R}_K^{\mathfrak{m}}$, and the obvious commutative diagram



show that if $\mathrm{Ker}(\Phi_{L/K}^{\mathfrak{m}})$ is a congruence subgroup for $\mathfrak{m}$, then $\mathrm{Ker}(\Phi_{L/K}^{\mathfrak{n}})$ is a congruence subgroup for $\mathfrak{n}$. ■

The theorem below shows that there is one minimal modulus $\mathfrak{m}$ for which $\mathrm{Ker}(\Phi^{\mathfrak{m}}_{L/K})$ is a congruence subgroup.

Theorem 4.3.23 (Conductor theorem)**.** *Let L/K be a finite abelian extension of number fields. Then there is a unique modulus $\mathfrak{f} = \mathfrak{f}(L/K)$ with the following properties:*

(i) *A (finite or infinite) place $\mathfrak{p} \in \Omega_K$ ramifies in L if and only if $\mathfrak{p} \mid \mathfrak{f}$.*

(ii) *For any modulus $\mathfrak{m}$ divisible by all places of K that ramify in L, $\mathrm{Ker}(\Phi^{\mathfrak{m}}_{L/K})$ is a congruence subgroup for $\mathfrak{m}$ if and only if $\mathfrak{f} \mid \mathfrak{m}$.*

Theorem 4.3.24 (Existence theorem)**.** *Let K be a number field and let $\mathfrak{m}$ be a modulus of K.*

Then for every congruence subgroup $\mathscr{N}$ for $\mathfrak{m}$, there is a unique finite abelian extension L/K with the following properties:

(i) *If a (finite or infinite) place $\mathfrak{p} \in \Omega_K$ ramifies in L, then $\mathfrak{p} \mid \mathfrak{m}$.*

In particular, the Artin symbol $\Phi^{\mathfrak{m}}_{L/K} : \mathscr{I}^{\mathfrak{m}}_K \to \mathrm{Gal}(L/K)$ is defined.

(ii) *One has $\mathscr{N} = \mathrm{Ker}(\Phi^{\mathfrak{m}}_{L/K}) = \mathscr{R}^{\mathfrak{m}}_K N_{L/K}(\mathscr{I}^{\mathfrak{m}}_L)$, and hence $\mathscr{I}^{\mathfrak{m}}_K/\mathscr{N} \cong \mathrm{Gal}(L/K)$.*

One reason why the above existence theorem is so important is that it can be used to construct abelian extensions with prescribed Galois group and restricted ramification.

Corollary 4.3.25. *Let L_1, L_2 be finite abelian extensions of a number field K. Let $\mathfrak{f}_i = \mathfrak{f}(L_i/K)$, $i = 1, 2$ be the moduli defined in Theorem 4.3.23.*

Then the following are equivalent:

(i) $L_1 \subseteq L_2$.

(ii) *There is a modulus $\mathfrak{m}$ of K divisible by both $\mathfrak{f}_1$ and $\mathfrak{f}_2$ (hence the Artin symbols $\Phi^{\mathfrak{m}}_{L_i/K}$ are defined and $\mathrm{Ker}(\Phi^{\mathfrak{m}}_{L_i/K}) = \mathscr{R}^{\mathfrak{m}}_K N_{L_i/K}(\mathscr{I}^{\mathfrak{m}}_{L_i})$), such that*

$$\mathscr{R}^{\mathfrak{m}}_K N_{L_2/K}(\mathscr{I}^{\mathfrak{m}}_{L_2}) \subseteq \mathscr{R}^{\mathfrak{m}}_K N_{L_1/K}(\mathscr{I}^{\mathfrak{m}}_{L_1})\,.$$

(iii) *There is a modulus $\mathfrak{m}$ of K divisible by all places of K that are ramified in L_1 or L_2 (hence the Artin symbols $\Phi^{\mathfrak{m}}_{L_i/K}$ are defined), such that*

$$\mathscr{R}^{\mathfrak{m}}_K \subseteq \mathrm{Ker}(\Phi^{\mathfrak{m}}_{L_2/K}) \subseteq \mathrm{Ker}(\Phi^{\mathfrak{m}}_{L_1/K})\,.$$

Proof. Exercise. □

(4.3.26) Let K be a number field. Let us explain very briefly how to translate the theory between the idelic and the ideal theoretic languages.

First consider a fixed modulus $\mathfrak{m}$ of K.

1. We have seen in Prop. 4.3.18 that there is an isomorphism between the idelic ray class group and the ideal theoretic ray class group:
$$\rho_{\mathfrak{m}} \,:\, \mathbf{C}_K/\mathbf{C}_K^{\mathfrak{m}} = \mathbf{I}_K/K^*\mathbf{I}_K^{\mathfrak{m}} \xrightarrow{\sim} \mathcal{C}l^{\mathfrak{m}}(K) = \mathscr{I}_K^{\mathfrak{m}}/\mathscr{R}_K^{\mathfrak{m}}\,.$$

2. Applying Thm. 4.3.24 with $\mathscr{N} = \mathscr{R}_K^{\mathfrak{m}}$, we obtain a unique (finite) abelian extension $H_K(\mathfrak{m})/K$ such that every place that ramifies in $H_K(\mathfrak{m})/K$ divides $\mathfrak{m}$ and that $\mathcal{C}l^{\mathfrak{m}}(K) \cong \mathrm{Gal}(H_K(\mathfrak{m})/K)$. Via the above isomorphism $\rho_{\mathfrak{m}}$, we see easily that $H_K(\mathfrak{m})$ is the same as the ray class field $K(\mathfrak{m})$ defined in (4.3.11).

   In particular, for the trivial modulus $\mathfrak{m} = (1)$, we have $H_K(1) = K(1) = H_K$, the Hilbert class field of K, which has Galois group $\mathrm{Gal}(H_K/K) \cong \mathcal{C}l(K)$. For the product $\mathfrak{m}$ of all real places of K, we obtain $H_K(\mathfrak{m}) = H_K^+$, the narrow Hilbert class field, whose Galois group $\mathrm{Gal}(H_K^+/K)$ is isomorphic to the narrow class group $\mathcal{C}l^+(K)$.

3. More generally, we have inclusion-reversing bijections
$$\left\{\begin{array}{c}\text{congruence subgroups}\\ \text{of } \mathscr{I}_K^{\mathfrak{m}} \text{ for } \mathfrak{m}\end{array}\right\} \xrightarrow{\sim} \{\text{subextensions of the ray class field } K(\mathfrak{m})\}$$
$$\mathscr{N} \longmapsto \text{subfield of } K(\mathfrak{m}) \text{ fixed by } \Phi^{\mathfrak{m}}_{K(\mathfrak{m})/K}(\mathscr{N})\,,$$
$$\mathscr{R}_K^{\mathfrak{m}} N_{L/K}(\mathscr{I}_L^{m}) \longmapsfrom L\,;$$
   and
$$\left\{\begin{array}{c}\text{congruence subgroups}\\ \text{of } \mathbf{C}_K \bmod \mathfrak{m}\end{array}\right\} \xrightarrow{\sim} \{\text{subextensions of the ray class field } K(\mathfrak{m})\}$$
$$N \longmapsto \text{subfield of } K(\mathfrak{m}) \text{ fixed by } \Psi_{K(\mathfrak{m})/K}(N)\,,$$
$$N_{L/K}(\mathbf{C}_L) \longmapsfrom L\,.$$
   Combining the above bijections yields a bijection
$$\left\{\begin{array}{c}\text{congruence subgroups}\\ \text{of } \mathbf{C}_K \bmod \mathfrak{m}\end{array}\right\} \xrightarrow{\sim} \left\{\begin{array}{c}\text{congruence subgroups}\\ \text{of } \mathscr{I}_K^{\mathfrak{m}} \text{ for } \mathfrak{m}\end{array}\right\}$$
$$N \longmapsto \mathscr{N}$$
   such that $\mathbf{C}_K^{\mathfrak{m}} \le N \le \mathbf{C}_K$ corresponds to $\mathscr{R}_K^{\mathfrak{m}} \le \mathscr{N} \le \mathscr{I}_K^{\mathfrak{m}}$ if and only if $\rho_{\mathfrak{m}}(N/\mathbf{C}_K^{\mathfrak{m}}) = \mathscr{N}/\mathscr{R}_K^{\mathfrak{m}}$, if and only if $\rho_{\mathfrak{m}}^{-1}(\mathscr{N}/\mathscr{R}_K^{\mathfrak{m}}) = N/\mathbf{C}_K^{\mathfrak{m}}$.

Now let L/K be a fixed finite abelian extension.

4. For any modulus $\mathfrak{m}$ of K we have the following equivalences:
$$\begin{aligned}
&L \subseteq K(\mathfrak{m})\\
\iff &N_{L/K}(\mathbf{I}_L) \supseteq \mathbf{I}_K^{\mathfrak{m}} \iff N_{L/K}(\mathbf{C}_L) \supseteq \mathbf{C}_K^{\mathfrak{m}}\\
\iff &\text{all places ramifying in } L \text{ divide } \mathfrak{m} \text{ and } \mathrm{Ker}(\Phi^{\mathfrak{m}}_{L/K}) \supseteq \mathscr{R}_K^{\mathfrak{m}}\\
\iff &\text{all places ramifying in } L \text{ divide } \mathfrak{m} \text{ and } \mathrm{Ker}(\Phi^{\mathfrak{m}}_{L/K}) = \mathscr{R}_K^{\mathfrak{m}} N_{L/K}(\mathscr{I}_L^{\mathfrak{m}})\\
\iff &\mathfrak{f}_{L/K} \,|\, \mathfrak{m}\,.
\end{aligned}$$
   In particular, the Artin conductor $\mathfrak{f}_{L/K}$ is the smallest (in the sense of divisibility) modulus $\mathfrak{m}$ such that $L \subseteq K(\mathfrak{m})$.

5. Assuming $L \subseteq K(\mathfrak{m})$ we have the following commutative diagram with exact rows

$$\begin{array}{ccccccccc}
1 & \longrightarrow & N_{L/K}(\mathbf{C}_L) & \longrightarrow & \mathbf{C}_K & \xrightarrow{\Psi_{L/K}} & \mathrm{Gal}(L/K) & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle \rho_{\mathfrak{m}}} & & \downarrow{\scriptstyle \rho_{\mathfrak{m}}} & & \| & & \\
1 & \longrightarrow & \mathscr{R}_K^{\mathfrak{m}} N_{L/K}(\mathscr{I}_L^{\mathfrak{m}}) & \longrightarrow & \mathcal{C}l^{\mathfrak{m}}(K) & \xrightarrow[\Phi_{L/K}^{\mathfrak{m}}]{} & \mathrm{Gal}(L/K) & \longrightarrow & 1
\end{array}$$

One of the shortcomings of the classical ideal theoretic language of class field theory is that it is not so convenient for studying infinite abelian extensions. Also, it is cumbersome to use when there are several finite abelian extensions coming into play, as one is constantly having to change the suitable modulus. But the classical language also has its advantages. It is very useful for the study of ideal classes in number fields.

Theorem 4.3.27 (Prime decomposition law)**.** *Let L/K be a finite abelian extension of number fields and let $\mathfrak{m}$ be a modulus such that $L \subseteq K(\mathfrak{m})$. Let $\mathfrak{p}$ be a maximal ideal of $\mathcal{O}_K$ that is coprime to $\mathfrak{m}$. Let f be the order of the class $[\mathfrak{p}]$ in the generalized ideal class group $\mathscr{I}_K^{\mathfrak{m}}/\mathscr{R}_K^{\mathfrak{m}} N_{L/K}(\mathscr{I}_L^{\mathfrak{m}})$.*

Then $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1 \cdots \mathfrak{P}_r$ where $\mathfrak{P}_i$ are distinct maximal ideals of $\mathcal{O}_L$ with each $f(\mathfrak{P}_i \,|\, \mathfrak{p}) = f$ (and $r = [L : K]/f$).

Proof. Since $\mathfrak{p} \nmid \mathfrak{m}$, the extension L/K is unramified at $\mathfrak{p}$. For each $\mathfrak{P}_i \,|\, \mathfrak{p}$, the residue degree $f(\mathfrak{P}_i \,|\, \mathfrak{p})$ is precisely the order the Frobenius element $\mathfrak{F}_{\mathfrak{p}} \in \mathrm{Gal}(L/K)$. But $\mathfrak{F}_{\mathfrak{p}}$ is the image of $[\mathfrak{p}]$ under the Artin symbol isomorphism

$$\Phi_{L/K}^{\mathfrak{m}} \;:\; \mathscr{I}_K^{\mathfrak{m}}/\mathscr{R}_K^{\mathfrak{m}} N_{L/K}(\mathscr{I}_L^{\mathfrak{m}}) \xrightarrow{\sim} \mathrm{Gal}(L/K)\,.$$

So we have $f(\mathfrak{P}_i \,|\, \mathfrak{p}) = f$. This proves the theorem. □

Corollary 4.3.28. *Let K be a number field and $H = H_K$ its Hilbert class field. Then for any maximal ideal $\mathfrak{p}$ of $\mathcal{O}_K$, we have*

$$\mathfrak{p} \text{ splits completely in } H \iff \mathfrak{p} \text{ is a principal ideal of } \mathcal{O}_K\,.$$

Proof. Apply Thm. 4.3.27 with $\mathfrak{m} = (1)$ and $L = K(1) = H$. □

The following result, conjectured by Hilbert in 1902 and proved by Furtwängler and Artin in 1929, was almost the last theorem before the classical class field theory was completed.

Theorem 4.3.29 (Principal ideal theorem)**.** *Let K be a number field and $H = H_K$ its Hilbert class field. Then $\mathfrak{a}\mathcal{O}_H$ is a principal ideal for every ideal $\mathfrak{a}$ of $\mathcal{O}_K$.*

4.3.4 Applications: Kronecker–Weber theorem and Hilbert reciprocity

Example 4.3.30. Let us consider the special case $K = \mathbb{Q}$. We shall denote the unique infinite place of $\mathbb{Q}$ by ∞ and identify the set of finite places with the set of prime

numbers. Then a modulus of $\mathbb{Q}$ can be written as $\mathfrak{m} = n$ or $\mathfrak{m} = n\infty$, where n is a positive integer. Let us write

$$\mathscr{I}^{(n)} = \mathscr{I}_{\mathbb{Q}}^{\mathfrak{m}}\ ,\quad \mathscr{R}^{(n)} = \mathscr{R}_{\mathbb{Q}}^{\mathfrak{m}}\ ,\quad \mathcal{C}l^{(n)}(\mathbb{Q}) = \mathscr{I}^{(n)}/\mathscr{R}^{(n)}$$

or

$$\mathscr{I}^{(n\infty)} = \mathscr{I}_{\mathbb{Q}}^{\mathfrak{m}}\ ,\quad \mathscr{R}^{(n\infty)} = \mathscr{R}_{\mathbb{Q}}^{\mathfrak{m}}\ ,\quad \mathcal{C}l^{(n\infty)}(\mathbb{Q}) = \mathscr{I}^{(n\infty)}/\mathscr{R}^{(n\infty)}$$

accordingly as $\mathfrak{m} = n$ or $\mathfrak{m} = n\infty$.

By definition,

$$\begin{aligned}
\mathscr{I}^{(n)} &= \left\{ab^{-1}\mathbb{Z} \,|\, a,\, b \in \mathbb{Z}\,,\, b \neq 0,\, \gcd(ab\,,\, n) = 1\right\}\ ,\\
\mathscr{R}^{(n)} &= \left\{ab^{-1}\mathbb{Z} \,\middle|\, a,\, b \in \mathbb{Z},\, b \neq 0,\ \text{and for all prime } p \,|\, n\,,\ v_p(ab^{-1} - 1) \geq v_p(n)\right\}\ .
\end{aligned}$$

Here for each prime number p, v_p denotes the (normalized) p-adic valuation. Note that for all $a,\, b \in \mathbb{Z}$, $b \neq 0$ and $r \geq 1$, we have

$$v_p(ab^{-1} - 1) \geq r \Longrightarrow v_p(a - b) \geq r + v_p(b) \geq r \Longrightarrow a \equiv b \pmod{p^r}\,.$$

If we further assume $\gcd(a,\, b) = 1$, then the congruence $a \equiv b \pmod{p^r}$ implies that $\gcd(ab,\, p) = 1$. Therefore, we can rewrite $\mathscr{R}^{(n)}$ as

$$\mathscr{R}^{(n)} = \left\{ab^{-1}\mathbb{Z} \,|\, a,\, b \in \mathbb{Z}\,,\, b \neq 0,\, \gcd(ab\,,\, n) = 1 \text{ and } a \equiv b \pmod{n}\right\}\ .$$

For any integer x let $[x]_n$ denote its canonical image in $\mathbb{Z}/n$.

