Local Class Field Theory

Richard Crew

April 6, 2019

Contents

Chapter 1

Nonarchimedean Fields

Without explicit notice to the contrary, all rings have an identity and all homomorphisms are unitary, i.e. send the identity to the identity.

1.1 Absolute values

1.1.1 Definitions. Let R be a ring (not necessarily commutative). An *absolute value* on R is a map $R \to \mathbb{R}^{\geq 0}$, written $x \mapsto |x|$, with the following properties:

$$|x| = 0 \text{ if and only if } x = 0. \tag{1.1.1.1}$$

$$|xy| = |x||y|. \tag{1.1.1.2}$$

$$|x + y| \leq |x| + |y|. \tag{1.1.1.3}$$

We are mostly interested in the case when R is a field or a division ring, but the general notion will be useful at times.

We will see numerous examples in section 1.1.4 and elsewhere. For now we make the following elementary observations:

- 1.1.1.2 implies $|1| = |-1| = 1$, so that $|-x| = |x|$ for all $x \in R$. Then 1.1.1.3 is equivalent to the *triangle inequality:* $|x - y| \leq |x| + |y|$.
- If $x \in R^\times$ then 1.1.1.1 and 1.1.1.2 imply $|x^{-1}| = |x|^{-1}$.
- If R is a division ring and $|\quad|$ is map satisfying 1.1.1.2, then 1.1.1.1 is equivalent the condition that $|\quad|$ is not identically zero.
- An absolute value on R defines an absolute value on the opposite ring R^{op}.
- If $R' \subseteq R$ is a subring, an absolute value on R induces one on R'.
- The image $|R^\times|$ of the unit group is a subgroup of $\mathbb{R}^{>0}$, the *value group* of the absolute value. We will denote it by Γ_R.

Most of the absolute values in this book have the property of being *nonarchimedan*, which means that condition 1.1.1.3 is replaced by the following stronger condition:

$$|x+y| \le \max(|x|,|y|) \quad \text{for all } x,\, y \in R. \tag{1.1.1.4}$$

An absolute value that is not nonarchimedean is called *archimedean*.

If $|\quad|$ is nonarchimedean, the triangle inequality says that $|x-y| \le \max|x|,|y|$. From this we deduce the following sharper form of 1.1.1.3:

$$|x| \ne |y| \Rightarrow |x+y| = \max|x|,|y|. \tag{1.1.1.5}$$

Suppose for example $|x| < |y|$; if $|x+y| < |y|$ then $|y| = |x+y-x| \le \max(|x+y|,|x|) < |y|$, a contradiction. We could rephrase 1.1.1.5 by saying that every triangle is isosceles.

For $a \in R$ and $r \ge 0$ the sets

$$B(a,r) = \{x \in R \,|\, |x-a| \le r\} \tag{1.1.1.6}$$

$$B(a,r^-) = \{x \in R \,|\, |x-a| < r\} \tag{1.1.1.7}$$

$$\tag{1.1.1.8}$$

are the *closed* and *open ball of radius r about a* respectively. Another consequence of 1.1.1.5 is that if two balls are not disjoint then one is contained in the other.

1.1.1.1 Lemma *Suppose K is a division ring. A function $|\quad| : K \to \mathbb{R}$ satisfying 1.1.1.1 and 1.1.1.2 satisfies 1.1.1.4 if and only if $|x| \le 1$ implies $|x+1| \le 1$ for all $x \in K$.*

Proof. The condition is clearly necessary. If $|x| \le |y|$ and $y \ne 0$ then $|xy^{-1}| \le 1$, so that $|xy^{-1}+1| \le 1$ and thus $|x+y| \le |y| = \max(|x|,|y|)$. ■

1.1.2 The integer ring and its ideals. If $|\quad|$ is a nonarchimedean valuation on R, the set

$$\mathcal{O}_R = \{x \in R \,|\, |x| \le 1\}$$

is a subring of R; if R is a field it is an integral domain. In any case it is called the *integer ring* of the absolute value. If K is a division ring, the unit group of $\mathcal{O}_K$ is

$$\mathcal{O}_K^\times = \{x \in K \,|\, |x| = 1\}. \tag{1.1.2.1}$$

For example if $x \in K$ satisfies $|x| < 1$ then $1+x \in \mathcal{O}_R^\times$. For any ring R the sets

$$\begin{aligned} I_r &= \{x \in R \,|\, |x| \le r\} \\ I_{<r} &= \{x \in R \,|\, |x| < r\} \end{aligned} \tag{1.1.2.2}$$

are 2-sided ideals of $\mathcal{O}_R$.

1.1.2.1 Proposition *Suppose K is a division ring with a nonarchimedean absolute value and $S \subseteq \mathcal{O}_K$ is a nonempty subset. If*

$$r = \sup_{x \in S} |x|. \tag{1.1.2.3}$$

the left (resp. right) ideal of $\mathcal{O}_K$ generated by S is I_r if there is an $x \in S$ such that $|x| = r$, and $I_{<r}$ otherwise.

Proof. It suffices to treat the case of left ideals, and in either case the inclusion $I \subseteq I_r$ is clear. Suppose first there is $x \in I$ with $|x| = r$; then $y \in I_r$ implies $|y| \leq |x|$, so that $|yx^{-1}| \leq 1$, $yx^{-1} \in \mathcal{O}_K$ and finally $y = (y/x)x \in I$.