For any $\mathfrak{a} \in \mathscr{I}^{(n)}$, by choosing a generator a/b of $\mathfrak{a}$ with $\gcd(ab,\, n) = 1$, the class $[\mathfrak{a}]_n := [|a|]_n[|b|]_n^{-1}$ is a well-defined element in $(\mathbb{Z}/n)^*$. We have thus a surjective group homomorphism

$$\mathscr{I}^{(n)} \longrightarrow (\mathbb{Z}/n)^*\,;\quad \mathfrak{a} = ab^{-1}\mathbb{Z} \longmapsto [|\mathfrak{a}|]_n := [|a|]_n \cdot [|b|]^{-1}\,. \tag{4.3.30.1}$$

The composite map

$$\mathscr{I}^{(n)} \longrightarrow (\mathbb{Z}/n)^* \longrightarrow \frac{(\mathbb{Z}/n)^*}{\langle [-1]_n \rangle}$$

has kernel $\mathscr{R}^{(n)}$. Hence

$$\mathcal{C}l^{(n)}(\mathbb{Q}) = \mathscr{I}^{(n)}/\mathscr{R}^{(n)} \cong \frac{(\mathbb{Z}/n)^*}{\langle [-1]_n \rangle}\,. \tag{4.3.30.2}$$

Similarly, one has

$$\begin{aligned}
\mathscr{I}^{(n\infty)} &= \left\{ab^{-1}\mathbb{Z} \,|\, a,\, b \in \mathbb{Z}\,,\, b \neq 0,\, \gcd(ab\,,\, n) = 1\right\} = \mathscr{I}^{(n)}\,,\\
\mathscr{R}^{(n\infty)} &= \left\{ab^{-1}\mathbb{Z} \,\middle|\, a,\, b \in \mathbb{Z},\, b \neq 0,\, ab^{-1} > 0 \text{ and } \forall\, p \,|\, n\,,\ v_p(ab^{-1} - 1) \geq v_p(n)\right\}\\
&= \left\{ab^{-1}\mathbb{Z} \,|\, a,\, b \in \mathbb{Z}\,,\, b \neq 0,\, ab > 0\,,\, \gcd(ab\,,\, n) = 1 \text{ and } a \equiv b \pmod{n}\right\}\ .
\end{aligned}$$

Since $\mathscr{I}^{(n\infty)} = \mathscr{I}^{(n)}$, we can consider (4.3.30.1) as a homomorphism

$$\mathscr{I}^{(n\infty)} \longrightarrow (\mathbb{Z}/n)^*\,;\quad \mathfrak{a} = ab^{-1}\mathbb{Z} \longmapsto [\mathfrak{a}]_n := [|a|]_n[|b|]_n^{-1}\,.$$

Its kernel is equal to $\mathscr{R}^{(n\infty)}$. Hence

$$\mathcal{C}l^{(n\infty)}(\mathbb{Q}) = \mathscr{I}^{(n\infty)}/\mathscr{R}^{(n\infty)} \cong (\mathbb{Z}/n)^* \,. \tag{4.3.30.3}$$

We have thus determined the ray class group $\mathcal{C}l^{\mathfrak{m}}(\mathbb{Q})$ for all moduli $\mathfrak{m}$ of $\mathbb{Q}$.

Letting $\xi_n \in \overline{\mathbb{Q}}$ be a primitive n-th root of unity, we have

$$(\mathbb{Z}/n)^* = \mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q}) \quad \text{and} \quad \frac{(\mathbb{Z}/n)^*}{\langle [-1]_n \rangle} = \mathrm{Gal}(\mathbb{Q}(\xi_n + \xi_n^{-1})/\mathbb{Q}) \,.$$

Thus, from (4.3.30.2) and (4.3.30.3) we see that the ray class field of $\mathbb{Q}$ corresponding to the moduli $\mathfrak{m} = n\infty$ and $\mathfrak{m} = n$ are $\mathbb{Q}(n\infty) = \mathbb{Q}(\xi_n)$ and $\mathbb{Q}(n) = \mathbb{Q}(\xi_n + \xi_n^{-1})$ respectively. ■

The description of all ray class fields of $\mathbb{Q}$ in Example 4.3.30 yields immediately the following theorem:

Theorem 4.3.31 (Kronecker–Weber)**.** *Every finite abelian extension K of $\mathbb{Q}$ is contained in some cyclotomic field $\mathbb{Q}(\xi_n)$.*

(4.3.32) Using class field theory, we can now give a reinterpretation of our proof of the quadratic reciprocity law in (2.5.14).

Let p, q be distinct odd prime numbers. Recall from Prop. 2.5.10 that the quadratic field $K := \mathbb{Q}(\sqrt{p^*})$ is contained in $\mathbb{Q}(\xi_p) = \mathbb{Q}(p\infty)$, where $p^* = (-1)^{\frac{p-1}{2}}p$. Let $\mathscr{N} \leq \mathscr{I}^{(p\infty)}$ be the congruence subgroup corresponding to K. We have the commutative diagram

$$\begin{array}{ccc} \mathscr{I}^{(p\infty)}/\mathscr{R}^{(p\infty)} & \xrightarrow[(\cdot,\,\mathbb{Q}(\xi_p)/\mathbb{Q})]{\cong} & \mathrm{Gal}(\mathbb{Q}(\xi_p)/\mathbb{Q}) \\ \downarrow & & \downarrow \\ \mathscr{I}^{(p\infty)}/\mathscr{N} & \xrightarrow[(\cdot,\,K/\mathbb{Q})]{\cong} & \mathrm{Gal}(K/\mathbb{Q}) \end{array} \tag{4.3.32.1}$$

where the vertical maps are natural surjections and the horizontal maps are the Artin symbols.

If we identify $\mathrm{Gal}(\mathbb{Q}(\xi_p)/\mathbb{Q})$ with $\mathbb{F}_p^* = (\mathbb{Z}/p\mathbb{Z})^*$, then $\mathrm{Gal}(\mathbb{Q}(\xi_p)/K)$ is the subgroup $\mathbb{F}_p^{*2}$ of square classes in $\mathbb{F}_p^*$, since it is the unique index 2 subgroup of $\mathbb{F}_p^*$. As was discussed in (4.3.10), the Artin symbol $\mathscr{I}^{(p\infty)} \to \mathrm{Gal}(\mathbb{Q}(\xi_p)/\mathbb{Q})$ can be identified with the map

$$\mathscr{I}^{(p\infty)} \longrightarrow \mathbb{F}_p^* \,; \quad a \longmapsto [a]_p$$

and hence the composite map

$$\mathscr{I}^{(p\infty)} \longrightarrow \mathrm{Gal}(\mathbb{Q}(\xi_p)/\mathbb{Q}) \longrightarrow \mathrm{Gal}(K/\mathbb{Q}) = \mathbb{F}_p^*/\mathbb{F}_p^{*2} \cong \{\pm 1\}$$

sends any integer a coprime to p to the Legendre symbol $\left(\frac{a}{p}\right)$. On the other hand, the commutative diagram (4.3.32.1) shows that the above map $\mathscr{I}^{(p\infty)} \to \mathrm{Gal}(K/\mathbb{Q}) \cong \{\pm 1\}$ sends $a \in \mathbb{Z}$ (coprime to p) to the Artin symbol $(a\mathbb{Z},\, K/\mathbb{Q}) \in \mathrm{Gal}(K/\mathbb{Q}) \cong \{\pm 1\}$.

For an odd prime $q \nmid p$, the Artin symbol $(q\mathbb{Z},\, K/\mathbb{Q})$ equals the Frobenius element $\mathfrak{F}_q \in \mathrm{Gal}(K/\mathbb{Q})$. Hence

$$q \text{ splits in } K \iff \mathfrak{F}_q = \mathrm{Id} \iff (q\mathbb{Z},\, K/\mathbb{Q})) = 1 \iff \left(\frac{q}{p}\right) = 1\,.$$

We already know (from Example 2.4.34) that q splits in $K = \mathbb{Q}(\sqrt{p^*})$ if and only if $\left(\frac{p^*}{q}\right) = 1$. So we get

$$\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)\,,$$

which is evidently equivalent to the quadratic reciprocity law of Gauss. ■

Besides the Kronecker–Weber theorem, which we linked to Gauss' quadratic reciprocity just now, class field theory is also the source of many other reciprocity laws.

(4.3.33) Let L/K be a finite abelian extension of global fields. We denote (by a little abuse of notation) by

$$(\cdot\,,\, L/K)\ :\ \mathbf{I}_K \longrightarrow \mathrm{Gal}(L/K)$$

the composition of the natural map $\mathbf{I}_K \to \mathbf{C}_K$ with the Artin reciprocity map $\Psi_{L/K}$: $\mathbf{C}_K \to \mathrm{Gal}(L/K)$. For each $\mathfrak{p} \in \Omega_K$, we fix a place $\mathfrak{P} \in \Omega_L$ lying over $\mathfrak{p}$ and write

$$(\cdot\,,\, L_{\mathfrak{P}}/K_{\mathfrak{p}})\ :\ K_{\mathfrak{p}}^* \longrightarrow \mathrm{Gal}(L/K)$$

for the composition of the local Artin reciprocity map $\Psi_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}\ :\ K_{\mathfrak{p}}^* \to \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$ with the natural inclusion $\mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}) \hookrightarrow \mathrm{Gal}(L/K)$. Note that if L/K is unramified at $\mathfrak{p}$, then

$$(\alpha_{\mathfrak{p}}\,,\, L_{\mathfrak{P}}/K_{\mathfrak{p}}) = 1 \quad \text{for all } \alpha_{\mathfrak{p}} \in U_{\mathfrak{p}}$$

by Prop. 4.2.6 (and Thm. 4.2.3 (1)). Since L/K is unramified at almost all $\mathfrak{p} \in \Omega_K$, the product map

$$\mathbf{I}_K \longrightarrow \mathrm{Gal}(L/K)\ ; \quad \alpha = (\alpha_{\mathfrak{p}}) \longmapsto \prod_{\mathfrak{p}} (\alpha_{\mathfrak{p}}\,,\, L_{\mathfrak{P}}/K_{\mathfrak{p}})$$

is a well defined group homomorphism.

By the compatibility of the local and global Artin reciprocity maps (Thm. 4.3.4 (2)), we have the commutative diagram

(4.3.33.1)

$$\begin{array}{ccc} K_{\mathfrak{p}}^* & \longrightarrow & \mathbf{I}_K \\ & {\scriptstyle (\cdot\,,\, L_{\mathfrak{P}}/K_{\mathfrak{p}})} \searrow \quad \swarrow {\scriptstyle (\cdot\,,\, L/K)} & \\ & \mathrm{Gal}(L/K) & \end{array}$$

for each $\mathfrak{p} \in \Omega_K$. Since $\mathbf{I}_K$ is topologically generated by the images of $K_{\mathfrak{p}}^*$ as $\mathfrak{p}$ varies over Ω_K, the diagram (4.3.33.1) shows that

(4.3.33.2)
$$(\alpha\,,\, L/K) = \prod_{\mathfrak{p}} (\alpha_{\mathfrak{p}}\,,\, L_{\mathfrak{P}}/K_{\mathfrak{p}}) \quad \text{for all } \alpha = (\alpha_{\mathfrak{p}}) \in \mathbf{I}_K\,.$$

This is called the ***product formula*** for the global Artin reciprocity map. ■

Since the map $(\cdot\,,\, L/K)$ vanishes at principal idèles, we get in particular the following theorem:

Theorem 4.3.34 (Hilbert reciprocity)**.** *For any finite abelian extension of global fields L/K, we have*

$$\prod_{\mathfrak{p}} (a\,,\, L_{\mathfrak{P}}/K_{\mathfrak{p}}) = 1 \;\in\; \mathrm{Gal}(L/K) \quad \textit{for all}\;\; a \in K^*\,.$$

(4.3.35) Let K be any global field and $n \in \mathbb{N}^*$ such that $\mathrm{char}(K) \nmid n$. Assume that K contains a primitive n-th root of unity $\xi_n \in \overline{K}$.

For each place $\mathfrak{p} \in \Omega_K$, let

$$(\cdot,\,\cdot)_{\mathfrak{p}} = (\cdot,\,\cdot)_{n,\mathfrak{p}} \;:\; K^* \times K^* \longrightarrow \mu_n(K)\;;\; (a,\,b) \longmapsto \frac{(a,\,K_{\mathfrak{p}}(\sqrt[n]{b})/K_{\mathfrak{p}})\,\sqrt[n]{b}}{\sqrt[n]{b}}$$

denote the restriction of the Hilbert symbol $(\cdot,\,\cdot)_{n,\,K_{\mathfrak{p}}}$ for the local field $K_{\mathfrak{p}}$, defined as in (4.2.13). ■

Theorem 4.3.36 (Product formula for the Hilbert symbol)**.** *With notation and hypotheses as in (4.3.35), we have*

$$\prod_{\mathfrak{p}} (a\,,\, b)_{\mathfrak{p}} = 1 \quad \textit{for all}\;\; a,\, b \in K^*\,.$$

Proof. Fix $b \in K^*$ and put $L = K(\sqrt[n]{b})$. Then $L_{\mathfrak{P}} = K_{\mathfrak{p}}(\sqrt[n]{b})$ in Thm. 4.3.34. Hence

$$\prod_{\mathfrak{p}} (a,\, K_{\mathfrak{p}}(\sqrt[n]{b})/K_{\mathfrak{p}}) = 1 \quad \text{in}\;\; \mathrm{Gal}(L/K)\,.$$

Letting both sides act on $\sqrt[n]{b}$ yields

$$\prod_{\mathfrak{p}} (a,\, K_{\mathfrak{p}}(\sqrt[n]{b})/K_{\mathfrak{p}})\,\sqrt[n]{b} = \left(\prod_{\mathfrak{p}} (a,\, K_{\mathfrak{p}}(\sqrt[n]{b})/K_{\mathfrak{p}})\right)\sqrt[n]{b} = \sqrt[n]{b}\,.$$

So we get

$$\prod_{\mathfrak{p}} (a\,,\, b)_{\mathfrak{p}} = \prod_{\mathfrak{p}} \frac{(a,\, K_{\mathfrak{p}}(\sqrt[n]{b})/K_{\mathfrak{p}})\,\sqrt[n]{b}}{\sqrt[n]{b}} = 1$$

as desired. □

(4.3.37) With notation and hypotheses as in (4.3.35), now suppose K is a number field. For each maximal ideal $\mathfrak{p}$ of $\mathcal{O}_K$, also regarded as a finite place of K, we have defined the n-th power residue symbol $\left(\frac{u}{\mathfrak{p}}\right)_n$ for all $\mathfrak{p}$ coprime to n and all $u \in U_{\mathfrak{p}}$ (Definition 4.2.16). Now we generalize this definition to the number field K as follows: For every fractional

ideal $\mathfrak{b}$ coprime to n, and every element $a \in K^*$ coprime to $\mathfrak{b}$, we define the ***n-th power residue symbol*** $\left(\frac{a}{\mathfrak{b}}\right)_n$ by

$$\left(\frac{a}{\mathfrak{b}}\right)_n := \prod_{\mathfrak{p} \in \Omega_K} \left(\frac{a}{\mathfrak{p}}\right)_n^{v_{\mathfrak{p}}(\mathfrak{b})} \in \mu_n(K)\,.$$

Here when $\mathfrak{p} \nmid \mathfrak{b}$ (e.g. $\mathfrak{p}$ is an infinite place), we have $v_{\mathfrak{p}}(\mathfrak{b}) = 0$ and the symbol $\left(\frac{a}{\mathfrak{p}}\right)_n^{v_{\mathfrak{p}}(\mathfrak{b})}$ is to be understood as $1 \in \mu_n(K)$. For $\mathfrak{p} \mid \mathfrak{b}$, we have $\mathfrak{p} \nmid n$ since $\mathfrak{b}$ is assumed coprime to n, so that $\left(\frac{a}{\mathfrak{p}}\right)_n$ is well defined in this case.

In the case $\mathfrak{b} = b\mathcal{O}_K$ is a principal ideal, we write for short $\left(\frac{a}{b}\right)_n = \left(\frac{a}{\mathfrak{b}}\right)_n$. ■

Using the product formula for the Hilbert symbol, one can easily prove the following:

Theorem 4.3.38 (Reciprocity law for n-th power residues)**.** *With notation and hypotheses as in (4.3.37), if $a, b \in K^*$ are coprime to each other and to n, then*

$$\left(\frac{a}{b}\right)_n \cdot \left(\frac{b}{a}\right)_n^{-1} = \prod_{\mathfrak{p} \mid n\infty} (a\,,\, b)_{n,\mathfrak{p}}\,.$$

Proof. Exercise. □

The interested reader may check that Thm. 4.3.38 generalizes the quadratic, cubic and quartic reciprocity laws (cf. Thms. 2.2.21 and 2.2.24) discussed earlier. (The case of quartic reciprocity involves more complicated computations.)

A Homework Assignments

A.1 Homework 1

Throughout what follows, let F be a finite field of characteristic $p > 0$ and let $q = |F|$. Let ζ be a primitive p-th root of unity in the field $\mathbb{C}$ of complex numbers, and Gauss sums and Jacobi sums are defined using ζ. The map $\psi : F \to \mathbb{C}^*$ is given by $\psi(\alpha) = \zeta^{\mathrm{Tr}_{F/\mathbb{F}_p}(\alpha)}$.

Exercise A.1.1. Let n, $n_1, \cdots, n_r$ be positive integers, $d = \gcd(n, q-1)$ and $d_i = \gcd(n_i, q-1)$. Let a, b, $a_1, \cdots, a_r \in F$.

1. Prove that $N(X^n = a) = \sum_{\chi^d = \varepsilon} \chi(a) = N(X^d = a)$.
2. Conclude that $N\big(a_1X_1^{n_1} + \cdots + a_rX_r^{n_r} = b\big) = N\big(a_1X_1^{d_1} + \cdots + a_rX_r^{d_r} = b\big)$.

Exercise A.1.2. Suppose p is odd.

1. Find a formula for the number of solutions to $X_1^2 + \cdots + X_r^2 = 0$ over F.
2. Let $a_1, \cdots, a_r \in F^*$. Generalize Prop. 1.5.2 by finding an explicit formula for the number of solutions to $a_1X_1^2 + \cdots + a_rX_r^2 = 1$ over F.

Exercise A.1.3. Let $\alpha \in F$. Prove that $\mathrm{Tr}_{F/\mathbb{F}_p}(\alpha) = 0$ if and only if $\alpha = \beta - \beta^p$ for some $\beta \in F$.

Exercise A.1.4. Let $\varphi : F \to \mathbb{C}^*$ be homomorphism from the additive group F to the multiplicative group $\mathbb{C}^*$.

Prove that there exists $a \in F$ such that $\varphi(x) = \psi(ax)$ for all $x \in F$.

Exercise A.1.5. For any function $f : F \to \mathbb{C}$, defines its ***Fourier transformation*** $\hat{f}$ to be the function

$$\hat{f}(s) = q^{-1} \sum_{t \in F} f(t)\overline{\psi(st)}\,.$$

1. Prove that $f(t) = \sum_{s \in F} \hat{f}(s)\psi(st)$ for all $t \in F$. (This is called the ***(finite) Fourier series expansion*** of f.)

2. Let χ be a nontrivial character of F. Prove that $\hat{\chi}(s) = q^{-1} g_{-s}(\chi)$.

Exercise A.1.6. Show that for every positive integer m, there is a homogeneous polynomial of degree m in m variables over F which has no nontrivial zero.

(*Hint: Let K be the unique degree m extension of F and fix a basis $\omega_1, \cdots, \omega_m$ of K over F. Show that $f(X_1, \cdots, X_m) := \prod_{i=0}^{m-1}(\omega_1^{q^i} X_1 + \cdots + \omega_m^{q^i} X_m)$ has the required properties.*)

Exercise A.1.7. Let $f \in F[X_1, \cdots, X_n]$ and $N = N(f = 0)$.

1. Show that
$$N = q^{n-1} + q^{-1} \sum_{a \in F^*} \sum_{x_1, \cdots, x_n \in F} \psi(af(x_1, \cdots, x_n))\,.$$

2. Let d be a positive divisor of $q - 1$. Let $a \in F^*$. Prove
$$\sum_{t \in F} \psi(at^d) = \sum_{\chi^d = \varepsilon \neq \chi} g_a(\chi)\,.$$

3. Let $m_1, \cdots, m_n \in \mathbb{N}^*$ and $d_i = \gcd(m_i, q-1)$. Let $a_i \in F^*$ and $f = a_1 X_1^{m_1} + \cdots + a_n X_n^{m_n}$. Show that
$$N = q^{n-1} + q^{-1} \sum_{a \in F^*} \prod_{i=1}^{n} \sum_{\chi_i^{d_i} = \varepsilon \neq \chi_i} g_{aa_i}(\chi_i)\,.$$

4. Deduce that
$$|N - q^{n-1}| \leq (q-1)(d_1 - 1) \cdots (d_n - 1) q^{\frac{n}{2} - 1}\,.$$

Exercise A.1.8. In this exercise, we prove the Chevalley–Warning theorem and provide a combinatorial application.

1. We use the convention that for every $x \in F$ (even for $x = 0$), $x^0 = 1$ in F. Let $i \in [\![0,\, q-2]\!]$. Prove that
$$\sum_{x \in F} x^i = 0\,.$$

2. Let $n \in \mathbb{N}^*$, and let S be a polynomial in $F[X_1, \ldots, X_n]$, written as a sum of monomials in the following form
$$S = \sum_{(u_1,\ldots,u_n)\in\mathbb{N}^n} s_{u_1,\ldots,u_n} X_1^{u_1} X_2^{u_2} \cdots X_n^{u_n}\,,$$
where the coefficients $s_{u_1,\ldots,u_n} \in F$ are zero except for finitely many $(u_1, \ldots, u_n) \in \mathbb{N}^n$. For any element $a = (a_1, \ldots, a_n) \in F^n$, we write $S(a) = S(a_1, \ldots, a_n)$.

   Prove the formula
$$\sum_{a \in F^n} S(a) = \sum_{(u_1,\ldots,u_n)\in\mathbb{N}^n} s_{u_1,\ldots,u_n} \prod_{i=1}^{n} \sum_{y \in F} y^{u_i}\,.$$

3. Now let $P_1, \ldots, P_r$ ($r \geq 1$) be polynomials in $F[X_1, \ldots, X_n]$. Define
$$Z := \{a \in F^n \mid P_1(a) = P_2(a) = \cdots = P_r(a) = 0\}$$
and put
$$S(X_1, \ldots, X_n) := \prod_{j=1}^{r} \left(1 - P_j(X_1, \ldots, X_n)^{q-1}\right)\,.$$
   Prove
$$\sum_{a \in F^n} S(a) = |Z| \quad \text{in} \quad F\,.$$
   (Here we identity the integer $|Z|$ with its canonical image $|Z| \cdot 1_F$ in F.)

4. Suppose that $\sum_{j=1}^{r} \deg(P_j) < n$. Show that $|Z| \equiv 0 \pmod{p}$.

   Deduce that if the polynomials P_j are all homogeneous with $\sum_{j=1}^{r} \deg(P_j) < n$, then they have at least one common zero $a \in F^n$ with $a \neq (0, 0, \ldots, 0)$.

5. Let $c_1, \ldots, c_{2p-1} \in \mathbb{Z}$ (where p is a prime number as before). By considering the common zeros of the polynomials
$$Q := \sum_{i=1}^{2p-1} X_i^{p-1} \;\in\; \mathbb{F}_p[X_1, \ldots, X_{2p-1}]$$
   and
$$R := \sum_{i=1}^{2p-1} c_i X_i^{p-1} \;\in\; \mathbb{F}_p[X_1, \ldots, X_{2p-1}]\,,$$
   show that there exists a subset I of $[\![1,\, 2p-1]\!] = \{1, 2, \ldots, 2p-1\}$ with $|I| = p$ such that
$$\sum_{i \in I} c_i \equiv 0 \pmod{p}\,.$$

A.2 Homework 2

Exercise A.2.1. Let p be an odd prime number and let $\zeta \in \mathbb{C}$ be a primitive p-th root of unity. Let $\chi = \left(\frac{\cdot}{p}\right)$ be the Legendre symbol.

Prove that for all $a \in \mathbb{F}_p^*$, the quadratic Gauss sum $g_a(\chi) = \sum_{t\in\mathbb{F}_p} \chi(t)\zeta^{at}$ is equal to

$$G_a(p) := \sum_{t\in\mathbb{F}_p} \zeta^{at^2} .$$

Exercise A.2.2. Prove Lemma 2.1.7.

Exercise A.2.3. Prove Prop. 2.1.10

Exercise A.2.4. Prove the description of the ring $\mathcal{O}_K$ for quadratic fields stated Example 2.2.3 of the instructor's notes.

Exercise A.2.5. For $d = -3$, 2, 5, prove that the ring $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is Euclidean.

Exercise A.2.6. Determine $\mathcal{O}_K^*$ for all imaginary quadratic fields K.

Exercise A.2.7. Prove Lemma 2.2.7.

Exercise A.2.8. Let $p \in \mathbb{N}$ be a prime number.

1. Suppose $p \equiv 1 \pmod 4$. Prove that p is not prime in $\mathbb{Z}[i]$ and deduce that $p = N(\pi)$ for some irreducible element $\pi \in \mathbb{Z}[i]$.
2. Deduce that p is the sum of two integer squares if and only if $p = 2$ or $p \equiv 1 \pmod 4$.
3. Suppose $p \equiv 3 \pmod 4$. Prove that p is an irreducible element in $\mathbb{Z}[i]$.
4. Prove that $1 + i$ is an irreducible element in $\mathbb{Z}[i]$ and that 2 is associate to $(1 + i)^2$ in $\mathbb{Z}[i]$.

   (Recall that two elements a, b in a domain are called ***associate*** to each other, if ab^{-1} is a unit in the domain.)
5. Find all irreducible elements of $\mathbb{Z}[i]$.
6. Let $n \geq 1$ be a positive integer and write

   $$n = 2^k p_1^{a_1} \cdots p_r^{a_r} q_1^{b_1} \cdots q_s^{b_s}$$

   where $p_1, \ldots, p_r$ are distinct prime numbers satisfying $p_i \equiv 1 \pmod 4$ and $q_1, \ldots, q_s$ are distinct primes satisfying $q_j \equiv 3 \pmod 4$.

   Prove that n is the sum of two integer squares if and only if each b_j, $1 \leq j \leq s$ is even. (*Hint: n is the sum of two integer squares if and only if n is the norm of an element $\alpha \in \mathbb{Z}[i]$. Consider the factorization of α into a product of irreducible elements in $\mathbb{Z}[i]$.*)
7. Prove that if an integer is the sum of two squares of rational numbers, then it is the sum of two integer squares.

Exercise A.2.9. Prove Prop. 2.2.8.

Exercise A.2.10. Prove Prop. 2.2.10.

A.3 Homework 3

Throughout what follows, let $R = \mathbb{Z}[\omega]$, $\omega = \frac{-1+\sqrt{-3}}{2}$ and $N = N_{\mathbb{Q}(\omega)/\mathbb{Q}}$.

Exercise A.3.1. Let $\pi \in R$ be a primary prime element and write $\pi = a + b\omega$ with $a, b \in \mathbb{Z}$. Put $a = 3m - 1$ and $b = 3n$.

1. Show that $\chi_\pi(\omega) = \omega^{m+n}$.
2. Show that $\chi_\pi(\omega) = \begin{cases} 1 & \text{if } \pi \equiv 8 \pmod{3(1-\omega)R}\,, \\ \omega & \text{if } \pi \equiv 2 \pmod{3(1-\omega)R}\,, \\ \omega^2 & \text{if } \pi \equiv 5 \pmod{3(1-\omega)R}\,. \end{cases}$
3. Let q be a prime number such that $q \equiv 2 \pmod 3$.
   Prove $\chi_q(\omega) = \begin{cases} 1 & \text{if } q \equiv 8 \pmod 9\,, \\ \omega & \text{if } q \equiv 2 \pmod 9\,, \\ \omega^2 & \text{if } q \equiv 5 \pmod 9\,. \end{cases}$

Exercise A.3.2. Show that the following elements are prime in R:

$$1 - 2\omega\,, \quad -7 - 3\omega\,, \quad 3 - \omega\,.$$

For each of the above elements, find the primary prime associate to it.

Exercise A.3.3. Factorize the following numbers into primes in R:

$$7\,,\ 21\,,\ 45\,,\ 22\,,\ 143\,.$$

Exercise A.3.4. Put $F = R/5R$.

1. Find the number of cubes in F^*.
2. Show that $\omega(1-\omega)$ has order 8 in F^* and that $\omega^2(1-\omega)$ has order 24.
3. Let $\pi \in R$ be a primary prime element such that $5 \nmid \pi$. Prove that the congruence $x^3 \equiv 5 \pmod \pi$ is solvable in R if and only if
$$\pi \equiv 1\,,\ 2\,,\ 3\,,\ 4\,,\ 1+2\omega\,,\ 2+4\omega\,,\ 3+\omega \text{ or } 4+3\omega \pmod 5\,.$$

Exercise A.3.5. Let $\pi \in R$ be a complex primary prime and let $p = N(\pi)$. Let $a \in \mathbb{Z}$. Prove that $x^3 \equiv a \pmod p$ is solvable in $\mathbb{Z}$ if and only if $\chi_\pi(a) = 1$.

Exercise A.3.6. Prove that the congruence $x^3 \equiv 2 - 3\omega \pmod{11}$ has solutions in R.

Exercise A.3.7. For an arbitrary (not necessarily prime) element $\alpha \in R$, we say α is **primary** if $\alpha \equiv 2 \pmod{3R}$.

1. If γ, $\rho \in R$ are primary, show that $-\gamma\rho$ is primary.

2. Prove that if $\gamma \in R$ is primary, then there is a factorization

$$\gamma = \pm\gamma_1 \cdots \gamma_r$$

where the γ_i are (not necessarily distinct) primary primes. We call such a factorization a **primary factorization** of γ.

3. Let γ be a primary element with a primary factorization $\gamma = \pm\gamma_1 \cdots \gamma_r$. Define

$$\chi_\gamma(\alpha) := \chi_{\gamma_1}(\alpha) \cdots \chi_{\gamma_r}(\alpha)$$

for all $\alpha \in R$.

Prove that for all α, $\beta \in R$, $\chi_\gamma(\alpha\beta) = \chi_\gamma(\alpha)\chi_\gamma(\beta)$ and if $\alpha \equiv \beta \pmod{\gamma}$, then $\chi_\gamma(\alpha) = \chi_\gamma(\beta)$.

4. If γ, ρ are primary elements, show that $\chi_\gamma(\alpha)\chi_\rho(\alpha) = \chi_{-\rho\gamma}(\alpha)$ for all $\alpha \in R$.

5. Let $\gamma = A + B\omega$ be primary, where A, $B \in \mathbb{Z}$. Put $A = 3m - 1$ and $B = 3n$. Prove that $\chi_\gamma(\omega) = \omega^{m+n}$.

6. Show that for all primary elements γ, ρ, one has $\chi_\gamma(\rho) = \chi_\rho(\gamma)$.

Exercise A.3.8. Let $\pi \in R$ be a primary prime and write $\pi = a + b\omega$ with a, $b \in \mathbb{Z}$. Put $a = 3m - 1$ and $b = 3n$.

1. If π is rational, prove that $\chi_\pi(1 - \omega) = \omega^{2m}$.

In the following questions we assume π is complex and put $p = N(\pi)$.

2. Prove

$$\frac{p-1}{3} \equiv -2m + n \pmod{3}, \quad \frac{a^2-1}{3} \equiv m \pmod{3}.$$

3. Show that $\chi_\pi(a) = \omega^m$.

4. Show that $\chi_\pi(a + b) = \omega^{2n}\chi_\pi(1 - \omega)$.

5. Show that $\chi_{a+b}(\pi) = \chi_{a+b}(1 - \omega) = \omega^{2(m+n)}$.

6. Prove that $\chi_\pi(1 - \omega) = \omega^{2m}$.

Exercise A.3.9. Let $\pi \in R$ be a primary prime and write $\pi = a + b\omega$ with a, $b \in \mathbb{Z}$. Put $a = 3m - 1$ and $b = 3n$.

Prove

$$\chi_\pi(3) = \omega^{2n} \quad \text{and} \quad \chi_\pi(1-\omega) = \begin{cases} 1 & \text{if } \pi \equiv 8,\ 8+3\omega \text{ or } 8+6\omega \pmod{9}, \\ \omega & \text{if } \pi \equiv 5,\ 5+3\omega \text{ or } 5+6\omega \pmod{9}, \\ \omega^2 & \text{if } \pi \equiv 2,\ 2+3\omega \text{ or } 2+6\omega \pmod{9}. \end{cases}$$

Exercise A.3.10. Find all the integer solutions to $y^2 + 2 = x^3$. (*You may use the fact that* $\mathbb{Z}[\sqrt{-2}]$ *is a UFD.*)

A.4 Homework 4

Throughout what follows, let R denote an integral domain with fraction field K.

Exercise A.4.1. Suppose R is a local domain. Let I be a fractional ideal of R. Prove that I is invertible if and only if it is principal.
Hint: There exist $x \in I$, $y \in I^{-1}$ such that $xy \in R^*$. Then prove $I = xR$.

Exercise A.4.2. An **exponential valuation** on a field K is a map

$$v \,:\, K \longrightarrow \mathbb{R} \cup \{+\infty\}$$

such that the following properties hold for all x, $y \in K$:
(V1) $v(x) = +\infty$ if and only if $x = 0$.
(V2) $v(xy) = v(x) + v(y)$.
(V3) $v(x + y) \geq \min\{v(x), v(y)\}$.

Let v be an exponent valuation on K.

1. Prove that the subset
$$\mathcal{O}_v := \{x \in K \,:\, v(x) \geq 0\}$$
is a local ring, called the **valuation ring** of v, and that its maximal ideal is given by
$$\mathfrak{p}_v := \{x \in K \,:\, v(x) > 0\}\,.$$
We call $\mathfrak{p}_v$ the **valuation ideal** of v.
Show also that the fraction field of $\mathcal{O}_v$ is K.

2. Let $a_1, \cdots, a_n \in K$, where $n \geq 2$. Show that if $v(a_1) < v(a_i)$ for all $i = 2, \cdots, n$, then
$$v(a_1 + \cdots + a_n) = v(a_1)\,.$$

Exercise A.4.3. Prove that a Dedekind domain with only finitely many prime ideals is a PID.

Exercise A.4.4. Suppose R is a DVR with maximal ideal $\mathfrak{p}$. Let $k = R/\mathfrak{p}$ and $U = R^*$. Let v be the normalized discrete valuation of K associated to R. For each $n \geq 1$, define

$$U_n = 1 + \mathfrak{p}^n = \{x \in K \,|\, v(x - 1) \geq n\}\,.$$

1. Show that each U_n is a subgroup of U and that $\bigcap_{n=1}^{\infty} U_n = 1$.

2. Prove that the natural quotient map $R \to k = R/\mathfrak{p}$ induces an isomorphism of multiplicative groups $U/U_1 \cong k^*$.

3. Prove that for each $n \in \mathbb{Z}$, there is an isomorphism of R-modules $k = R/\mathfrak{p} \xrightarrow{\sim} \mathfrak{p}^n/\mathfrak{p}^{n+1}$.

4. Prove that for each $n \geq 1$, the map $u \mapsto u - 1$ induces an isomorphism of abelian groups $U_n/U_{n+1} \xrightarrow{\sim} \mathfrak{p}^n/\mathfrak{p}^{n+1}$.

5. Let p be the characteristic of k. (So $p = 0$ or p is a prime number.)

   (a) Show that $U_n^p := \{a^p \mid a \in U_n\}$ is contained in U_{n+1} for every $n \geq 1$.

   (b) Let $m \geq 1$ be an integer not divisible by p. Prove that for every $n \geq 1$, the group homomorphism
   $$U_n \longrightarrow U_n \; ; \quad u \longmapsto u^m$$
   is injective.

Exercise A.4.5. Prove that if a domain R is integrally closed, then so is the polynomial ring $R[t]$.

Exercise A.4.6. Let $A = \mathbb{Q}[X, Y]/(X^2 - Y^3)$. Show that A is a domain but it is not integrally closed.

Exercise A.4.7. Let R be a Dedekind domain and let $\mathfrak{a} \subseteq R$ be a nonzero ideal. Show that every ideal in the quotient ring $R/\mathfrak{a}$ is a principal ideal.

Exercise A.4.8. Show that every integral ideal of a Dedekind domain can be generated by two elements.

A.5 Homework 5

Throughout what follows, let R denote an integral domain with fraction field K and suppose $R \neq K$.

Generalizing the case of Dedekind domains, we denote by $\mathscr{I}(R)$ the set of *invertible* fractional ideals of R, and let $\mathscr{P}(R)$ be the subset consisting of principal fractional ideals. It is easily seen that $\mathscr{I}(R)$ is a multiplicative group and that $\mathscr{P}(R)$ is a subgroup of $\mathscr{I}(R)$. The quotient group $\mathrm{Pic}(R) := \mathscr{I}(R)/\mathscr{P}(R)$ is called the ***Picard group*** of R.