If there is no $x \in I$ such that $|x| = r$ we must have $I \subseteq I_{<r}$, and we can find a sequence of $x_n \in I$ with $|x_n| \to r$. For any $y \in I_{<r}$ there is an n such that $|y| \leq |x_n|$ and as before we have $y \subseteq x_n \mathcal{O}_K \subseteq I$ and consequently $I_{<r} \subseteq I$. ■

1.1.2.2 Corollary *Suppose K is a division ring with a nonarchimedean absolute value. Then all left and right ideals of $\mathcal{O}_K$ are 2-sided, and the set of ideals of $\mathcal{O}_K$ are totally ordered under inclusion. In particular $\mathcal{O}_K$ is a local ring with maximal ideal $I_{<1}$.*

The ring $\mathcal{O}_K$ is not necessarily noetherian, but it is "almost" a PID:

1.1.2.3 Corollary *A finitely generated ideal in $\mathcal{O}_K$ is principal.*

Proof. In fact if S is finite, the maximum in 1.1.2.1 and then $I = (x)$ for any x such that $|x| = r$. ■

A commutative ring with this property of proposition 1.1.2.3 is called a *Bezout ring.*

Suppose K is a division ring and $\mathfrak{m} = I_{<1}$ is the maximal ideal of $\mathcal{O}_K$. The quotient $\mathcal{O}_K/\mathfrak{m} = k$ is also a division ring and is called the *residue field* of $\mathcal{O}_K$, or of K (it might be a skew field if K is). The reduction map $\mathcal{O}_K \to k$ will generally be written $x \mapsto \bar{x}$, and we will use the same notation for all derived homomorphisms, such as the reduction maps $\mathcal{O}_K[X] \to k[X]$, $\mathcal{O}_K[[X]] \to k[[X]]$ etc.

Suppose now K is a field with a nonarchimdean valuation. We say that K is *equicharacteristic* if K and its residue field k have the same characteristic (note that the notion of characteristic has an obvious meaning for a division ring). If they have different characteristics then K must have characteristic 0 and k characteristic $p > 0$. In this case we say that K has *mixed characteristic.* One says "equicharacteristic p" or "mixed characteristic p" to indicate the characteristic.

If K is a division ring and $a \in K^\times$ then $|axa^{-1}| = |x|$ for all $x \in K$. Therefore the inner automorphism induced by a induces automorphisms of the integer ring $\mathcal{O}_K$ and the residue field k. We denote by $\mathrm{ad}_k(a)$ the automorphism of k induced in this way by $a \in K$. If the residue field k is commutative, $\mathrm{ad}_k(u)$

is trivial for any $u \in \mathcal{O}_K^\times$, and it follows that $\mathrm{ad}_k(a)$ depends only on $|a|$. Clearly $\mathrm{ad}_k(ab) = \mathrm{ad}_k(a)\mathrm{ad}_k(b)$, so we have defined a homomorphism

$$\mathrm{inv}_K : \Gamma_K \to \mathrm{Aut}(k) \tag{1.1.2.4}$$

for any division ring K whose residue field k is commutative. We could call this map the "invariant map" but this term is already used in a different (but closely related sense) for division algebras over local fields.

1.1.3 Valuations. A nonarchimedean absolute value on a ring R can be given by the function $v : R \to \mathbb{R} \cup \{\infty\}$ defined by

$$v(x) = \begin{cases} -\log x & x \neq 0 \\ \infty & x = 0 \end{cases} \tag{1.1.3.1}$$

where the logarithm can have any base greater than one. The function $v(x)$ clearly satisfies the conditions

$$v(x) = \infty \text{ if and only if } x = 0 \tag{1.1.3.2}$$
$$v(xy) = v(x) + v(y) \tag{1.1.3.3}$$
$$v(x+y) \geq v(x),\ v(y) \tag{1.1.3.4}$$

and conversely any function $R \to \mathbb{R} \cup \{\infty\}$ satisfying the conditions 1.1.3.2-1.1.3.4 defines an valuation by taking $|x| = a^{-v(x)}$ for any $a > 1$. A function $R \to \mathbb{R} \cup \{\infty\}$ satisfying 1.1.3.2-1.1.3.4 is called a *valuation*. A valuation is *trivial* if this is the case for the associated absolute value, or in other words if $v(x) = 0$ for all $x \neq 0$. The subset $v(R^\times) \subseteq \mathbb{R}$ is the *value group* of the valuation; it is isomorphic to the value group of the associated absolute value. We will use the same notation Γ_R for this group.

If $I = (x) \subseteq \mathcal{O}_K$ is a principal ideal we will use the notation $v(I) = v(x)$ and speak of $v(I)$ as the valuation of I. In fact if $(x) = (y)$ then $y = ux$ for some $u \in \mathcal{O}_K^\times$, and thus $v(x) = v(y)$.

1.1.3.1 Remark In the definition the additive group $\mathbb{R}$ can be replaced by any totally ordered group, and functions of this sort are also called valuations. With that definition what we are calling valuations are called rank one valuations. We will not use this more general notion.

We leave to the reader the proof of the following easy

1.1.3.2 Lemma *A subgroup of the additive group of $\mathbb{R}$ is either infinite cyclic or dense.*

If R is a ring with valuation v, we say that the valuation v is *discrete* if the value group $\Gamma_R \subset \mathbb{R}$ is infinite cyclic, and *nondiscrete* otherwise. If v is a discrete valuation on R an element $\pi \in \mathcal{O}_K$ such that $v(\pi)$ generates $v(R^\times)$ is called a *uniformizer* of $\mathcal{O}_R$ (or of R). If R is a division ring, any two uniformizers

differ by a unit factor on the left or right. If K is a division ring and π is a uniformizer, it follows from proposition 1.1.2.1 that the ideals of $\mathcal{O}_K$ are (π^n) for all $n \geq 0$.