Exercise A.5.1. Let $I \in \mathscr{I}(R)$ (i.e. I is an invertible fractional ideal of R). Prove:

1. As an R-module, I is finitely generated.
2. For every maximal ideal $\mathfrak{m}$ of R, $IR_{\mathfrak{m}}$ is an invertible fractional ideal of $R_{\mathfrak{m}}$.

Exercise A.5.2. Prove Lemma 2.3.18.

Exercise A.5.3. Prove that the converse of Exercise A.5.1 is also true. That is, if I is a fractional ideal of R satisfying the two conditions in Exercise A.5.1, then I is invertible.

(*Hint: Use Lemma* 2.3.18.)

Exercise A.5.4. Let I, J be ideals in a ring A and suppose that they are coprime (i.e. $I + J = A$). Let n be a positive integer. Prove:

1. If $IJ = M^n$ for some ideal $M \subseteq A$, then $(I + M)^n = I$. (This shows that if a product of two coprime ideals is an n-th power, then both factors are n-th powers.)
2. If $I^n = J^n$, then $I = J = A$.

Exercise A.5.5. Let $R = \mathbb{Z}[\sqrt{-19}]$. Consider the principal ideals $I = (18 + \sqrt{-19})$ and $J = (18 - \sqrt{-19})$ in R.

1. Show that IJ is the cube of a principal ideal.
2. Show that there is a unique prime ideal $\mathfrak{p}$ of R such that $I = \mathfrak{p}^3$ and that this ideal $\mathfrak{p}$ is a non-principal maximal ideal.
3. Find $|R/\mathfrak{p}|$.
4. Is the Picard group $\mathrm{Pic}(R)$ trivial? Why?

Exercise A.5.6. Let $R = \mathbb{Z}[\sqrt{-19}]$ again. Now consider the ideal $\mathfrak{m} = (2\,,\, 1 - \sqrt{-19})$.

1. Show that $\mathfrak{m}$ is a maximal ideal and $\mathfrak{m}^2 = 2\mathfrak{m}$.
2. Show that in the localization $R_{\mathfrak{m}}$ the ideal $\mathfrak{m}R_{\mathfrak{m}}$ is not principal.
3. Show that $\mathfrak{m}$ is not invertible as a fractional ideal.

Exercise A.5.7. Let $R = \mathbb{Z}[\sqrt{-3}]$ and $R' = \mathbb{Z}[\omega]$, where $\omega = \frac{-1+\sqrt{-3}}{2}$.

1. Prove that for every $x \in \mathbb{C}$, there exists $r \in R$ such that $|x - r| \leq 1$.
2. Determine for which $x \in \mathbb{C}$ there is no element $r \in R$ such that $|x - r| < 1$.
3. Show that R' is a fractional ideal of R and that $(R')^{-1} = 2R'$ (as a fractional ideal of R).
4. Find a non-invertible fractional ideal of R.
5. Let I be a fractional ideal of R. Prove that either I is principal or $I = R'\alpha$ for some $\alpha \in K^*$ (with $K = \mathbb{Q}(\sqrt{-3})$).
6. Prove that R is not a PID but the Picard group $\mathrm{Pic}(R)$ is trivial.

Exercise A.5.8. Let R be the ring of algebraic integers in $\mathbb{C}$. Consider the ideal $I \subseteq R$ generated by the infinite subset $\{\sqrt[2^n]{2} \,|\, n \in \mathbb{N}\}$.

Show that I is not finitely generated. Deduce that R is not Noetherian (and hence not a Dedekind domain).

Exercise A.5.9. Prove that if R is a Dedekind domain, then there exists a set Ω of normalized discrete valuations of K such that the following two properties hold:

(R1) $R = \{x \in K \,|\, v(x) \geq 0 \text{ for all } v \in \Omega\}$;

(R2) for every $a \in K^*$, the set $\{v \in \Omega \,|\, v(a) \neq 0\}$ is finite.

Exercise A.5.10. Let Ω be a set of normalized discrete valuations of K satisfying properties (R1) and (R2) in Exercise A.5.9. For each $v \in \Omega$, let R_v be its valuation ring and let $\mathfrak{p}_v$ be the maximal ideal of R_v.

Suppose further that every nonzero prime ideal of R is maximal.

1. Let $\mathfrak{p}$ be a maximal ideal of R.

   (a) Let $z \in K^*$ be such that $R \cap z^{-1}R \subseteq \mathfrak{p}$. Show that there exists $v \in \Omega$ such that $\mathfrak{p} = R \cap \mathfrak{p}_v$ and $v(z) < 0$.

   (b) Prove that $\Omega_{\mathfrak{p}} := \{v \in \Omega \mid R_v \supseteq R_{\mathfrak{p}}\}$ is a finite set.

   (c) Prove that $R_{\mathfrak{p}} = R_v$ for a unique $v \in \Omega$. Thus $\Omega_{\mathfrak{p}}$ consists of a single element.

2. Prove that for every $v \in \Omega$, there exists a unique maximal ideal $\mathfrak{p}$ such that $R_v = R_{\mathfrak{p}}$.

3. Deduce from (1) and (2) that the map

$$\Omega \longrightarrow \mathrm{Spm}(R)\ ; \quad v \longmapsto \mathfrak{p}_v \cap R$$

   is well defined and bijective. Let $\mathfrak{p} \mapsto v_{\mathfrak{p}}$ denote its inverse map.

4. Let $I \subseteq R$ be a nonzero ideal.

   (a) Prove that $\{\mathfrak{p} \in \mathrm{Spm}(R) \mid v_{\mathfrak{p}}(I) \neq 0\}$ is finite, where $v_{\mathfrak{p}}(I) := \min\{v_{\mathfrak{p}}(x) \mid x \in I\}$.

   (b) Prove that there is a unique factorization $I = \prod_{\mathfrak{p} \in \mathrm{Spm}(R)} \mathfrak{p}^{r_{\mathfrak{p}}}$, where each $r_{\mathfrak{p}} \in \mathbb{N}$ and almost all of them are zero.

   (c) If $J \subseteq R$ is another nonzero ideal, show that $I \mid J$ if and only if $I \supseteq J$.

5. Prove that R is a Dedekind domain.

A.6 Homework 6

Throughout what follows, let A denote a Dedekind domain with fraction field K. Denote by $\overline{K}$ an algebraic closure of K and consider all algebraic extensions of K as contained in $\overline{K}$. Let L/K be a finite separable extension (contained in $\overline{K}$) and B be the integral closure of A in L. Let $\mathfrak{p} \in \mathrm{Spm}(A)$ and set $T_{\mathfrak{p}} := \{\mathfrak{P} \in \mathrm{Spm}(B) \mid \mathfrak{P} \cap A = \mathfrak{p}\}$.

Exercise A.6.1. Let $\mathfrak{P} \in T_{\mathfrak{p}}$. Let E/K be a subextension of L/K.

1. Prove that L/K is unramified at $\mathfrak{P}$ if and only if E/K is unramified at $\mathfrak{P} \cap E$ and L/E is unramified at $\mathfrak{P}$.

2. Prove that $\mathfrak{p}$ is totally ramified (resp. inert) in L/K if and only if $\mathfrak{P} \cap E$ is totally ramified (resp. inert) in L/E and $\mathfrak{p}$ is totally ramified (resp. inert) in E/K.

3. Prove that the following conditions are equivalent:

   (a) $\mathfrak{p}$ splits completely in L/K.

   (b) $\mathfrak{p}$ splits completely in E/K and every prime ideal of $B \cap E$ lying over $\mathfrak{p}$ splits completely in L/E.

When L/K is a Galois extension, show that the above conditions are also equivalent to the following:

(c) $\mathfrak{p}$ splits completely in E/K and some prime ideal of $B \cap E$ lying over $\mathfrak{p}$ splits completely in L/E.

4. Let L'/K be another finite separable extension. Suppose that $\mathfrak{p}$ is unramified in L/K and totally ramified in L'/K. Show that $L \cap L' = K$.

Exercise A.6.2. Suppose that L/K is a Galois extension with group $G = \mathrm{Gal}(L/K)$. Fix a $\mathfrak{P} \in T_{\mathfrak{p}}$ and let I, $D \leq G$ be the inertia group and the decomposition group of $\mathfrak{P}$. Let K_I and K_D denote the inertia field and the decomposition field of $\mathfrak{P}$ in L. Let E/K be a subextension of L/K and put $\mathfrak{P}_E = \mathfrak{P} \cap E$.

Prove:

1. $K_D \subseteq E$ if and only if $\mathfrak{P}_E B$ is a power of $\mathfrak{P}$.
2. $E \subseteq K_D$ if and only if $e(\mathfrak{P}_E|\mathfrak{p}) = f(\mathfrak{P}_E|\mathfrak{p}) = 1$.

   When K_D/K is a Galois extension, $\mathfrak{p}$ splits completely in E if and only if $E \subseteq K_D$.
3. $K_I \subseteq E$ if and only if $\mathfrak{P}_E B$ is a power of $\mathfrak{P}$ and the residue field extension $\kappa(\mathfrak{P})/\kappa(\mathfrak{P}_E)$ is purely inseparable.

   When $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ is separable, $K_I \subseteq E$ if and only if $\mathfrak{P}_E$ is totally ramified in L.
4. $E \subseteq K_I$ if and only if E/K is unramified at $\mathfrak{P}_E$.

Exercise A.6.3. Recall the following definition in group theory: For subgroups U, V of a group G, a **double coset** of G mod U, V is a subset of the form

$$U\sigma V := \{x\sigma y \,|\, x \in U,\, y \in V\} \quad \text{where } \sigma \in G\,.$$

The set of all these double cosets, which form a partition of G, is denoted $U\backslash G/V$.

1. Prove that if U and V are finite, then for any $\sigma \in G$,

$$|U\sigma V| = |U| \cdot [V : V \cap \sigma^{-1}U\sigma] = |V| \cdot [U : U \cap \sigma V \sigma^{-1}]\,.$$

2. Suppose G is finite and let $X \subseteq G$ be a complete system of representatives of the double cosets of G mod U, V (i.e., the map $X \to U\backslash G/V\,;\ x \mapsto UxV$ is bijective).

   Prove that $[G : U] = \sum_{\sigma \in X} [V : V \cap \sigma^{-1}U\sigma]$.

Exercise A.6.4. Let M/K be a finite Galois extension containing L/K, $G = \mathrm{Gal}(M/K)$ and $H = \mathrm{Gal}(M/L)$. Let C be the integral closure of A in M and fix a $\mathfrak{Q} \in \mathrm{Spm}(C)$ lying over $\mathfrak{p}$. Let $G_{\mathfrak{Q}} \leq G$ be the decomposition group of $\mathfrak{Q}$.

1. Prove that the rule

$$H\backslash G/G_{\mathfrak{Q}} \longrightarrow T_{\mathfrak{p}}\ ; \quad H\sigma G_{\mathfrak{Q}} \longmapsto \sigma\mathfrak{Q} \cap L$$

   is a well defined bijection.

2. Now suppose that M/K is the Galois closure of L/K, i.e., M/K is the smallest Galois extension (inside $\overline{K}$) containing L/K.

   Show that $\bigcap_{\sigma\in G} \sigma^{-1}H\sigma = 1$. Then deduce that $\mathfrak{p}$ splits completely in L/K if and only if $\mathfrak{p}$ splits completely in M/K.

Exercise A.6.5. Let L'/K be another finite separable extension.

1. Show that if $\mathfrak{p}$ splits completely in both L/K and L'/K, then $\mathfrak{p}$ also splits completely in the composite extension LL'/K.

2. Prove that if $\mathfrak{p}$ is unramified in both L/K and L'/K, then $\mathfrak{p}$ is also unramified in LL'/K. (*Hint: Question* 4 *in Exercise* A.6.2 *may be useful.*)

3. Let M/K be the Galois closure of L/K. Prove that $\mathfrak{p}$ is unramified in L/K if and only if it is unramified in M/K.

Exercise A.6.6. Suppose that L/K is a Galois extension with group $G = \mathrm{Gal}(L/K)$, and suppose that the residue field $\kappa(\mathfrak{p}) = A/\mathfrak{p}$ is a finite field.

1. Prove that if $\mathfrak{p}$ is inert in L/K, then G is cyclic.

   In the remaining questions of this exercise, by an **intermediate field** we mean a field E such that $K \subseteq E \subseteq L$ and $E \neq L$.

2. Suppose $\mathfrak{p}$ is totally ramified in every intermediate field, but not totally ramified in L. Prove that G is cyclic of prime order.

3. Suppose that for every intermediate field E, $B \cap E$ has a unique prime ideal lying over $\mathfrak{p}$, but B has more than one prime ideals lying over $\mathfrak{p}$. Prove the same conclusion as in the previous question.

4. Suppose $\mathfrak{p}$ is unramified in every intermediate field, but ramified in L. Prove that G has a unique smallest nontrivial subgroup H, and that H is normal in G. Deduce that G has prime power order, H has prime order, and H is contained in the center of G.

5. Suppose $\mathfrak{p}$ splits completely in every intermediate field, but not in L. Prove the same conclusion as in the previous question.

6. Suppose $\mathfrak{p}$ is inert in every intermediate field but not inert in L. Prove that G is cyclic of prime power order.

Exercise A.6.7. Suppose L/K is a Galois extension and let K'/K be another finite separable extension. Let $L' = LK'$. Then L'/K' is a Galois extension and we can identify the Galois group $\mathrm{Gal}(L'/K')$ as a subgroup of $\mathrm{Gal}(L/K)$ by the restriction map $\sigma' \mapsto \sigma'|_L$.

Let A', B' denote the integral closures of A in K' and L' respectively. Fix a prime ideal $\mathfrak{P}'$ of B' lying over $\mathfrak{p}$ and put $\mathfrak{P} = \mathfrak{P}' \cap B$, $\mathfrak{p}' = \mathfrak{P}' \cap A'$. Let $D(\mathfrak{P}|\mathfrak{p}) \leq \mathrm{Gal}(L/K)$ and $I(\mathfrak{P}|\mathfrak{p}) \leq \mathrm{Gal}(L/K)$ be the decomposition group and the inertial group of $\mathfrak{P}|\mathfrak{p}$ and similarly for $D(\mathfrak{P}'|\mathfrak{p}') \leq \mathrm{Gal}(L'/K')$ and $I(\mathfrak{P}'|\mathfrak{p}') \leq \mathrm{Gal}(L'/K')$.

1. Show that $D(\mathfrak{P}'|\mathfrak{p}') \leq D(\mathfrak{P}|\mathfrak{p})$ and $I(\mathfrak{P}'|\mathfrak{p}') \leq I(\mathfrak{P}|\mathfrak{p})$ (when $\mathrm{Gal}(L'/K')$ is considered as a subgroup of $\mathrm{Gal}(L/K)$).

2. Assume $\kappa(\mathfrak{p})$ is perfect. Prove that if $\mathfrak{p}$ is unramified (resp. splits completely) in L/K, then $\mathfrak{p}'$ is unramified (resp. splits completely) in L'/K'.

Exercise A.6.8. Suppose L/K is a Galois extension with Galois group $G = \mathrm{Gal}(L/K)$. Fix $\mathfrak{P} \in T_{\mathfrak{p}}$ and let $D \leq G$ be the decomposition group of $\mathfrak{P}|\mathfrak{p}$. For each $m \in \mathbb{N}$ define

$$G_m := \{\sigma \in G \,|\, \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{P}^{m+1}} \text{ for all } \alpha \in B\}\,.$$

Prove:

1. Each G_m is a normal subgroup of D.

2. The intersection $\bigcap_{m\geq 0} G_m$ is 1, hence $G_m = 1$ for sufficiently large m.

A.7 Homework 7

Throughout what follows, let A be a Dedekind domain with fraction field K and L/K be a finite separable extension. Let B denote the integral closure of A in L.

Exercise A.7.1. Let $n \geq 2$. Suppose that $f(t) = t^n + bt + c \in K[t]$ is a separable irreducible polynomial.

Show that

$$\mathrm{disc}(f) = (-1)^{\frac{n(n-1)}{2}}\left((1-n)^{n-1}b^n + n^n c^{n-1}\right).$$

Exercise A.7.2. Let F be a number field and let d_F be its absolute discriminant.

Prove Stickelberger's relation: $d_F \equiv 0$ or $1 \pmod 4$.

Exercise A.7.3. Let $\alpha_1, \cdots, \alpha_n$ be a K-basis of L with each $\alpha_i \in B$. Let $\Delta := \mathrm{disc}_{L/K}(\alpha_1, \cdots, \alpha_n)$.

Prove that every element $\alpha \in B$ can be expressed in the form

$$\alpha = \frac{a_1\alpha_1 + \cdots + a_n\alpha_n}{\Delta} \quad \text{with each } a_i \in A \text{ and } \frac{a_i^2}{\Delta} \in A\,.$$

In particular, $\Delta B \subseteq A\alpha_1 + \cdots + A\alpha_n$.

Exercise A.7.4. Let M/K and L/K be separable extensions of degree m and n respectively, both contained in a fixed algebraic closure $\overline{K}$ of K. Let $F = ML$ be the composite field inside $\overline{K}$. Suppose that $[F : K] = mn$.

Prove that the restriction map

$$\begin{aligned} \mathrm{Hom}_{K\text{-alg}}(F, \overline{K}) &\longrightarrow \mathrm{Hom}_{K\text{-alg}}(M, \overline{K}) \times \mathrm{Hom}_{K\text{-alg}}(L, \overline{K}) \\ \tau &\longmapsto (\tau|_M\,,\, \tau|_L) \end{aligned}$$

is bijective.

Hint: If $L = K(\alpha)$, then $F = M(\alpha)$. Show that every K-embedding $M \to \overline{K}$ extends to precisely n K-embeddings of $F = ML$ into $\overline{K}$.

Exercise A.7.5. Let M, L, F be as in Exercise A.7.4. Let $\mathcal{O}_M$, $\mathcal{O}_L$ and $\mathcal{O}_F$ be the integral closures of A in M, L and F respectively.