A valuation v on K is *normalized* if $v(\pi) = 1$ for one (or equivalently, any) uniformizer π. Any discrete valuation can be *normalized* by dividing it by $v(\pi)$ for any uniformizer π. When a valuation v of K is given we denote by v_K the unique normalized valuation that is a multiple of v.

It is clear that if K is a field with a discrete valuation, $\mathcal{O}_K$ is a discrete valuation ring and is in particular noetherian. Similarly if K is a division ring, $\mathcal{O}_K$ is (left and right) noetherian; it is as it were a "noncommutative discrete valuation ring." In general, if v is a nondiscrete valuation on a ring R then $\mathcal{O}_R$ is not noetherian. In fact in this case 0 must be an accumulation point of $v(K^\times)$; then 1 is an accumulation point of the corresponding absolute value, and the set of $I_{<r}$ for all $r \leq 1$ is an infinite ascending chain.

1.1.4 Examples. Suppose K is a division ring with an absolute value. The minimal possibility for the value group Γ_R is the trivial group $1 \subset \mathbb{R}^{>0}$, so that

$$|x| = \begin{cases} 1 & x \neq 0 \\ 0 & x = 0 \end{cases}$$

and conversely the above formula defines a nonarchimedean absolute value on K. It is called the *trivial absolute value.* Any absolute value on a finite field is trivial.

The field $\mathbb{R}$ has an archimedean absolute given by $|x| = \max(x, -x)$. Similarly the complex norm is an archimedean absolute value on the field of complex numbers $\mathbb{C}$, and the quaternionic norm is an archimedean absolute value on the field $\mathbb{H}$ of Hamilton quaternions. The Gelfand-Tornheim theorem asserts that any (commutative) field with an archimedean absolute value is isomorphic to a subfield of $\mathbb{C}$ (and of course any such field has an archimedean absolute value). In particular, any field with an archimedean absolute value has cardinality at most that of the continuum.

If R is a discrete valuation ring with maximal ideal $\mathfrak{p}$ and fraction field K, the function $v_\mathfrak{p} : K \to \mathbb{N} \cup \{\infty\}$ defined by

$$v_\mathfrak{p}(x) = \text{the largest } n \in \mathbb{Z} \text{ such that } x \in \mathfrak{p}^n \tag{1.1.4.1}$$

defines a normalized discrete valuation on K such that $\mathcal{O}_K = R$. More generally if R is a Dedekind domain with fraction field K, the formula 1.1.4.1 defines a normalized discrete valuation $v_\mathfrak{p}$ on the localization $R_\mathfrak{p}$ of R at $\mathfrak{p}$ for any maximal ideal $\mathfrak{p} \subset R$, and thus a normalized valuation $v_\mathfrak{p}$ on K itself. The integer ring of $v_\mathfrak{p}$ is $R_\mathfrak{p}$.

A particularly important special case is when K is a number field, i.e. a finite extension of $\mathbb{Q}$, and R is the integer ring of K, i.e. the integral closure of $\mathbb{Z}$ in K. When $R = \mathbb{Z}$, $K = \mathbb{Q}$ the valuation associated to $\mathfrak{p} = (p)$ is denoted by v_p and can be computed as follows: if $x = p^r(a/b)$ with a and b prime to

p, then $v_p(x) = p^{-r}$. The integer ring of v_p is the localization $\mathbb{Z}_{(p)}$. The*p-adic absolute value* of $\mathbb{Q}$ is the absolute value $|\ |_p$ associated to v_p.

A number field K also has archimedean absolute values which arise as follows: the tensor product $\mathbb{R} \otimes_{\mathbb{Q}} K$ is isomorphic to a direct sum of copies of $\mathbb{R}$ and $\mathbb{C}$, whence a set of embeddings of K into $\mathbb{C}$. The standard archimedean absolute value of $\mathbb{C}$ then induces archimedean absolute values on K.

If k is any field and and K is a finite extension of the field $k(T)$ of rational functions in one variable, the integral closure R of the polynomial ring $k[T]$ in K is a Dedekind domain (this is easy if k has characteristic 0, and a more difficult theorem of Zariski in general). The above remarks then apply to K, so that fields of algebraic functions have a large supply of discrete valuations.

Finally let k be any field and set $K = k((T))$, the field of Laurent series with coefficients in k. For $f = \sum_{n \gg -\infty} a_n T^n \in K$,

$$v(f) = \min\{n | a_n \neq 0\}.$$

defines a normalized discrete valuation with integer ring $k[[T]]$ and residue field k; it is called the *T-adic valuation* of K. This shows that any field can be residue field of a discretely valued field.

Fields with nondiscrete valuations can be constructed by taking infinite algebraic extensions of the above examples, as we shall see later.

1.1.5 The topology definded by an absolute value. The axioms 1.1.1.1 and 1.1.1.3 say that an absolute value on R is a *metric*, whence a Hausdorff topology on R. A basis of neighborhoods of $a \in K$ is given by sets of open balls $B(a, r^-)$ for all $r > 0$. The axioms 1.1.1.2 and 1.1.1.3 imply that addition and multiplication are continuous. When R is a field K, division is also continuous since $|x - x_0| < |x_0|$ implies $|x| = |x_0|$ and therefore

$$\left|\frac{1}{x} - \frac{1}{x_0}\right| = \frac{|x - x_0|}{|xx_0|} = \frac{|x - x_0|}{|x_0|^2}.$$

The calculation in fact shows that inversion is uniformly continuous on any set of the form $r \leq |x|$ for $r > 0$. Thus K is a topological field for this topology, and in particular its additive and multiplicative groups are topological groups.