Suppose that M/K (resp. L/K) integral basis $\alpha_1, \cdots, \alpha_m$ (resp. $\beta_1, \cdots, \beta_n$) relative to A. Put

$$d_M := \mathrm{disc}_{M/K}(\alpha_1, \cdots, \alpha_m)\,, \quad d_L := \mathrm{disc}_{L/K}(\beta_1, \cdots, \beta_n)\,.$$

1. Show that the discriminant of the mn elements $\alpha_i\beta_j \in F$ is $\mathrm{disc}_{F/K}(\alpha_i\beta_j) = d_M^n d_L^m$.
2. Prove that $\mathrm{disc}_{F/L}(\alpha_1, \cdots, \alpha_m) = d_M$ and that $d_M\mathcal{O}_F \subseteq \mathcal{O}_L\mathcal{O}_M$.
3. Assume further that there exists $d \in A$ such that $dA = d_MA + d_LA$. Show that $d\mathcal{O}_F \subseteq \mathcal{O}_L\mathcal{O}_M$.
4. Suppose that $A = d_MA + d_LA$. Prove that the mn elements $\alpha_i\beta_j$ form an integral basis of F/K relative to A and that $d_F = d_M^n d_L^m$.

Exercise A.7.6. In the context of Thm. 2.4.32 (Kummer–Dedekind theorem), prove that the condition $\mathfrak{p} \nmid \mathrm{disc}(f)\mathfrak{d}(B/A)^{-1}$ holds if the following holds:

As a subgroup, $A[\alpha]$ has finite index in B and $\mathrm{char}(A/\mathfrak{p}) \nmid [B : A[\alpha]]$.

(*Hint: Compare $\mathfrak{d}(mB/A)$ and $\mathfrak{d}(A[\alpha]/A)$, where $m = [B : A[\alpha]]$.*)

Exercise A.7.7. Let L be a quadratic field, σ the nontrivial element of $\mathrm{Gal}(L/\mathbb{Q})$. Show that L has an integral basis of the form α, $\sigma(\alpha)$ (with $\alpha \in \mathcal{O}_L$) if and only if d_L is odd.

Exercise A.7.8. Let $A = \mathbb{Z}$ and $L = \mathbb{Q}(\xi_5)$, where $\xi_5 \in \mathbb{C}$ is a primitive 5-th root of unity. Find the explicit prime factorization of $p\mathcal{O}_L$ for $p = 2$, 3, 5, 11, 19.

Exercise A.7.9. Suppose that K is a finite field of cardinality q. Let r be the order of q mod n, i.e.,

$$r = \min\{m \in \mathbb{N}^* \mid q^m \equiv 1 \pmod{n}\}\,.$$

Prove that $[K(\xi_n) : K] = r$ and that the minimal polynomial of ξ_n over K is $f(t) = (t - \xi)(t - \xi^q)\cdots(t - \xi^{q^{r-1}}) = \prod_{i=0}^{r-1}(t - \xi^{q^i})$. Let $L^{(1)}$ be the kernel of the norm map $N_{L/K} : L^* = K(\xi_n)^* \to K^*$. Prove that for every generator α of the (cyclic) group $L^{(1)}$ we have $L = K(\alpha)$.

Exercise A.7.10. Let $L = \mathbb{Q}(\sqrt{5}, \sqrt{-1})$.

1. Show that $L/\mathbb{Q}$ is Galois extension of degree 4 and find its Galois group.
2. Find an integral basis of L and compute d_L.
3. Let p be a prime number. Show that p is ramified in L if and only if $p \in \{2, 5\}$, and that for $p = 2, 5$, the ramification index $e(\mathfrak{P} \,|\, p)$ is 2 for any $\mathfrak{P} \in \mathrm{Spm}(\mathcal{O}_L)$ lying over p.
4. For each prime number p, let D_p (resp. I_p) be the decomposition group $D(\mathfrak{P} \,|\, \mathfrak{p})$ (resp. the inertia group $I(\mathfrak{P} \,|\, p)$) of $\mathfrak{P}$ in $\mathrm{Gal}(L/\mathbb{Q})$, for any $\mathfrak{P} \in \mathrm{Spm}(\mathcal{O}_L)$ lying over p.

   Find D_2, D_5, I_2, I_5 and their fixed subfields in L.
5. Let $K = \mathbb{Q}(\sqrt{-5})$. Show that every maximal ideal of $\mathcal{O}_K$ is unramified in L/K.

A.8 Homework 8

For each positive integer n, let ξ_n denote a primitive n-th root of unity in $\overline{\mathbb{Q}}$.

Exercise A.8.1. Let K be a finitely generated field, i.e., if F denotes the prime field of K, then there exist finitely many elements $\alpha_1, \cdots, \alpha_m \in K$ such that $K = F(\alpha_1, \cdots, \alpha_n)$.

Prove that

$$\mu_\infty(K) := \bigcup_{n \geq 1} \mu_n(K)$$

is a finite cyclic subgroup of K^*.

Exercise A.8.2. Let K be a number field.

1. (Kronecker) Suppose $\alpha \in \mathcal{O}_K$. Prove that α is a root of unity if and only if $|\sigma(\alpha)| = 1$ for all field embeddings $\sigma : K \to \mathbb{C}$.

   (*Hint: In the minimal polynomial of α, the absolute value of the coefficient of t^i is bounded in terms of n and i. The same property holds for all powers of α.*)
2. Give an example to show that the above statement is false if we only assume α lies in K but not necessarily in $\mathcal{O}_K$. That is, there may exists $\beta \in K$ such that $|\sigma(\beta)| = 1$ for all embeddings $\sigma : K \to \mathbb{C}$, but β is not a root of unity.

Exercise A.8.3. Prove Corollary 2.5.11.

Exercise A.8.4. Let m, n be natural numbers ≥ 1.

1. Suppose that m and n are coprime.

   (a) Show that $\alpha = \xi_m \xi_n$ is a primitive mn-th root of unity.

(b) Show that $\mathbb{Q}(\xi_m, \xi_n) = \mathbb{Q}(\alpha)$ and $\mathbb{Q}(\xi_m) \cap \mathbb{Q}(\xi_n) = \mathbb{Q}$.

2. More generally, let $l = \mathrm{lcm}(m, n)$ and $d = \gcd(m, n)$.

   (a) Prove that $\varphi(l)\varphi(d) = \varphi(m)\varphi(n)$.

   (b) Prove that $\mathbb{Q}(\xi_m, \xi_n) = \mathbb{Q}(\xi_l)$ and $\mathbb{Q}(\xi_m) \cap \mathbb{Q}(\xi_n) = \mathbb{Q}(\xi_d)$.

   (c) Is $\xi_m \xi_n$ always a primitive l-th root of unity ?

Exercise A.8.5. Let $n \geq 2$, $\xi = \xi_n \in \overline{\mathbb{Q}}$ and $K = \mathbb{Q}(\xi)$.

1. Let $k \in [\![1, n]\!]$ be coprime to n. Show that $\frac{1-\xi^k}{1-\xi} \in \mathcal{O}_K^*$.

2. Suppose that $n = p^r$ is a prime power and put $\eta = 1 - \xi$. Prove that $p\mathcal{O}_K = (\eta\mathcal{O}_K)^{\varphi(n)}$.

Exercise A.8.6. Let $n \geq 3$ be an integer and $K = \mathbb{Q}(\xi_n) \cap \mathbb{R}$.

1. Prove that for all $\ell \in \mathbb{Z}$ which is coprime to n, we have $K = \mathbb{Q}\left(\cos(2\pi\ell/n)\right)$.

2. Find $[K : \mathbb{Q}]$.

3. Show that $\mathcal{O}_K = \mathbb{Z}[\theta]$ where $\theta = \xi_n + \xi_n^{-1}$.

Exercise A.8.7. Recall that the Möbius function $\mu : \mathbb{N}^* \to \mathbb{Z}$ is defined by

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1\,, \\ (-1)^r & \text{if } n = p_1 \cdots p_r \text{ with } p_i \text{ distinct primes}\,, \\ 0 & \text{otherwise.} \end{cases}$$

1. (Möbius inversion formula) Let M be a multiplicative abelian group and let f, $g : \mathbb{N}^* \to M$ be functions. Prove that the following two statements are equivalent:

   (a) For all $n \in \mathbb{N}^*$,
   $$f(n) = \prod_{d\,|\,n} g(d)\,,$$
   where the product is taken over all positive divisors of n.

   (b) For all $n \in \mathbb{N}^*$,
   $$g(n) = \prod_{d\,|\,n} f(d)^{\mu(n/d)}\,.$$

2. Prove that for all $n \geq 1$,
$$\Phi_n(t) = \prod_{d\,|\,n} (t^d - 1)^{\mu(n/d)}$$
where d runs over positive divisors of n.

Exercise A.8.8. Let p be an odd prime and $\xi \in \overline{\mathbb{Q}}$ a primitive p^2-th root of unity.

1. Show that $\mathbb{Q}(\xi)$ contains a unique subfield F with $[F : \mathbb{Q}] = p$.
2. Show that 2 splits completely in F if and only if $2^{p-1} \equiv 1 \pmod{p^2}$.
3. Now suppose $p = 5$.
   (a) For $q = 2, 3, 5$, find the prime factorization of $q\mathcal{O}_F$.
   (b) For $q = 2, 3, 5$, find the decomposition field and the inertia field of q in F.
   (c) Prove that a prime number q splits completely in F if and only if $q \equiv \pm 1, \pm 7 \pmod{25}$.

A.9 Homework 9

Throughout what follows, let K be a number field of degree n and let r_1 (resp. $2r_2$) be the number of real (resp. imaginary) embeddings of K into $\mathbb{C}$.

Exercise A.9.1 (Brill's theorem)**.** Show that the sign of the discriminant d_K is $(-1)^{r_2}$, i.e., $d_K = (-1)^{r_2}|d_K|$.

Exercise A.9.2. Prove that in Thm. 2.6.4, the second assertion follows from the first one.

Exercise A.9.3. Find the class number of the field $\mathbb{Q}(\sqrt{14})$.

Exercise A.9.4. Let A be a domain and let a, $b \in A$ be nonzero elements. Suppose that A/aA and A/bA are finite. Prove that A/abA is finite and $|A/abA| = |A/aA| \cdot |A/bA|$.

Exercise A.9.5. By a **number ring** we mean a subring of a number field, which is not a field itself.

Let R be a number ring with fraction field K.

1. Prove that for every nonzero ideal I of R, $I \cap \mathbb{Z} \neq 0$.
2. Let $m \in \mathbb{N}^*$. Prove that for every finitely generated $\mathbb{Z}$-submodule $M \subseteq R$, the quotient M/mM is finite of order $\leq m^n$ (where $n = [K : \mathbb{Q}]$).
3. Prove that for every nonzero ideal I of R, the quotient R/I is finite.

   We can thus define the **absolute norm** of I as $\mathbf{N}(I) := |R/I|$.
4. Show that R is Noetherian and that every nonzero prime ideal of R is maximal.
5. Let $N \in \mathbb{N}^*$. Prove that there are only finitely many nonzero ideals of R with absolute norm $\leq N$.

6. Let $I \subseteq R$ be a nonzero ideal. Prove that there is a natural isomorphism of R-modules
$$R/I \xrightarrow{\sim} \bigoplus_{\mathfrak{p}\in \mathrm{Spm}(R)} R_{\mathfrak{p}}/IR_{\mathfrak{p}} = \bigoplus_{\substack{\mathfrak{p}\in \mathrm{Spm}(R)\\ I\subseteq\mathfrak{p}}} R_{\mathfrak{p}}/IR_{\mathfrak{p}}\ .$$
(*Hint: Since $A := R/I$ is finite, it is not hard to show that every maximal ideal of A is nilpotent, for example, by localization and then applying Nakayama's lemma. Then prove that the only prime ideal of R containing $J_{\mathfrak{p}} := IR_{\mathfrak{p}} \cap R$ is $\mathfrak{p}$, and deduce that $R/J_{\mathfrak{p}} \cong R_{\mathfrak{p}}/IR_{\mathfrak{p}}$.*)

7. Let I, J be nonzero ideals in R and suppose that I and J are invertible as fractional ideals. Prove $\mathbf{N}(I)\mathbf{N}(J) = \mathbf{N}(IJ)$. (*Hint: By Exercises A.4.1 and A.5.1, $IR_{\mathfrak{p}}$ is a principal ideal for every $\mathfrak{p} \in \mathrm{Spm}(R)$. Then use Exercise A.9.4.*)

8. Let $\mathfrak{p} \in \mathrm{Spm}(R)$. Prove that $\mathfrak{p}$ is invertible (as a fractional ideal) if and only if $R_{\mathfrak{p}}$ is a DVR. (*Hint: You may use Exercise A.5.3.*)

Exercise A.9.6. Let A be a ring. An ideal $I \subseteq A$ is called **primary** if $I \neq A$ and if for all a, $b \in A$, $ab \in I$ implies $a \in I$ or $b \in \sqrt{I}$. Here
$$\sqrt{I} := \{x \in A \,|\, x^m \in I \text{ for some } m \in \mathbb{N}^*\}$$
is the **radical** of I.

1. Show that an ideal $I \subseteq A$ is primary if and only if $A/I \neq 0$ and every zero-divisor in A/I is nilpotent.

2. Show that a prime ideal is primary, and that if $I \subseteq A$ is a primary ideal, then $\sqrt{I}$ is a prime ideal.

   For any $\mathfrak{p} \in \mathrm{Spec}(A)$, a primary ideal I with $\sqrt{I} = \mathfrak{p}$ is called a **$\mathfrak{p}$-primary** ideal.

3. Suppose that the radical $\sqrt{I}$ of an ideal I is a maximal ideal. Prove that I is primary.

4. Find all the primary ideals in $\mathbb{Z}$.

5. Let $f : A \to B$ be a ring homomorphism. Show that if J is a primary ideal in B, then $f^{-1}(J)$ is a primary ideal in A.

6. Now suppose A is Noetherian. Let $\mathfrak{m}$ be a maximal ideal of A. Prove that the following statements are equivalent for an ideal $I \subseteq A$:

   (a) I is $\mathfrak{m}$-primary.

   (b) $\sqrt{I} = \mathfrak{m}$.

   (c) $\mathfrak{m}^r \subseteq I \subseteq \mathfrak{m}$ for some positive integer r.

7. Suppose A is a Noetherian local ring in which the only nonzero prime ideal is the maximal ideal $\mathfrak{m}$. Show that every nonzero ideal of A contains a power of $\mathfrak{m}$.

   (*Hint: Consider the collection S of nonzero ideals violating the statement. Then S has a maximal member I since A is Noetherian. Prove that I is a prime ideal and derive a contradiction.*)

Exercise A.9.7. Let R be a number ring in the sense of Exercise A.9.5. Let $I \subseteq R$ be a nonzero ideal. For each $\mathfrak{p} \in \mathrm{Spm}(R)$, put $I_{(\mathfrak{p})} := R \cap IR_{\mathfrak{p}}$.

1. Show that $I_{(\mathfrak{p})} = R$ if and only if $I \nsubseteq \mathfrak{p}$, and that when $I \subseteq \mathfrak{p}$, $I_{(\mathfrak{p})}$ is a $\mathfrak{p}$-primary ideal of R.

2. Let $\mathfrak{p}$, $\mathfrak{p}'$ be distinct maximal ideals of R. Let J and J' be $\mathfrak{p}$-primary and $\mathfrak{p}'$-primary ideals in R. Prove that J and J' are coprime.

3. Prove that
$$I = \prod_{\mathfrak{p} \in \mathrm{Spm}(R)} I_{(\mathfrak{p})} = \prod_{\substack{\mathfrak{p} \in \mathrm{Spm}(R) \\ \mathfrak{p} \supseteq I}} I_{(\mathfrak{p})} \ .$$
   Here, the rightmost product is to be understood as R if the set $\{\mathfrak{p} \in \mathrm{Spm}(R) \mid I \subseteq \mathfrak{p}\}$ is empty.

Exercise A.9.8. Let R be an order in K (cf. (2.6.13) in the lecture notes) and let $I \subseteq R$ be a nonzero ideal.

1. For any nonzero element $x \in R$, show that $\mathbf{N}(xR) = \#(R/xR) = |N_{K/\mathbb{Q}}(x)|$.

2. Prove that every ideal class in $\mathrm{Pic}(R)$ contains an integral ideal with absolute norm not exceeding the Minkowski constant $\leq M_R$, that $\mathrm{Pic}(R)$ is generated by the classes of invertible primary ideals of absolute norm $\leq M_R$, and that $\mathrm{Pic}(R)$ is a finite group.

3. Now let $R = \mathbb{Z}[\sqrt{-19}]$.

   (a) Prove that $3R$ is a maximal ideal and that $5R = \mathfrak{pq}$ with $\mathfrak{p}$, $\mathfrak{q}$ two distinct maximal ideals such that $\mathfrak{p}^3$ is principal.
   (*Hint: The generator of $\mathfrak{p}^3$ should be an element of norm 125. One can first find all elements of norm 125 and then check that one of them generates $\mathfrak{p}^3$.*)

   (b) Find all the primary ideals of R with absolute norm $\leq M_R$. (*Hint: You may use Exercise A.5.6.*)

   (c) Conclude that $\mathrm{Pic}(R) \cong \mathbb{Z}/3$.

A.10 Homework 10

Exercise A.10.1. Let $D > 1$ be a square-free integer, $K = \mathbb{Q}(\sqrt{D})$ and $d = d_K$ the discriminant of K.

1. Show that at least one of the equations $x^2 - dy^2 = -4$ and $x^2 - dy^2 = 4$ have integer solutions with both x and y positive.

2. Prove that the equation $x^2 - dy^2 = -4$ has integer solutions if and only if the fundamental unit of K has norm -1.

   (Recall that the fundamental unit of K is the unique element $\varepsilon \in \mathcal{O}_K^*$ such that $\mathcal{O}_K^* = \{\pm 1\} \times \varepsilon^{\mathbb{Z}}$.)

3. Let (x_1, y_1) be the unique pair of positive integers determined as follows:

   If $x^2 - dy^2 = -4$ has solutions in positive integers $(x, y) \in \mathbb{N}^* \times \mathbb{N}^*$, let (x_1, y_1) be the solution with smallest y; otherwise, let (x_1, y_1) be the solution in positive integers of $x^2 - dy^2 = 4$ with smallest y.