By construction the metric is continuouus for the topology it defines. It follows that the ideals $I_{<r}$ are open and the I_r are closed. However any open subgroup of a topological group is also closed, so $I_{<r}$ is closed. Furthermore I_r is open since it as a union of open sets

$$I_r = \bigcup_{|a| \leq r} (a + I_{<r}).$$

Since any closed ball is a disjoint union of closed bass of smaller radius, K is totally disconnected.

Two absolute values $|\quad|_1$, $|\quad|_2$ are *equivalent* if they define the same topology on K. For example the absolute values $|\quad|_\infty$ and $|\quad|_p$ on $\mathbb{Q}$ are inequivalent

for all p: in fact $|p^n|_\infty \to \infty$ as $n \to \infty$, while $|p^n|_p \to 0$. One can show in the same way that $|\quad|_p$ and $|\quad|_q$ are inequivalent for distinct primes p, q.

A theorem of Ostrowski shows that any absolute value on $\mathbb{Q}$ is equivalent to $|\quad|_\infty$ or to $|\quad|_p$ for some prime p. We will not prove this here. More generally, if R is the integer ring of a number field K then any absolute value on K is equivalent to one of the $v_\mathfrak{p}$ constructed in section §1.1.4, or else one of the archimedean absolute values arising from the decomposition $\mathbb{R}\otimes_\mathbb{Q} K \simeq \mathbb{R}^{r_1}\oplus\mathbb{C}^{r_2}$.

1.1.5.1 Theorem *Let K be a division ring and suppose $|\quad|_1$, $|\quad|_2$ are nonarchimedean absolute values on K. The following are equivalent:*

(i). $|\quad|_1$ *and* $|\quad|_2$ *are equivalent.*

(ii). $|x|_1 < 1$ *(resp.* $|x|_1 = 1$, $|x|_1 > 1$*) if and only if* $|x|_2 < 1$ *(resp.* $|x|_2 = 1$, $|x|_2 > 1$*).*

(iii). $|x|_1 = |x|_2^\alpha$ *for some* $\alpha > 0$.

Proof. (i) implies (ii): The inequality $|x|_1 < 1$ implies that $|x|_1^n \to 0$ as $n \to \infty$ and thus $x^n \to 0$ for the topology defined by $|\quad|_1$. But $|x|_2 \geq 1$ would imply that $\{x^n\}_{n>0}$ does not converge to zero if $|\quad|_2$ defines the same topology as $|\quad|_1$. Therefore $|x|_2 < 1$.

Since (i) is symmetric in the two absolute values, we have shown that $|x|_1 < 1$ if and only if $|x|_2 < 1$. If $|x|_1 > 1$ then $x \neq 0$ and $|x^{-1}|_1 < 1$, and from the preceding argument we conclude that $|x|_1 > 1$ if and only if $|x|_2 > 1$. By elimination, $|x|_1 = 1$ if and only if $|x|_2 = 1$.

(iii) clearly implies (i).

(ii) implies (iii): It suffices to show that

$$\frac{\log|a|_1}{\log|a|_2} = \frac{\log|b|_1}{\log|b|_2}$$

for a, $b \in K$ such that both fractions are defined and nonzero. Equivalently, we must show that

$$\frac{\log|a|_1}{\log|b|_1} = \frac{\log|a|_2}{\log|b|_2}$$

for all such a, b. If not we may assume that the left hand side is the smaller one and that

$$\frac{\log|a|_1}{\log|b|_1} < \frac{m}{n} < \frac{\log|a|_2}{\log|b|_2}$$

for some a, $b \in K$ and integers m, n. By (ii) we know $\log|b|_1$ and $\log|b|_2$ have the same sign, and we may further assume n has the same sign as $\log|b|_1$ and $\log|b|_2$. Then $n\log|b|_1$ and $n\log|b|_2$ are positive and these inequalities imply

$$|a^n b^{-m}|_1 < 1, \qquad |a^n b^{-m}|_2 > 1$$

which contradicts (ii). ■

We say that two valuations of K are equivalent if the corresponding absolute values are. From the theorem and 1.1.3.1 we see that two valuations v_1, v_2 are equivalent if and only if $v_1 = \alpha v_2$ for some $\alpha > 0$.

1.1.6 Completion. Suppose K is a commutative ring with an absolute value. Since addition, multiplication and inversion are all continuous, the extend to the completion $\hat{K}$ of K for the metric defined by the absolute value. The absolute value likewise extends to $\hat{K}$ since it too is continuous. The closure $\hat{\mathcal{O}}_K$ of the integer ring $\mathcal{O}_K \subset K$ is the integer ring of $\hat{K}$. For any $r \leq 1$ the natural maps $\mathcal{O}_K/I_r \to \hat{\mathcal{O}}_K/\hat{I}_r$ and $\mathcal{O}_K/I_{<r} \to \hat{\mathcal{O}}_K/\hat{I}_{<r}$ are isomorphisms. In particular $\mathcal{O}_K$ and $\hat{\mathcal{O}}_K$ have the same residue field.

1.1.6.1 Proposition *If R is a discretely valued commutative, the maps*

$$f_n : \hat{\mathcal{O}}_R \to \hat{\mathcal{O}}_R/\hat{\mathfrak{m}}^n \simeq \mathcal{O}_R/\mathfrak{m}^n$$

induce a topological isomorphism

$$\hat{\mathcal{O}}_R \simeq \varprojlim_n \mathcal{O}_R/\mathfrak{m}^n. \tag{1.1.6.1}$$

where each $\mathcal{O}_R/\mathfrak{m}^n$ has the discrete topology.