   Show that $\varepsilon_1 = \frac{x_1 + y_1\sqrt{d}}{2}$ is the fundamental unit of K.

Exercise A.10.2. Let K be a totally real number field of degree n and let T be a nonempty set of field embeddings from K to $\mathbb{R}$ such that $|T| < n$.

Prove that there exists $\varepsilon \in \mathcal{O}_K^*$ such that

$$0 < \tau(\varepsilon) < 1 \text{ for all } \tau \in T \quad \text{and} \quad \tau(\varepsilon) > 1 \text{ for all } \tau \notin T\,.$$

Exercise A.10.3. Let M be a subgroup of the additive group $\mathbb{R}$ endowed with the usual Euclidean topology. Prove that the following assertions are equivalent:
(i) M is not dense in $\mathbb{R}$.
(ii) There exists a real number $\varepsilon > 0$ such that $M \cap]-\varepsilon, \varepsilon[= \{0\}$.
(Here $]-\varepsilon, \varepsilon[$ denotes the open interval $\{x \in \mathbb{R} \mid -\varepsilon < x < \varepsilon\}$.)
(iii) M is discrete in $\mathbb{R}$, i.e., the subspace topology on M is the discrete topology.
(iv) $M = r\mathbb{Z}$ for some $r \in \mathbb{R}$.

Exercise A.10.4. Let K be a field and let v be an exponential valuation on K with valuation ring A. Let $(\hat{K}, \hat{v})$ be the completion of the valued field (K, v).

1. Let $\hat{A}$ denote the valuation ring of $\hat{v}$ in $\hat{K}$. Prove that $\hat{A}$ equals the topological closure of A in $\hat{K}$.

2. Show that $\hat{v}(\hat{K}^*) = v(K^*)$ and that the natural map $A \to \hat{A}$ induces an isomorphism on their residue fields. In particular, if v is discrete (resp. discrete and normalized), then so is $\hat{v}$.

Exercise A.10.5. Let R be a proper subring of a field K such that for every $x \in K^*$, either $x \in R$ or $x^{-1} \in R$. (We say that R is a **valuation ring** in K.)

1. Prove that R is integrally closed.

2. Let v be a nontrivial exponential valuation on a field K. Show that the ring $\mathcal{O}_v = \{x \in K \mid v(x) \geq 0\}$ is a valuation ring in the above sense, i.e., for all $x \in K^*$, either $x \in \mathcal{O}_v$ or $x^{-1} \in \mathcal{O}_v$. Deduce that $\mathcal{O}_v$ is integrally closed.

Exercise A.10.6. Let L/K be an algebraic extension of fields and let $|\cdot|_L$ be an absolute value on L. Let $|\cdot|_K$ be the restriction of $|\cdot|_L$ to K.

Prove that the absolute value $|\cdot|_L$ is trivial if and only if $|\cdot|_K$ is trivial.

Exercise A.10.7. Let $(K, |\cdot|)$ be a complete non-archimedean valued field. Let $(a_n)_{n\in\mathbb{N}}$ be a sequence in K. Prove that the series $\sum_{n=0}^{\infty} a_n$ converges in K if and only if $\lim_{n\to\infty} a_n = 0$ in K.

Exercise A.10.8. Let p be a prime number.

1. Show that the sequence $(10^{-n})_{n\in\mathbb{N}}$ diverges in $\mathbb{Q}_p$.

2. Let $\alpha \in \mathbb{Z}$ be coprime to p. Show that the sequence $(\alpha^{p^n})_{n\in\mathbb{N}}$ is convergent in $\mathbb{Q}_p$.

Exercise A.10.9. Let p be a prime number. Show that the only field automorphism of $\mathbb{Q}_p$ is the identity.

Exercise A.10.10. Let $|\cdot|_1, \cdots, |\cdot|_n$ be pairwise inequivalent non-archimedean absolute values of a field K. Prove that for all $a_1, \cdots, a_n \in K^*$ there exists an element $x \in K^*$ such that $|x|_i = |a_i|_i$ for each $i = 1, \cdots, n$.

A.11 Homework 11

Throughout what follows, let K be a field with a fixed algebraic closure $\overline{K}$, v a nontrivial (exponential) valuation on K. (Note that the existence of v implies that K is infinite.)

Exercise A.11.1. Let p, q be distinct prime numbers. Show that there is no field isomorphism between $\mathbb{Q}_p$ and $\mathbb{Q}_q$. (*Hint: Consider irreducible polynomials over the two fields.*)

Exercise A.11.2. Prove that if L/K is a purely inseparable extension, then v has a unique extension to L. Deduce that a separably closed field is henselian with respect to any non-archimedean valuation.

Exercise A.11.3. Suppose that (K, v) is henselian. Let $\alpha_1, \cdots, \alpha_n \in K$ be nonzero elements such that $v(\alpha_i)$, $1 \leq i \leq n$ are pairwise distinct. Let $f(t) = \prod_{i=1}^{n}(t - \alpha_i)$.

Show that there is a real number $\delta > 0$ such that for every monic polynomial $g \in K[t]$ of degree n with $|g - f| < \delta$, where $|\cdot|$ denotes the absolute value associated to v, the polynomial g has n distinct roots in K.

Hint: Consider the Newton polygon and use Prop. 3.2.9.

Exercise A.11.4. Prove the following theorem of F.K. Schmidt: Suppose that there are two inequivalent nontrivial valuations v, w on K such that (K, v) and (K, w) are both henselian. Then K is separably closed.

Hint: Use Exercise A.11.3.

Exercise A.11.5. Suppose that $(K, |\cdot|)$ is complete and denote the unique extension of $|\cdot|$ to $\overline{K}$ again by $|\cdot|$. Let L/K be an infinite separable algebraic extension in $\overline{K}/K$. For each $x \in L \setminus K$, define

$$\delta(x) := \min\{|x' - x| : \ x' \text{ is a conjugate of } x \text{ over } K \text{ and } x' \neq x\}\,.$$

1. Show that there is an infinite sequence $(x_n)_{n\geq 0}$ of elements in $L\setminus K$ that are linearly independent over K such that

$$|x_{n+1}| < \min\left\{\frac{1}{2}|x_n|\,,\ \delta\Big(\sum_{i=0}^{n} x_n\Big)\right\}.$$

2. Show that L is not complete.

Exercise A.11.6. Let $\mathcal{O}_v$ be the valuation ring of v in K and $\mathfrak{p}_v$ its maximal ideal. Prove that (K, v) is henselian if and only if every monic polynomial

$$f(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0 \in \mathcal{O}_v[t] \quad \text{ with } n \geq 1,\ a_0 \in \mathfrak{p}_v \text{ and } \ a_1 \notin \mathfrak{p}_v$$

has a root $a \in \mathfrak{p}_v$.

Hint: Use the Newton polygon.

Exercise A.11.7. Suppose that (K, v) is complete. Show that if K is separably closed, then it is algebraically closed.

Hint: Polynomials of the form $t^p - a$ can be approximated by separable polynomials of the form $t^p - \pi^n t - a$.

Exercise A.11.8. Suppose K is algebraically closed and let K_v be the completion of K with respect to v. Prove that K_v is algebraically closed.

Exercise A.11.9. Suppose (K, v) is henselian and let K_v be the completion of K with respect to v. Prove that K is separably closed in K_v.

Exercise A.11.10. Suppose v is a discrete valuation. Let w be a nontrivial valuation on K that is not equivalent to v.

Prove that (K, w) is not henselian. *Hint: Consider polynomials of the form $t^2 + \pi t + \pi'$, where π, π' are uniformizers for v.*

A.12 Homework 12

Exercise A.12.1. Let v be the usual archimedean absolute value on $\mathbb{Q}$, $n \in \mathbb{N}^*$ and $L = \mathbb{Q}(\sqrt[n]{2})$. Find the number of extensions of v to L.

Exercise A.12.2. Determine, up to equivalence, all the absolute values of the field $\mathbb{Q}(i)$.

Exercise A.12.3 (Newton iteration)**.** Let $(K, |\cdot|)$ be a non-archimedean valued field with valuation ring $\mathcal{O}_K$. Let $f \in \mathcal{O}_K[t]$. Let $a \in \mathcal{O}_K$ be such that $f'(a) \neq 0$ and

$$C := \Big|\frac{f(a)}{f'(a)^2}\Big| < 1\,.$$

1. Prove that there exists a polynomial $g(X, Y) \in \mathcal{O}_K[X, Y]$ such that $f(X+Y) = f(X) + f'(X)Y + Y^2 g(X, Y)$.

2. Define $a_1 = a - \frac{f(a)}{f'(a)}$. Show that $|f'(a_1)| = |f'(a)|$. (In particular, $f'(a_1) \neq 0$.)

3. Define the Newton sequence $(a_n)_{n\in\mathbb{N}}$ by

$$a_0 := a\,,\ a_{n+1} := a_n - \frac{f(a_n)}{f'(a_n)} \ \text{ for all } n \geq 0\,.$$

   Prove that

$$\Big|\frac{f(a_n)}{f'(a_n)^2}\Big| \leq C^{2^n} \quad \text{ for all } n \geq 0\,.$$

4. Now suppose that $(K, |\cdot|)$ is complete.

   (a) Show that the Newton sequence (a_n) above converges to an element $\xi \in \mathcal{O}_K$ and that it satisfies

$$f(\xi) = 0\,,\ |f'(\xi)| = |f'(a)| \quad \text{ and } |\xi - a_n| \leq C^{2^n}|f'(a)| \text{ for all } n \geq 0\,.$$

   (b) Show that ξ is the unique root of f in $\overline{K}$ such that $|\xi - a| \leq |f(a)/f'(a)|$.

Exercise A.12.4. Let $(K, |\cdot|)$ be a non-archimedean valued field with valuation ring $\mathcal{O}_K$.

1. Show that for every positive real number r, the subset

$$\{x \in K \,:\, |x| \leq r\}$$

   is open and closed in K for the valuation topology (i.e. the metric topology defined by the absolute value $|\cdot|$).

   In particular, $\mathcal{O}_K$ is open and closed in K.

2. Show that the unit group $\mathcal{O}_K^*$ is open and closed in K^*.

3. Show that K is totally disconnected.

   (A topological space is called **totally disconnected** if the only connected subsets are the singletons.)

Exercise A.12.5. Let $(K, |\cdot|)$ be a complete non-archimedean valued field of characteristic 0. Let $|\cdot|_{\mathbb{Q}}$ denote the restriction of $|\cdot|$ to $\mathbb{Q}$. It is either trivial or p-adic (i.e., equivalent to the p-adic absolute value for some prime number p). Define

$$B := \{x \in K \,:\, |x| < r\} \quad \text{ where } \ r := \begin{cases} 1 & \text{if } |\cdot|_{\mathbb{Q}} \text{ is trivial}\,, \\ |p|^{\frac{1}{p-1}} & \text{if } |\cdot|_{\mathbb{Q}} \text{ is } p\text{-adic}\,. \end{cases}$$

1. Show that B is an $\mathcal{O}_K$-submodule (in particular, an additive subgroup) of K.

2. Let $\mathcal{O}_K$ be the valuation ring of K and let $\mathfrak{p}_K$ be its maximal ideal. Prove that the power series

$$\log(1+x) := \sum_{n\geq 1} \frac{(-1)^{n+1}x^n}{n} \quad \text{and} \quad \exp(x) := \sum_{n\geq 0} \frac{x^n}{n!}$$

define continuous group homomorphisms

$$\log \,:\, U_1 := 1+\mathfrak{p}_K \longrightarrow K \quad \text{and} \quad \exp \,:\, B \longrightarrow K^*$$

such that $\log \circ \exp = \mathrm{Id}_B$ and $\exp \circ \log|_{1+B} = \mathrm{Id}_{1+B}$.

3. Show that if $|\cdot|_{\mathbb{Q}}$ is trivial, then the above homomorphism log is injective; and if $|\cdot|_{\mathbb{Q}}$ is p-adic, then the kernel of this log map consists precisely of roots of unity of p-power order.

Exercise A.12.6. Let $(K,\, v)$ be a discrete valuation field and let $\pi \in K$ be a uniformizer.

1. Show that the multiplicative subgroup $\pi^{\mathbb{Z}} := \{\pi^m \,|\, m \in \mathbb{Z}\}$, endowed with the subspace topology induced from the valuation topology of K, is a discrete subgroup in K^*.

2. Show that any finite subgroup of K^* is discrete.

3. Prove that there is an isomorphism of topological groups $K^* \cong \pi^{\mathbb{Z}} \times \mathcal{O}_K^*$.

   (A (multiplicative) **topological group** is a group G equipped with a topology such that the multiplication map $G \times G \to G \,:\, (a,\, b) \mapsto ab$ and the inversion map $G \to G \,:\, a \mapsto a^{-1}$ are both continuous, where $G \times G$ is endowed with the product topology. A **morphism of topological groups** is a continuous group homomorphism.)

Exercise A.12.7. Let p be a prime number and $r \in \mathbb{N}^*$. Let $\Phi(t) = \Phi_{p^r}(t) \in \mathbb{Q}[t]$ be the p^r-th cyclotomic polynomial over $\mathbb{Q}$.

Prove that $\Phi(t)$ remains irreducible in $\mathbb{Q}_p[t]$.

Exercise A.12.8. Let K be a complete discrete valuation field with valuation ring $\mathcal{O}_K$ and residue field k. Suppose that k is a finite field of cardinality q. Let π be a uniformizer of K and $U_1 := 1 + \pi\mathcal{O}_K$.

1. Prove that the group $\mu_\infty(K)$ is finite. (*You may use the fact that K must be a p-adic field if* $\mathrm{char}(K) = 0$.)

   (For any field F and any $n \in \mathbb{N}^*$, let $\mu_\infty(F)$ (resp. $\mu_n(F)$) denote the multiplicative groups of all (resp. n-th) roots of unity in F.)

2. Prove that there is an isomorphism of topological groups

$$K^* \cong \pi^{\mathbb{Z}} \times \mu_{q-1}(K) \times U_1$$

3. Suppose that K is a p-adic field. Let p^a, where $a \in \mathbb{N}$, be the number of roots of unity of p-power order in K.

   (a) Prove that there is an isomorphism of topological groups

   $$U_1 \cong \mu_{p^a}(K) \times \mathbb{Z}_p^{\oplus[K:\mathbb{Q}_p]} .$$

   (b) Prove that for every $n \geq 1$,

   $$\#\big(K^*/K^{*n}\big) = n \cdot \#\big(\mathcal{O}_K^*/\mathcal{O}_K^{*n}\big) = n \cdot q^{v_K(n)} \cdot \#\mu_n(K) .$$

A.13 Homework 13

Exercise A.13.1. Prove Prop. 3.3.11.

Exercise A.13.2. In the context of Thm. 3.3.14, prove that taking residue fields defines an inclusion-preserving bijection

$$\{\text{subextensions of } K^{ur}/K\} \xrightarrow{\sim} \{\text{subextensions of } k_s/k\} ;$$

Show also that if L/K corresponds to ℓ/k via this bijection, then there is an isomorphism $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(\ell/k)$, and L/K is Galois if and only if ℓ/k is Galois.

Exercise A.13.3. Prove Lemma 3.3.16.

Throughout what follows, let K be a complete discrete valuation field with normalized discrete valuation v, $\mathcal{O}_K$ the valuation ring of K, $\pi \in \mathcal{O}_K$ a uniformizer and $k = \mathcal{O}_K/\pi\mathcal{O}_K$ the residue field. We fix an algebraic closure $\overline{K}$ of K and consider all algebraic extensions of K as contained in $\overline{K}$. For each algebraic extension M/K, let w_M denote the (unique) extension of v to M and $\mathcal{O}_M$ the valuation ring of M.

Exercise A.13.4. Show that if k is perfect and M is an infinite separable algebraic extension of K^{ur}, then w_M is not a discrete valuation.

Exercise A.13.5. Let L/K be a totally ramified extension of degree n and let F/K be an unramified extension of degree m. Let $M = LF$.

Prove that M/L is unramified, M/F is totally ramified and $[M : K] = mn$.

Exercise A.13.6. Recall that an **Eisenstein polynomial** of degree $n \geq 1$ over K is a polynomial of the form $f(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0$ with each $a_i \in \pi\mathcal{O}_K$ and $a_0 \notin \pi^2\mathcal{O}_K$.

1. Let $f \in \mathcal{O}_K[t]$ be an Eisenstein polynomial of degree $n \geq 1$. Let α be a root of f, $R = \mathcal{O}_K[\alpha]$ and $L = K(\alpha)$.

   Prove that R is a discrete valuation ring with fraction field L, that R is the integral closure of $\mathcal{O}_K$ in L and that L/K is totally ramified.

2. Conversely, let L/K be a totally ramified extension of degree n and let π_L be a uniformizer of L. Let $f(t) \in K[t]$ be the characteristic polynomial of the K-linear map $L \to L\,;\ x \mapsto \pi_L x$.

   Show that f is an Eisenstein polynomial and that the valuation ring $\mathcal{O}_L$ of L is $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$.

Exercise A.13.7. Let $e \geq 1$ be an integer such that $\mathrm{char}(k) \nmid e$. Let $\xi \in \overline{K}$ be a primitive e-th root of unity. Let $a \in K^*$ and write $a = \pi^r u$, where $\pi \in K$ is a uniformizer and $u \in \mathcal{O}_K^*$. Put

$$L := K(\sqrt[e]{a})\,,\ F := K(\xi,\ \sqrt[e]{u}) \quad \text{and} \quad M := K(\xi,\ \sqrt[e]{u},\ \sqrt[e]{\pi})\,.$$

1. Prove that F/K is an unramified extension and that M/F is totally and tamely ramified.

2. Prove that L/K is tamely ramified.

3. Prove that if $\gcd(v(a),\, e) = 1$, then L/K is totally ramified of degree e.

Exercise A.13.8. Let L/K and K'/K be finite extensions and $L' = LK'$. Prove:

1. Let F be an intermediate field of $K \subseteq L$. Then L/K is tamely ramified if and only if F/K and L/F are tamely ramified.