Proof. It suffices to show that the f_n satisfy the universal property of the inverse limit. Suppose in fact that S is a ring and $g_n : S \to \mathcal{O}_R/\mathfrak{m}^n$ are a family of homomorphisms compatible with the projection maps. For any $x \in S$ and $n > 0$ pick $x_n \in \mathcal{O}_R$ such that the image of x_n in $\mathcal{O}_R/\mathfrak{m}^n$ is $g_n(x)$. Then $(x_n)_{n>0}$ is a Cauchy sequence and we define $g(x) = \lim_n x_n \in \hat{\mathcal{O}}_R$. It is easily checked that g is a ring homomorphism and that g_n is the composition of g with the projections. ■

A *nonarchimedean ring* is a (not necessarily commutative) ring R with a nonarchimedean absolute value for which R is complete. Examples of noncommutative nonarchimedean division rings will be constructed later. For nonarchimedean fields, we have the following important examples:

For any prime p the *field of p-adic numbers* is the completion $\mathbb{Q}_p$ of $\mathbb{Q}$ for the p-adic absolute value $|\quad|_p$ on $\mathbb{Q}$. The closure of of the valuation ring $\mathbb{Z}_{(p)}$ the integer ring of $\mathbb{Q}_p$; it is the *ring of p-adic integers.*

For any field k the Laurent series field $K = k((T))$ is complete with respect to its T-adic valuation, and is thus a nonarchimedean field.

1.1.6.2 Proposition *Any nonarchimedean field of mixed characteristic $p > 0$ is an extension of $\mathbb{Q}_p$.*

Proof. If K is any such field then $p \in \mathfrak{m}$ or equivalently $|p| < 1$. Then any integer a prime to p is a unit in $\mathcal{O}_K$, for if $ra + sp = 1$, $ra = 1 - sp \in \mathcal{O}_K^\times$ and then $a \in \mathcal{O}_K^\times$ as well. Now any $x \in \mathbb{Q}$ can be written $x = p^r(a/b)$ with integers r, a, b and a, b relatively prime to p. Then $|x| = |p|^{-r}$ and the absolute value induced on $\mathbb{Q}$ is equivalent to the p-adic one. The closure of $\mathbb{Q}$ in K is isomorphic to $\mathbb{Q}_p$ as a nonarchimedean field, so K is an extension of $\mathbb{Q}_p$. ■

Convergence questions in nonarchimedean rings are particularly simple.

1.1.6.3 Proposition *A sequence $\{a_n\}_{n\geq 0}$ in a nonarchimedean ring is a Cauchy sequence if and only if* $\lim_{n\to\infty} |a_n - a_{n+1}| = 0$.

Proof. The condition is evidently necessary. Suppose conversely that $\lim |a_n - a_{n+1}| = 0$ that $\epsilon > 0$ is given. Pick an integer N such that $|a_n - a_{n+1}| < \epsilon$ for all $n \geq N$; then $m > n \geq N$ implies

$$\begin{aligned} |a_n - a_m| &= |(a_n - a_{n+1}) + (a_{n+1} - a_{n+2}) + \cdots + (a_{m-1} - a_m)| \\ &\leq \max(|a_n - a_{n+1}|, |a_{n+1} - a_{n+2}|, \ldots, |a_{m-1} - a_m|) < \epsilon \end{aligned}$$

and thus $\{a_n\}_{n\geq 0}$ is a Cauchy sequence. ■

1.1.6.4 Corollary *A series $\sum_{n\geq 0} a_n$ in a nonarchimedean ring converges if and only if $|a_n| \to 0$ as $n \to \infty$.*

The well-known criteria for convergence of power series in the case of $K = \mathbb{R}$ or $\mathbb{C}$ hold for any power series with coefficients in a commutative nonarchimedean ring: if $f(X) = \sum_{n\geq 0} a_n X^n$ and $\limsup_{n\to\infty} \sqrt[n]{|a_n|} = L$ exists, set $R = L^{-1}$ if $L \neq 0$ and $R = \infty$ otherwise; then the series $f(x) = \sum_{n\geq 0} a_n x^n$ converges for any $x \in K$ such that $|x| < R$, and diverges if $|x| > R$.

For example if $f = \sum_n a_n X^n \in \mathcal{O}_K[[X]]$ then $f(x)$ is convergent for any x such that $|x| < 1$, since we must have $\limsup_n \sqrt[n]{|a_n x^n|} \leq |x| \limsup_n \sqrt[n]{|a_n|} \leq |x|$. If in fact $a_n \to 0$ as $n \to \infty$, $f(x)$ converges for $|x| \leq 1$ by corollary 1.1.6.4.

1.1.6.5 Binomial series. In any field K of characteristic zero we can define the binomial coefficient $\binom{a}{n}$ for $a \in K$ by the usual polynomial formula:

$$\binom{a}{n} = \frac{a(a-1)\cdots(a-n+1)}{n!}.$$

If $a \in \mathbb{Z}_p$ then $\binom{a}{n} \in \mathbb{Z}_p$ for all $n \geq 0$. In fact since $\binom{a}{n}$ is a polynomial it is a continuous function of a and $\binom{a}{n} \in \mathbb{Z}$ for any $a \in \mathbb{Z}$; then for $z \in \mathbb{Z}_p$ the value of $\binom{a}{n}$ must lie in the closure of $\mathbb{Z}$ in $\mathbb{Q}_p$, which is $\mathbb{Z}_p$.

We have seen that if K is nonarchimedean and of mixed characteristic $p > 0$, $\mathbb{Q}_p$ is canonically a subfield of K, so for any $a \in \mathbb{Z}_p$,

$$(1+X)^a = \sum_{n\geq 0} \binom{a}{n} X^n$$

defines an element of $K[[X]]$. The previous remarks show that it coverges in the open disk $|X| < 1$. The formula

$$(1+X)^a(1+X)^b = (1+X)^{a+b}$$

holds for all a, $b \in \mathbb{Z}_p$ since it clearly holds for a, $b \in \mathbb{Z}$ and on both sides the coefficient of X^n is a continuous function of a and b. Thus if $x \in K$ satisfies $|x| < 1$, $(1+x)^{1/n}$ is an nth root of $1+x$ for any integer prime to p.

1.1.6.6 Exponentials and logarithms. Still supposing that K is a mixed characteristic nonarchimedean field, the series

$$\log(1+x) = \sum_{n\geq 1}(-1)^{n+1}\frac{X^n}{n} \tag{1.1.6.2}$$

belongs to $K[[X]]$, and the series converges if we substitute for X any $x \in K$ satsifying $|x| < 1$. In fact if the valuation on K is normalized so that $v(p) = 1$, $v(n) \leq \log_p n$ and then since $v(x) > 0$,

$$v\left(\frac{x^n}{n}\right) \geq nv(x) - \log_p n \to \infty$$

as $n \to \infty$.

The exponential is similarly defined by

$$\exp(X) = \sum_{n\geq 0}\frac{X^n}{n!}$$

and the radius of convergence can be found with the root test: since

$$v\left(\sqrt[n]{\frac{1}{n!}}\right) = -\frac{1}{n}\frac{n-s(n)}{p-1} \to -\frac{1}{p-1}$$

we see that the series for $\exp(x)$ converges if $v(x) > 1/(p-1)$, and diverges if $v(x) < 1/(p-1)$.

1.1.7 Local Fields. A nonarchimedean field K is a *local field* if it is locally compact with its metric topology.

1.1.7.1 Lemma *If K is a locally compact division ring, the ideals I_r, $I_{<r}$ are compact. In particular $\mathcal{O}_K$ and its maximal ideal $\mathfrak{m}$ are compact.*

Proof. If U is a compact neighborhood of 0, $I_r \subseteq U$ for all sufficiently small $r > 0$, and any such I_r is compact since it is closed in U. Pick a nonzero $r \leq 1$ such that $I_r \subseteq U$; then $r = |x|$ for some $x \in K^\times$ and multiplication by x induces a homeomorphism $\mathcal{O}_K \xrightarrow{\sim} I_r$ and it follows that $\mathcal{O}_K$ is compact. Since the I_r and $I_{<r}$ for all $r \leq 1$ are closed they are compact as well. ■

1.1.7.2 Proposition *A nonarchimedean division algebra is locally compact if and only if its valuation is discrete and its residue field is finite.*

Proof. Let K be such an algebra. To prove the conditions are sufficient it is enough to show that $\mathcal{O}_K$ is a compact neighborhood of 0. It is certainly a neighborhood. Since the residue field is finite the quotient rings $\mathcal{O}_K/\mathfrak{m}^n$ are finite for all n. The topological isomorphism 1.1.6.1 then shows that $\mathcal{O}_K$ is compact.

Suppose now K is a local field and S is a set of representatives in $\mathcal{O}_K$ of the residue field k. Then

$$\mathcal{O}_K = \bigcup_{a \in S} (a + \mathfrak{m})$$

is a disjoint union and the $a + \mathfrak{m}$ are open. It follows that S, and therefore k is finite.

If the valuation of K is not discrete, some point $r \in |K^\times|$ must be an accumulation point. Then it is easy to check that there is then a sequence $\{r_n\}_{n \geq 0}$ with $0 < r_n < r$ such that $\lim_n r_n = r$. Then

$$I_{<r} = \bigcup_n I_{r_n}$$

is an open cover of the compact set $I_{<r}$ with no finite refinement, a contradiction. ■

In particular a nonarchimedean field is local field if and only if it is discretely valued with finite residue field.

1.1.8 Systems of representatives. Let K be a nonarchimedean field with residue field k. A *system of representatives* of k is a splitting $s : k \to \mathcal{O}_K$ of the canonical homomorphism $\mathcal{O}_K \to k$.

1.1.8.1 Proposition *Suppose K is a nonarchimedean field with a normalized discrete valuation v, valuation ring $\mathcal{O}_K$ and residue field $k = \mathcal{O}_K/\mathfrak{m}$. Choose a generator π of the maximal ideal $\mathfrak{m}$ and a section $s : k \to \mathcal{O}_K$ of the reduction map $V \to k$. Then every $x \in K$ has a unique expression in the form*

$$x = \sum_{n \geq N} s(a_n)\pi^n \tag{1.1.8.1}$$

where $N = v(x)$ and each $a_n \in k$ for all k.

Proof. If we replace x by $x\pi^{-N}$ with $N = v(x)$ we reduce to the case $v(x) = 0$, and in partcular $x \in \mathcal{O}_K$. We will choose the a_k successively so that for all $n \geq 0$,

$$x - \sum_{0 \leq k \leq n} a_k \pi^i \in \pi^{n+1}\mathcal{O}_K.$$

Recall that the reduction map $\mathcal{O}_K \to k$ is denoted $a \mapsto \bar{a}$, and let $a_0 = s(\bar{x})$, so that $x - a_0 \in \pi\mathcal{O}_K$. If $a_0, \ldots, a_n$ have been determined we set $x_n = \sum_{0 \leq k \leq k} a_k \pi^i$. Then $x - x_n = \pi^{n+1} b$ for some $b \in \mathcal{O}_K$ and we set $a_{n+1} = s(\bar{b})$. Since $b \equiv s(\bar{b}) \mod \pi$, $x - x_{n+1} \in \pi^{n+2}\mathcal{O}_K$. Clearly $|x - x_n| \to 0$ as $n \to \infty$, yielding 1.1.8.1. To show uniqueness it suffices to observe that if $x = \sum_{k \geq N} a_k \pi^k$ and $y = \sum_{k \geq N} b_k \pi^k$ are distinct series of this type we find the smallest k such that $a_k \neq b_k$. Since a_k and b_k are in the image of s we must have $a_k \not\equiv b_k \mod \pi$. Then $x - y \equiv a_k - b_k \mod \pi^k$, whence $x \neq y$. ■