2. If L/K is tamely ramified, then L'/K' is also tamely ramified.

3. If both L/K and K'/K are tamely ramified, then L'/K is tamely ramified.

Exercise A.13.9. Let L/K be an algebraic extension.

1. Prove that the following assertions are equivalent:

   (a) The extension L/K is tamely ramified.

   (b) Every finite subextension of L/K is tamely ramified.

   (c) The field L is a union of finite tamely ramified extensions of K.

2. Show that the statements in Exercise A.13.8 are still true for any algebraic extensions L/K and K'/K.

Exercise A.13.10. Let L/K and K'/K be finite totally ramified extensions. Let $L' = LK'$. Is the extension L'/K necessarily totally ramified? If yes, please give a proof. Otherwise, please provide a counterexample.

A.14 Homework 14

Exercise A.14.1. Let p, q be distinct odd primes such that $p \equiv 1 \pmod 4$ and the Legendre symbol $\left(\frac{q}{p}\right) = -1$. Let $L = \mathbb{Q}_p(\sqrt[4]{qp^2})$.

Show that there is no intermediate field F in $L/\mathbb{Q}_p$ such that L/F is unramified and $F/\mathbb{Q}_p$ is totally ramified.

Exercise A.14.2. Prove Lemma 4.1.6.

Exercise A.14.3. Let $m \in \mathbb{N}^*$ and let $\xi \in \overline{\mathbb{Q}}_p$ be a primitive p^m-th root of unity. Put $K = \mathbb{Q}_p(\xi)$.

1. Prove that $K/\mathbb{Q}_p$ is totally ramified of degree $\varphi(p^m) = (p-1)p^{m-1}$.
2. Prove that $K/\mathbb{Q}_p$ is a Galois extension with $\mathrm{Gal}(K/\mathbb{Q}_p) \cong (\mathbb{Z}/p^m\mathbb{Z})^*$.
3. Show that the valuation ring of K is $\mathcal{O}_K = \mathbb{Z}_p[\xi]$ and that $1-\xi$ is a uniformizer of K.

Exercise A.14.4. Let K be a p-adic field with residue field k and $q = |k|$. Let $n \in \mathbb{N}^*$ be coprime to p and let $\xi \in \overline{K}$ be primitive n-th root of unity. Let $L = K(\xi)$.

1. Show that L/K is unramified of degree f, where f is the smallest positive integer such that $q^f \equiv 1 \pmod n$.
2. The Galois group $\mathrm{Gal}(L/K)$ is isomorphic to $\mathrm{Gal}(\ell/k)$ and is generated by the *Frobenius automorphism* $\varphi : x \mapsto x^q$, where ℓ/k denotes the residue field extension of L/K.
3. The valuation rings of L and K satisfy the relation $\mathcal{O}_L = \mathcal{O}_K[\xi]$.

Exercise A.14.5. Prove that for $K = \mathbb{Q}_p$, the maximal unramified extension K^{ur}/K is generated by all roots of unity of order prime to p.

Exercise A.14.6. Let A be a Dedekind domain with fraction field K and let L/K be a finite separable extension of degree n. Let B be the integral closure of A in L. Let $\alpha \in B$ be an element such that $L = K(\alpha)$ and let

$$f(t) = a_0 + a_1 t + \cdots + a_{n-1}t^{n-1} + t^n \in A[t]$$

be the monic minimal polynomial of α over K. Write

$$\frac{f(t)}{t-\alpha} = b_0 + b_1 t + \cdots + b_{n-1}t^{n-1} \quad \text{with } b_{n-1} = 1 \text{ and each } b_i \in B\,.$$

1. Prove that the dual basis of $1, \alpha, \ldots, \alpha^{n-1}$ with respect to the trace form $\mathrm{Tr}_{L/K}$ is given by $\frac{b_0}{f'(\alpha)}, \ldots, \frac{b_{n-1}}{f'(\alpha)}$. In particular, $b_0 b_1 \cdots b_{n-1} \neq 0$ and

$$\mathrm{Tr}_{L/K}\left(\frac{\alpha^i}{f'(\alpha)}\right) = \begin{cases} 0 & \text{if } 0 \le i \le n-2\,, \\ 1 & \text{if } i = n-1\,. \end{cases}$$

2. Let $\mathfrak{r}$ be the **conductor** of $A[\alpha]$ in B, i.e., $\mathfrak{r} := \{z \in B \,|\, zB \subseteq A[\alpha]\}$. Prove $\mathfrak{r} = f'(\alpha)\mathfrak{C}_{B/A}$.

   (*Hint: Use Prop.* 3.4.6.)

3. Show that $\mathfrak{D}_{B/A} \supseteq f'(\alpha)B$, and that the equality $\mathfrak{D}_{B/A} = f'(\alpha)B$ holds if and only if $B = A[\alpha]$.

4. If $\mathfrak{p} \subseteq A$ is a maximal ideal not contained in the conductor $\mathfrak{r}$, then $B_{\mathfrak{p}} = A_{\mathfrak{p}}[\alpha]$.

Exercise A.14.7. With notation and hypotheses as in Exercise A.14.6, assume that B is a discrete valuation ring with residue field ℓ.

1. Prove that A is also a discrete valuation ring.

2. Let k be the residue field of A, and suppose that ℓ/k is a separable extension. Let $\bar{x} \in \ell$ be such that $\ell = k(\bar{x})$ and let $g(t) \in A[t]$ be a lifting of the minimal polynomial $\bar{g}$ of $\bar{x}$.

   Prove that there is a lifting $x \in B$ of $\bar{x}$ such that $\pi := g(x)$ is a uniformizer of B.

3. Prove that there is an element $x \in B$ such that $B = A[x]$.

In Exercises A.14.8–A.14.10, let K be a complete discrete valuation field with normalized discrete valuation v and residue field k. We consider all algebraic extensions of K as contained in $\overline{K}$, a fixed an algebraic closure of K. For each algebraic extension M/K, let w_M denote the (unique) extension of v to M and $\mathcal{O}_M$ the valuation ring of M.

Exercise A.14.8. Let L/K be an algebraic extension with residue field extension ℓ/k. The composite V/K of all tamely ramified subextensions of L/K is called the **maximal tamely ramified subextension** of L/K. Suppose $p = \mathrm{char}(k) > 0$.

Prove that the residue field of V is the separable closure of k in ℓ and that

$$w_V(V^*) = w_L(L^*)^{(p)} := \{a \in w_L(L^*) \,|\, ma \in v(K^*) \text{ for some } m \in \mathbb{N} \text{ coprime to } p\}.$$

Exercise A.14.9. Let L/K be a finite totally and tamely ramified extension. Show that the intermediate fields of L/K correspond bijectively to the subgroups of the quotient $w_L(L^*)/v(K^*)$.

Exercise A.14.10. Let L/K be a finite separable extension with residue field extension ℓ/k. Assume that ℓ/k is a separable extension. Let $e = e(w_L|v)$ and let $s \in \mathbb{Z}$ be determined by $\mathfrak{P}^s = \mathfrak{D}_{L/K}$, where $\mathfrak{P}$ denotes the maximal ideal of $\mathcal{O}_L$. Let v_L be the normalized discrete valuation of L.

Prove:

1. If L/K is tamely ramified, then $s = e - 1$.

2. If L/K is wildly ramified, then $e \leq s \leq e - 1 + v_L(e)$.

A.15 Homework 15

Exercise A.15.1. Let R be a topological ring and let R^* be its group of units. Let $\mathcal{T}_1$ be the subspace topology on R^* induced from the inclusion $R^* \hookrightarrow R$. Let $\mathcal{T}_2$ be the subspace topology on R^* induced from the injection

$$R^* \hookrightarrow R \times R \,;\; x \longmapsto (x,\, x^{-1})\,,$$

where $R \times R$ is endowed with the product topology.

1. Show that $\mathcal{T}_1$ is weaker than $\mathcal{T}_2$, i.e., open subsets in $\mathcal{T}_1$ are all open subsets in $\mathcal{T}_2$.
2. Prove that R^* is a topological group with respect to the topology $\mathcal{T}_2$.
3. Now suppose $R = \mathbf{A}_K$ is the ring of adèles of a global field K, equipped with the adelic topology. Show that the topology $\mathcal{T}_2$ defined above is the same as the idelic topology on $\mathbf{I}_K = \mathbf{A}_K^*$.

Exercise A.15.2. Let $\mathcal{T}_1$ be the topology on the idèle group $\mathbf{I}_\mathbb{Q}$ induced from the adelic topology via the natural inclusion $\mathbf{I}_\mathbb{Q} \hookrightarrow \mathbf{A}_\mathbb{Q}$. Let us identify the set $\Omega_\mathbb{Q}$ of places of $\mathbb{Q}$ with the set $\mathcal{P} \cup \{\infty\}$, where $\mathcal{P}$ denotes the set of prime numbers. For each $i \geq 1$, let p_i be the i-th prime number (so that $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, etc.), and define the idèle $\alpha^{(i)} = (\alpha_v^{(i)})$ by

$$\alpha_v^{(i)} = \begin{cases} p_i & \text{if } v = p_i\,, \\ 1 & \text{if } v \neq p_i\,. \end{cases}$$

1. Prove that the sequence $\alpha^{(i)}$, $i \geq 1$ tends to 1 in the topology $\mathcal{T}_1$ of $\mathbf{I}_\mathbb{Q}$.
2. Prove that the inversion map $\mathbf{I}_\mathbb{Q} \to \mathbf{I}_\mathbb{Q}\,;\; x \mapsto x^{-1}$ is not continuous.
3. Deduce that the idelic topology of $\mathbf{I}_\mathbb{Q}$ is not equal to the above topology $\mathcal{T}_1$ (the adelic subspace topology).

Exercise A.15.3. Let F/K be a finite separable extension of non-archimedean local fields, and let L/K and M/F be finite Galois extensions with $L \subseteq M$. Show that the diagram

$$\begin{array}{ccc} F^* & \xrightarrow{N_{F/K}} & K^* \\ {\scriptstyle \Psi_{M/F}}\big\downarrow & & \big\downarrow{\scriptstyle \Psi_{L/K}} \\ \mathrm{Gal}(M/F)^{ab} & \xrightarrow{\sigma \mapsto \sigma|_L} & \mathrm{Gal}(L/K)^{ab} \end{array}$$

is commutative. (*Hint: Reduce to the case M/K is Galois and consider the extensions $M/(F \cap L)$ and $L/(F \cap L)$.*)

Exercise A.15.4. Let K be a non-archimedean local field. Let E_1/K and E_2/K be finite abelian extensions. Prove

$$\begin{aligned} N_{E_1E_2/K}((E_1E_2)^*) &= N_{E_1/K}(E_1^*) \cap N_{E_2/K}(E_2^*)\,, \\ N_{E_1 \cap E_2/K}((E_1 \cap E_2)^*) &= N_{E_1/K}(E_1^*) \cdot N_{E_2/K}(E_2^*)\,. \end{aligned}$$

Exercise A.15.5. Prove that Prop. 4.2.6 is a consequence of Thm. 4.2.3.

(*Hint: Consider the maximal unramified subextension T/K in L/K and show that for every uniformizer π_L of L, $N_{L/T}(\pi_L)$ is a uniformizer of T. Then use Thm.* 4.2.3 (4).)

Exercise A.15.6. With the notation and terminology of (4.2.10), prove that Theorems 4.2.3 and 4.2.9 are also true for archimedean local fields.

Exercise A.15.7. Let K be a non-archimedean local field. Let $n \in \mathbb{N}^*$.

1. Prove that if $\mathrm{char}(K) \nmid n$, then K^{*n} is an open subgroup of K^*.
2. Show that if $\mathrm{char}(K) = 0$, then every finite-index subgroup of K^* is an open subgroup. Show also that every open subgroup of K^* has finite index.

Exercise A.15.8. Prove Cor. 4.3.6.

B Exam Problems

B.1 Midterm (Takehome) Exam: 2021 fall semester

Exercise B.1.1. Let $L = \mathbb{Q}(\alpha)$ where $\alpha \in \mathbb{C}$ is a root of $f(t) = t^3 - t^2 - 2t - 8$. Let $\beta = \frac{\alpha^2 - \alpha}{2} - 1$.

1. Prove that f is irreducible over $\mathbb{Q}$.
2. Show that $\beta \in \mathcal{O}_L$ and find the minimal polynomial of β over $\mathbb{Q}$.
3. Compute $\mathrm{disc}_{L/\mathbb{Q}}(1, \alpha, \alpha^2)$ and $\mathrm{disc}_{L/\mathbb{Q}}(1, \alpha, \beta)$.
4. Prove that $1, \alpha, \beta$ form an integral basis of $\mathcal{O}_L$.
5. Prove that $\mathcal{O}_L^* \cong \mathbb{Z} \oplus (\mathbb{Z}/2)$.
6. Find the prime factorization of $p\mathcal{O}_L$ for $p = 503$. (*Observe that $f'/3$ has discriminant* $59 \pmod{503}$, *and* $59 \equiv 131^2 \pmod{503}$. *If needed, you may use the fact that a prime number ramifies in L if and only if it divides d_L.*)
7. Show that there is no element $\eta \in \mathcal{O}_L$ such that $\mathcal{O}_L = \mathbb{Z}[\eta]$. (*Hint: Show that* $\mathrm{disc}_{L/\mathbb{Q}}(1, \eta, \eta^2)$ *is always even.*)
8. Show that every element $\omega \in \mathcal{O}_L$ satisfies $\omega^2 \equiv \omega \pmod{2\mathcal{O}_L}$. Deduce that 2 splits completely in L.
9. Show that the class group $\mathcal{C}l(L)$ can be generated by 3 elements.

For each $n \in \mathbb{N}^*$, let Φ_n denote the n-th cyclotomic polynomial over $\mathbb{Q}$.

Exercise B.1.2. Let $n \in \mathbb{N}^*$ and p a prime number. Prove:

1. If n is odd and $n > 1$, then $\Phi_{2n}(t) = \Phi_n(-t)$.
2. If n is even, then $\Phi_{2n}(t) = \Phi_n(t^2)$.
3. If $p \,|\, n$, then $\Phi_n(t^p) = \Phi_{np}(t)$.
4. If $p \nmid n$, then $\Phi_n(t^p) = \Phi_{np}(t)\Phi_n(t)$.
5. Let $n = p_1^{r_1} \cdots p_k^{r_k}$ with p_i distinct prime numbers and $r_i \in \mathbb{N}^*$. Put $m = p_1 \cdots p_k$. Then
$$\Phi_n(t) = \Phi_m\left(t^{n/m}\right) .$$

Exercise B.1.3. Calculate $\Phi_n(1)$ and $\Phi_n(-1)$ for all $n \in \mathbb{N}^*$.

Exercise B.1.4. Let $K \subseteq L \subseteq M$ be finite separable extensions of fields with $l = [L : K]$ and $[M : L] = m$.

1. Let $\alpha_1, \cdots, \alpha_l \in L$ and $\beta_1, \cdots, \beta_m \in M$. Prove
$$\mathrm{disc}_{M/K}(\alpha_1\beta_1, \cdots, \alpha_l\beta_m) = \big(\mathrm{disc}_{L/K}(\alpha_1, \cdots, \alpha_l)\big)^m \cdot N_{L/K}\big(\mathrm{disc}_{M/L}(\beta_1, \cdots, \beta_m)\big) .$$
(*Hint: Some Galois-theoretic results, such as* [Mor96, Prop. 3.28 (3)] *and* [Hun80, p.286, Lemma V.6.11] *may be useful.*)
2. Let n be an integer ≥ 3 with $n \not\equiv 2 \pmod 4$. Let ξ be a primitive n-th root of unity in $\overline{\mathbb{Q}}$ and $L = \mathbb{Q}(\xi) \cap \mathbb{R}$. Compute the discriminant d_L of L.

B.2 Final Exam: 2021 fall semester

Duration: 3 hours

For each of the following exercises, you should try to give as much detail as necessary to justify your answer.

You are always allowed to assume the statements of some questions to answer subsequent questions.

Notation and conventions are used as in the instructor's lecture notes

[Hu] *Topics in Algebra and Number Theory*, SUSTech lecture notes, Jan. 3, 2022.

In case of any questions about the notation or the statements of exam problems, feel free to ask the proctor.

Exercise B.2.1. Let A be a Dedekind domain with fraction field K and let L/K be a finite separable extension. Let B be the integral closure of A in L. Assume that B is a discrete valuation ring with residue field ℓ.

1. Prove that A is also a discrete valuation ring.
2. Let k be the residue field of A, and suppose that ℓ/k is a separable extension. Let $\bar{x} \in \ell$ be such that $\ell = k(\bar{x})$ and let $g(t) \in A[t]$ be a lifting of the (monic) minimal polynomial $\bar{g}$ of $\bar{x}$.

   Prove that there is a lifting $x \in B$ of $\bar{x}$ such that $\pi := g(x)$ is a uniformizer of B.

3. Prove that there is an element $x \in B$ such that $B = A[x]$.

In Exercises B.2.2 and B.2.3, let K be a complete discrete valuation field with normalized discrete valuation v. For any finite extension L/K, let $\mathcal{O}_L$ denote the valuation ring of L and let w_L be the unique extension of v to L.

Exercise B.2.2. Recall that an Eisenstein polynomial of degree $n \geq 1$ over K is a polynomial of the form $f(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0$ with each $a_i \in \pi\mathcal{O}_K$ and $a_0 \notin \pi^2\mathcal{O}_K$, where $\pi \in \mathcal{O}_K$ denotes a uniformizer.

1. Let $f \in \mathcal{O}_K[t]$ be an Eisenstein polynomial of degree $n \geq 1$. Let α be a root of f, $R = \mathcal{O}_K[\alpha]$ and $L = K(\alpha)$.

   Prove that R is a discrete valuation ring with fraction field L, that R is the integral closure of $\mathcal{O}_K$ in L and that L/K is totally ramified.

2. Conversely, let L/K be a totally ramified extension of degree n and let π_L be a uniformizer of L. Let $f(t) \in K[t]$ be the characteristic polynomial of the K-linear map $L \to L\,;\ x \mapsto \pi_L x$.