1.1.8.2 Remark. In fact if $\pi_n \in L$ is any set of elements of L indexed by $\mathbb{Z}$ such that $v(\pi_n) = n$ for all k, then any $x \in L$ has a unique representation in the form

$$x = \sum_{n \geq N} s(a_n)\pi_n \tag{1.1.8.2}$$

as can be proven with the same argument as in the proposition.

For the field $\mathbb{Q}_p$ it is conventional to take $\pi = p$ and s so that its image is the set $0, 1, \ldots p-1$. For $x \in \mathbb{Z}$ the series 1.1.8.1 is the base p expansion of x, so we can think of the proposition as providing a sort of base p expansion for any element of $\mathbb{Q}_p$. For the nonarchimedean field $K = k((T)$ with its T-adic valuation, the a_k are just the Laurent series coefficients.

1.1.8.3 Corollary *A discretely valued nonarchimedean field with residue field k has cardinality $|k|^{\aleph_0}$.*

In particular the cardinality of $\mathbb{Q}_p$ or of $\mathbb{F}_q((T))$ is the that of the continuum. The corollary implies that there are nonarchidean fields of arbitrarily large cardinality. In fact if k is any field the Laurent series field $k((T))$ is an equicharacteristic nonarchimedean field of cardinality greater than $|k|$; when k has characteristic $p > 0$ we will see later how to construct mixed characteristic fields with this property.

1.1.9 Polynomials and their roots. If R is a quotient of $\mathcal{O}_K$ we will use the notation $x \mapsto \bar{x}$ for the reduction map $R \to k$ by $a \mapsto \bar{a}$, and similarly for $R[X] \to k[X]$.

1.1.9.1 Lemma *Suppose K is a nonarchimedean field with integer ring $\mathcal{O}_K$ and π is an element of the maximal ideal. If f, $g \in (\mathcal{O}_K/\pi\mathcal{O}_K)[X]$ are polynomials whose images in $k[X]$ generate the unit ideal, then f and g generate the unit ideal in $(\mathcal{O}_K/\pi\mathcal{O}_K)[X]$.*

Proof. Choose a, $b \in (\mathcal{O}_K/\pi\mathcal{O}_K)[X]$ such that $\bar{a}\bar{f} + \bar{b}\bar{g} = 1$. The ideal $I \subseteq \mathcal{O}_K/\pi\mathcal{O}_K$ generated by the coefficients of $af + bg - 1$ is contained in the maximal ideal and finitely generated; it is therefore nilpotent. If we set $M = (\mathcal{O}_K/\pi\mathcal{O}_K)[X]/(f, g)$ then $M/IM = 0$, and thus $M = 0$ by Nakayama's lemma. ■

1.1.9.2 Theorem *(Hensel's Lemma) Suppose K is a nonarchimedean field with integer ring $\mathcal{O}_K$ and residue field k. Let $f \in \mathcal{O}_K[X]$ be a polynomial such that $\bar{f} = g^0 h^0$ with relatively prime polynomials g^0, $h^0 \in k[X]$. Then there are polynomials g, $h \in \mathcal{O}_K[X]$ such that $f = gh$, $\bar{g} = g^0$, $\bar{h} = h^0$ and $\deg g = \deg g^0$. If g^0 is monic we can take g monic as well.*

Proof. The theorem reduces immediately to the case where g^0 is monic. Choose g', $h' \in \mathcal{O}_K[X]$ so that

$$\bar{g}' = g^0,\ \bar{h}' = h^0,\ \deg g' = \deg g^0,\ \deg h' \leq \deg f - \deg g^0$$

and g' is monic. Since g^0 and h^0 are relatively prime there are a, $b \in \mathcal{O}_K[X]$ such that $\bar{a}g^0 + \bar{b}h^0 = 1$. The ideal generated by the coefficients of $f - g'h'$ and $ag' + bh' - 1$ is finitely generated and thus principal, say (π). For $n \geq 0$ set $\mathcal{O}_n = \mathcal{O}_K/\pi^{n+1}\mathcal{O}_K$. We will show by induction that for all $n \geq 0$ there are g_n, h_n in $\mathcal{O}_n[X]$ such that

$$\begin{aligned} f &\mapsto g_n h_n \text{ under } \mathcal{O}_K[X] \to \mathcal{O}_n[X] \\ g_{n+1} &\mapsto g_n \text{ under } \mathcal{O}_{n+1}[X] \to \mathcal{O}_n[X] \\ h_{n+1} &\mapsto h_n \text{ under } \mathcal{O}_{n+1}[X] \to \mathcal{O}_n[X] \\ \deg g_n &= \deg g^0 \text{ and } g_n \text{ is monic if } g^0 \text{ is} \\ \deg h_n &\leq \deg f - \deg g^0. \end{aligned}$$

Then $g = \varprojlim_n g_n$ and $h = \varprojlim_n h_n$ satisfy the conditions of the theorem.