   Show that f is an Eisenstein polynomial and that the valuation ring of L is $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$.

Exercise B.2.3. Let L/K be a finite separable extension with residue field extension ℓ/k. Assume that ℓ/k is a separable extension. Let $e = e(w_L|v)$ and let $s \in \mathbb{Z}$ be determined by $\mathfrak{P}^s = \mathfrak{D}_{L/K}$, where $\mathfrak{P}$ denotes the maximal ideal of $\mathcal{O}_L$. Let v_L be the normalized discrete valuation of L.

Prove:

1. If L/K is tamely ramified, then $s = e - 1$.

2. If L/K is wildly ramified, then $e \leq s \leq e - 1 + v_L(e)$.

(You are allowed to use without proof Exercise A.14.6 in [Hu].)

Exercise B.2.4. Let p be a prime number. Prove that the maximal unramified extension of $\mathbb{Q}_p$ is generated over $\mathbb{Q}_p$ by all roots of unity of order prime to p.

Exercise B.2.5. Let K be a p-adic field with valuation ring $\mathcal{O}_K$ and let $\pi \in \mathcal{O}_K$ be a uniformizer.

1. Prove that if $x \in 1 + 4\pi\mathcal{O}_K$, then x is a square in K.

2. Show that $K^{*2} = \{y^2 \,|\, y \in K^*\}$ is an open subgroup of K^*.

Exercise B.2.6. Let R be a topological ring and let R^* be its group of units. Let $\mathcal{T}_1$ be the subspace topology on R^* induced from the inclusion $\iota : R^* \hookrightarrow R$. Let $\mathcal{T}_2$ be the subspace topology on R^* induced from the injection

$$j \ :\ R^* \hookrightarrow R \times R\ ;\ x \longmapsto (x,\, x^{-1})\,,$$

where $R \times R$ is endowed with the product topology.

1. Show that $\mathcal{T}_1$ is weaker than $\mathcal{T}_2$, i.e., open subsets in $\mathcal{T}_1$ are all open subsets in $\mathcal{T}_2$.

2. Prove that R^* is a topological group with respect to the topology $\mathcal{T}_2$.

3. Now suppose $R = \mathbf{A}_K$ is the ring of adèles of a number field K, equipped with the adelic topology. Show that the topology $\mathcal{T}_2$ defined above is the same as the idelic topology on $\mathbf{I}_K = \mathbf{A}_K^*$.

   (*Hint: You may use that* $\mathbf{I}_K$ *is a topological group for the idelic topology and reduce to considering open neighborhoods of the identity.*)

In Exercises B.2.7 and B.2.8, let K be a number field with ring of integers $\mathcal{O}_K$, and let Ω_K be the set of all places of K. For each $\mathfrak{p} \in \Omega_K$, let $K_\mathfrak{p}$ be the completion of K at $\mathfrak{p}$. If $\mathfrak{p} \nmid \infty$, we shall also consider $\mathfrak{p}$ as a maximal ideal of $\mathcal{O}_K$, so that the absolute norm $\mathbf{N}(\mathfrak{p}) = \#(\mathcal{O}_K/\mathfrak{p})$ is defined.

If L/K is a finite Galois extension and $\mathfrak{p}$ is unramified in L/K, then for every place $\mathfrak{P}$ of L lying over $\mathfrak{p}$, we regard the Frobenius element $\mathfrak{F}_{\mathfrak{P}/\mathfrak{p}}$ as an element in $G = \mathrm{Gal}(L/K)$ (cf. [Hu] (4.3.3)). If C is a conjugacy class in G, i.e., $C = \{g\sigma g^{-1} \,|\, g \in G\}$ for some $\sigma \in G$, whether the condition $\mathfrak{F}_{\mathfrak{P}/\mathfrak{p}} \in C$ holds is independent of the choice of $\mathfrak{P}$, since for any two places $\mathfrak{P}$, $\mathfrak{P}'$ lying over $\mathfrak{p}$, the Frobenius elements $\mathfrak{F}_{\mathfrak{P}/\mathfrak{p}}$ and $\mathfrak{F}_{\mathfrak{P}'/\mathfrak{p}}$ are conjugate in G.

Exercise B.2.7. For any real number $x > 0$, define

$$\pi(x) := \#\{\mathfrak{p} \in \Omega_K \,:\, \mathfrak{p} \nmid \infty \text{ and } \mathbf{N}(\mathfrak{p}) \le x\}\,.$$

For any subset $S \subseteq \Omega_K$, the **density** $\delta(S)$ of S, if it exists, is defined to be the limit

$$\delta(S) := \lim_{x \to +\infty} \frac{\#\{\mathfrak{p} \in S \,:\, \mathfrak{p} \nmid \infty \text{ and } \mathbf{N}(\mathfrak{p}) \le x\}}{\pi(x)}\,.$$

1. Prove that if $S \subseteq \Omega_K$ is a finite subset, then $\delta(S) = 0$ and $\delta(\Omega_K \setminus S) = 1$.

   For the remaining questions, you are allowed to use without proof **Chebotarev's density theorem**: *Let L/K be a finite Galois extension with Galois group $G = \mathrm{Gal}(L/K)$. Let C be a conjugacy class in G. Then the set*

   $$\{\mathfrak{p} \,|\, L/K \text{ is unramified at } \mathfrak{p} \text{ and } \mathfrak{F}_{\mathfrak{P}/\mathfrak{p}} \in C\}$$

   has density $|C|/|G|$. In particular, this set is infinite.

2. Prove that Chebotarev's density theorem implies **Dirichlet's theorem on primes in arithmetic progressions**: *If $a \ge 1$ and $m \ge 2$ are relatively prime integers, then the set of prime numbers p satisfying $p \equiv a \pmod m$, considered as a subset of $\Omega_\mathbb{Q}$, has density $1/\varphi(m)$, where $\varphi(m) = \#(\mathbb{Z}/m)^*$. In particular, there are infinitely many prime numbers p such that $p \equiv a \pmod m$.*

3. Prove that if F/K is a finite extension in which almost all $\mathfrak{p} \in \Omega_K$ splits completely, then $F = K$.

   (*For this question, you are allowed to use Exercise* A.6.4 in [Hu].)

4. Let $f \in \mathcal{O}_K[t]$ be a monic polynomial. Prove that the following assertions are equivalent:

   (a) f splits completely into linear factors over K, i.e., f is a product of linear factors in $K[t]$.

   (b) For every maximal ideal $\mathfrak{p}$ of $\mathcal{O}_K$ with residue field $\kappa(\mathfrak{p})$, the canonical reduction $\bar{f}$ of f mod $\mathfrak{p}$ splits completely into linear factors over the residue field $\kappa(\mathfrak{p})$.

   (c) For almost all maximal ideals $\mathfrak{p}$ of $\mathcal{O}_K$, the canonical reduction $\bar{f}$ of f mod $\mathfrak{p}$ splits completely into linear factors over the residue field $\kappa(\mathfrak{p})$.

5. Prove the **global square theorem**: *An element $c \in K^*$ is a square in K if and only if c is a square in $K_\mathfrak{p}$ for almost all $\mathfrak{p} \in \Omega_K$.*

   Fix an element $\alpha \in K^*$ and put

   $$\begin{aligned} \mathrm{Nm}(\alpha) &:= \{z \in K^* \mid z \text{ is a norm from the extension } K(\sqrt{\alpha})/K\}\,, \\ \mathrm{Nm}_\mathfrak{p}(\alpha) &:= \{z \in K_\mathfrak{p}^* \mid z \text{ is a norm from the extension } K_\mathfrak{p}(\sqrt{\alpha})/K_\mathfrak{p}\} \quad \text{for all } \mathfrak{p} \in \Omega_K\,. \end{aligned}$$

6. Prove that for each $\mathfrak{p} \in \Omega_K$, the natural inclusion $\iota_\mathfrak{p} : K^* \hookrightarrow K_\mathfrak{p}^*$ sends $\mathrm{Nm}(\alpha)$ into $\mathrm{Nm}_\mathfrak{p}(\alpha)$, and that for any $b \in K^*$, we have $\iota_\mathfrak{p}(b) \in \mathrm{Nm}_\mathfrak{p}(\alpha)$ for almost all $\mathfrak{p}$.

   Therefore, we have an induced map

   $$\iota : \frac{K^*}{\mathrm{Nm}(\alpha)} \longrightarrow \bigoplus_\mathfrak{p} \frac{K_\mathfrak{p}^*}{\mathrm{Nm}_\mathfrak{p}(\alpha)}\,; \quad b \longmapsto (\iota_\mathfrak{p}(b))\,.$$

7. For each $\mathfrak{p} \in \Omega_K$, let

   $$(\cdot\,,\cdot)_\mathfrak{p} : K_\mathfrak{p}^* \times K_\mathfrak{p}^* \longrightarrow \{\pm 1\}$$

   denote the Hilbert symbol $(\cdot\,,\cdot)_{2,\mathfrak{p}}$ defined as in [Hu] (4.2.13) (for $n = 2$). Prove that the map

   $$\phi : \bigoplus_\mathfrak{p} \frac{K_\mathfrak{p}^*}{\mathrm{Nm}_\mathfrak{p}(\alpha)} \longrightarrow \{\pm 1\}\,; \quad (b_\mathfrak{p}) \longmapsto \prod_\mathfrak{p} \big(\alpha\,,\, b_\mathfrak{p}\big)_\mathfrak{p}$$

   is well defined and that ϕ is surjective if and only if α is not a square in K.

Exercise B.2.8. With notation and hypotheses as in Exercise B.2.7, we now specialize to the case $K = \mathbb{Q}$. We identify Ω_K with $\mathcal{P} \cup \{\infty\}$, where $\mathcal{P}$ denotes the set of prime numbers. For each $p \in \mathcal{P}$, let v_p be the normalized p-adic valuation on $\mathbb{Q}_p$.

Let $\beta = (b_\mathfrak{p}) \in \prod_\mathfrak{p} K_\mathfrak{p}^*$ be such that

$$\big(\alpha,\, b_\mathfrak{p}\big)_\mathfrak{p} = 1 \text{ for almost all } \mathfrak{p} \text{ and } \prod_\mathfrak{p} \big(\alpha,\, b_\mathfrak{p}\big)_\mathfrak{p} = 1\,.$$

Consider the following subsets of Ω_K:

$$S := \{2, \infty\} \cup \{ \text{ odd primes } p \text{ such that } v_p(\alpha) \neq 0\};$$
$$T = T(\beta) := \{\mathfrak{p} \in \Omega_K \ : \ \left(\alpha\,,\, b_\mathfrak{p}\right)_\mathfrak{p} = -1\}.$$

(Note that S and T are both finite.)

1. First assume $S \cap T = \emptyset$ and put

$$A := \prod_{\ell \in T} \ell \quad \text{and} \quad M := 8 \prod_{\ell \in S \setminus \{2,\infty\}} \ell\,.$$

   (a) Show that there exists an odd prime number q such that $q \equiv A \pmod{M}$ and $q \notin S \cup T$.

   (b) Let q be such a prime and put $x = Aq$. Prove that $(\alpha,\, b_\mathfrak{p})_\mathfrak{p} = (\alpha,\, x)_\mathfrak{p}$ for all $\mathfrak{p} \in \Omega_K$.

2. Now consider the general case where $S \cap T$ may be nonempty.

   (a) Prove that there exists $y \in K^*$ such that $y^{-1} b_\mathfrak{p} \in K_\mathfrak{p}^{*2}$ for all $\mathfrak{p} \in S$.

   (b) Show that there exists an element $x \in K^*$ such that $(\alpha,\, b_\mathfrak{p})_\mathfrak{p} = (\alpha,\, x)_\mathfrak{p}$ for all $\mathfrak{p} \in \Omega_K$.
   (*Hint: Letting y be as above and putting $\beta' := y\beta = (yb_\mathfrak{p})$, consider $T(\beta')$ instead of $T = T(\beta)$.*)

3. Prove that the sequence

$$\frac{K^*}{\mathrm{Nm}(\alpha)} \xrightarrow{\ \iota\ } \bigoplus_\mathfrak{p} \frac{K_\mathfrak{p}^*}{\mathrm{Nm}_\mathfrak{p}(\alpha)} \xrightarrow{\ \phi\ } \{\pm 1\}$$

   is exact.

Remark: In fact, for any number field K the map ι in Exercise B.2.7 is injective and the sequence in Exercise B.2.8 (3) is exact. This follows from more general theorems well known as the **Hasse norm principle** and the **Albert–Brauer–Hasse–Noether theorem** (which are important applications of global class field theory).

References

[AT09] Emil Artin and John Tate. *Class field theory.* AMS Chelsea Publishing, Providence, RI, 2009. Reprinted with corrections from the 1967 original.

[Bak66] A. Baker. Linear forms in the logarithms of algebraic numbers. I, II, III. *Mathematika*, 13:204–216; ibid. 14 (1967), 102–107; ibid. 14 (1967), 220–228, 1966.

[Bou06] N. Bourbaki. *Éléments de mathématique. Algèbre commutative. Chapitres 5 à 7. [Commutative algebra. Chapters 5–7]*. Springer, Berlin, 2006. Reprint of the 1975 original.

[CF67] J.W.S Cassels and A. Fröhlich. *Algebraic number theory*. Proceedings of an instructional conference organized by the London Mathematical Society (a NATO Advanced Study Institute) with the support of the Inter national Mathematical Union. Edited by J. W. S. Cassels and A. Fröhlich. Academic Press, London; Thompson Book Co., Inc., Washington, D.C., 1967.

[Che36] C. Chevalley. Généralisation de la théorie du corps de classes pour les extensions infinies. *J. Math. Pures Appl. (9)*, 15:359–371, 1936.

[Che40] C. Chevalley. La théorie du corps de classes. *Ann. of Math. (2)*, 41:394–418, 1940.

[Che51] Claude Chevalley. *Introduction to the Theory of Algebraic Functions of One Variable*. Mathematical Surveys, No. VI. American Mathematical Society, New York, N. Y., 1951.

[Con] Keith Conrad. History of class field theory. notes available at https://kconrad.math.uconn.edu/blurbs/gradnumthy/cfthistory.pdf.

[Del74] Pierre Deligne. La conjecture de Weil. I. *Inst. Hautes Études Sci. Publ. Math.*, (43):273–307, 1974.

[EP05] Antonio J. Engler and Alexander Prestel. *Valued fields*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2005.

[Har20] David Harari. *Galois cohomology and class field theory*. Universitext. Springer, Cham, [2020] ©2020. Translated from the 2017 French original by Andrei Yafaev.

[Has67] Helmut Hasse. History of class field theory. In *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, pages 266–279. Thompson, Washington, D.C., 1967.

[Hu21] Yong Hu. Basic number theory. SUSTech lecture notes, 2021.

[Hun80] Thomas W. Hungerford. *Algebra*, volume 73 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1980. Reprint of the 1974 original.

[HV49] L. K. Hua and H. S. Vandiver. Characters over certain types of rings with applications to the theory of equations in a finite field. *Proc. Nat. Acad. Sci. U.S.A.*, 35:94–99, 1949.

[IR90] Kenneth Ireland and Michael Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.

[Iwa86] Kenkichi Iwasawa. *Local class field theory*. Oxford Science Publications. The Clarendon Press Oxford University Press, New York, 1986. Oxford Mathematical Monographs.

[Jaf56] Paul Jaffard. Anneaux d'adèles d'après Iwasawa. In *Séminaire Bourbaki, Vol. 3*, pages Exp. No. 103, 23–33. Soc. Math. France, Paris, 1956.

[Lan02] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[Mar18] Daniel A. Marcus. *Number fields*. Universitext. Springer, Cham, 2018. Second edition of [MR0457396], With a foreword by Barry Mazur.

[Mil20] J.S. Milne. Class field theory (v4.03), 2020. Available at www.jmilne.org/math/.

[Mor96] Patrick Morandi. *Field and Galois theory*, volume 167 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1996.

[Mun00] James R. Munkres. *Topology*. Prentice Hall, Inc., Upper Saddle River, NJ, 2000. Second edition of [MR0464128].

[Neu86] Jürgen Neukirch. *Class field theory*, volume 280 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1986.

[Neu99] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[NSW00] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 2000.

[O'M00] O. Timothy O'Meara. *Introduction to quadratic forms*. Classics in Mathematics. Springer-Verlag, Berlin, 2000. Reprint of the 1973 edition.

[Roq01] Peter Roquette. Class field theory in characteristic p, its origin and development. In *Class field theory—its centenary and prospect (Tokyo, 1998)*, volume 30 of *Adv. Stud. Pure Math.*, pages 549–631. Math. Soc. Japan, Tokyo, 2001.

[Ros11] Kenneth H. Rosen. *Elementary number theory and its applications*. Addison-Wesley, Reading, MA, sixth edition, 2011.

[RV99] Dinakar Ramakrishnan and Robert J. Valenza. *Fourier analysis on number fields*, volume 186 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1999.

[Ser79] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1979. Translated from the French by Marvin Jay Greenberg.

[Sta67] H. M. Stark. A complete determination of the complex quadratic fields of class-number one. *Michigan Math. J.*, 14:1–27, 1967.

[Tat50] John Torrence Tate, Jr. *Fourier analysis in number fields and Hecke's Zeta-functions*. ProQuest LLC, Ann Arbor, MI, 1950. Thesis (Ph.D.)–Princeton University.

[Tat67] J. T. Tate. Fourier analysis in number fields and Hecke's Zeta-functions. In *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, pages 305–347. Thompson, Washington, D.C., 1967.

[TW15] Jean-Pierre Tignol and Adrian R. Wadsworth. *Value functions on simple algebras, and associated graded rings*. Springer Monographs in Mathematics. Springer, Cham, 2015.

[Was97] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.

[Wei38] A. Weil. Zur algebraischen Theorie der algebraischen Funktionen. (Aus einem Brief an H. Hasse.). *J. Reine Angew. Math.*, 179:129–133, 1938.

[Wei49] André Weil. Numbers of solutions of equations in finite fields. *Bull. Amer. Math. Soc.*, 55:497–508, 1949.