We take g_0 and h_0 to be the reductions of g' and h' modulo π. If g_n and h_n have been found, we look for g_{n+1}, h_{n+1} of the form

$$g_{n+1} = g'_n + \pi^n u, \qquad h_{n+1} = h'_n + \pi^n v$$

where g'_n, h'_n are elements of $\mathcal{O}_{n+1}[X]$ lifting g_n and h_n, u and v can be viewed as elements of $\mathcal{O}_0[X]$ and we need

$$\deg u < \deg g^0, \qquad \deg v \leq \deg f - \deg g^0$$

to insure that g_{n+1} and h_{n+1} satisfy the last two displayed conditions above. Since $n > 1$, $2n \geq n+2$ and the condition that f reduce to $g_{n+1}h_{n+1}$ in $\mathcal{O}_{n+1}[X]$ is

$$f \equiv g'_n h'_n + \pi^n(g'_n v + h'_n u) \mod \pi^{n+1}$$

since $2n \geq n+1$. If we set, with an obvious sense,

$$w = g'_n v + h'_n u = \frac{f - g'_n h'_n}{\pi^n} \in \mathcal{O}_0[X]$$

then we have to solve $g_0 v + h_0 u = w$ with $\deg u < \deg_0 = \deg g^0$. Since g^0 and h_{-1} generate the unit ideal of $k[X]$, g_0 and h_0, lemma 1.1.9.1 shows that they generate the unit ideal of $\mathcal{O}_0[X]$ and it follows that we can solve $g_0 v + h_0 u = w$ for u and v. Furthermore we are always free to change u and v by $u \mapsto u - qg_0$, $v \mapsto v + qh_0$ for any $q \in \mathcal{O}_0[X]$. Since g_0 is monic we can choose q so that $\deg u < \deg g_0$ by Euclidean division. Since $\deg h_0 \leq \deg f - \deg g_0$, $\deg h_0 u \leq \deg f$ and thus $\deg g_0 v \leq \deg w \leq \deg f$ as well and it follows that $\deg v \leq \deg f - \deg g_0 = \deg f - \deg g^0$ as required. ■

1.1.9.3 Corollary *With K as in the theorem, suppose $f \in \mathcal{O}_K[X]$ is such that $\bar{f}$ has a simple root $a \in k$. Then f has a root in $\mathcal{O}_K$ reducing to a modulo $\mathfrak{m}$.*

Proof. Apply the theorem to $\bar{f} = (X - a)h^0$ and observe that $X - a$ and h^0 are relatively prime. ■

1.1.9.4 Roots again. Consider for example the polynomial $f(X) = X^{p-1} - 1 \in \mathbb{Z}_p[X]$. Modulo p, f has $p-1$ distinct roots $1, 2, \ldots, p-1$. The corollary implies that $\mathbb{Z}_p$ has a full set of $(p-1)$-st roots of unity, whose reductions modulo p are the $p-1$ elements of $\mathbb{F}_p$. When $p > 2$ $\mathbb{Z}$ has no $(p-1)$-st roots of unity, which strongly suggests that completeness is essential here. There are nonetheless incomplete discrete valuation rings, in fact fairly important ones, for which the Hensel's lemma is true.

We saw in section 1.1.6.5 that if K is a nonarchimedean field of mixed characteristic $p >$ and $p \not| n$, any $x \in K$ such that $|x-1| < 1$ has an nth-root. Corollary 1.1.9.3 shows more generally that if $a \in \mathcal{O}_K^\times$ reduces to an n-power in $k^\times$ and $p \not| n$ then a has an nth root in $\mathcal{O}_K^\times$. In fact if $f(X) = X^n - a$ and $f(a_0) \equiv 0 \mod \mathfrak{m}$, a_0 is a simple root of f modulo $\mathfrak{m}$ and thus $X^n - a$ has a root in $\mathcal{O}_K$ (and thus necessarily in $\mathcal{O}_K^\times$.

1.1.9.5 Corollary *If $f \in K[X]$ is monic and irreducible then $f \in \mathcal{O}_K[X]$ if and only if its constant term is in $\mathcal{O}_K$.*

Proof. We need only show that the condition is sufficient. If we write $f = X^n + a_1 X^{n-1} + \cdots + a_n$ it suffices to show that $|a_i| \le |a_n|$ for all i. Set $a_0 = 1$ and choose i as large as possible so that $|a_i|$ is maximal. If $i = 0$ or $i = n$ we are done; otherwise $0 < i < n$ and dividing by a_i yields a irreducible $g \in \mathcal{O}_K[X]$ for which the coefficient of X^i is 1, and $a_j \in \mathfrak{m}$ for $j > i$. We may factor $\bar{g} = X^i h$, where h has nonzero constant term. Then X^i and h are relatively prime, and by Hensel's lemma g factors into polynomials of degree i and $n-i$, contradicting the irreducibility of g in $\mathcal{O}_K[X]$. ■

When the reduction of f has multiple roots Hensel's lemma is not applicable, but the following version of Newton's method can sometimes be used. We will need the following version of Taylor's theorem with remainder. Recall that for any commutative ring with identity R, differentiation can be defined purely formally on the polynomial ring $R[X]$ and and satisfies the usual identities (additivity, Leibnitz rule). Then for any $f(X) \in R[X]$ there is a polynomial $g(X,Y) \in R[X,Y]$ such that

$$f(X+Y) = f(X) + f'(X)Y + Y^2 g(X,Y). \tag{1.1.9.1}$$

It suffices to check this for mononials, in which case it follows from the binomial identity.

1.1.9.6 Theorem *(Newton's method) Suppose K is a nonarchimedean field with integer ring $\mathcal{O}_K$, $f \in \mathcal{O}_K[X]$, and $a_0 \in \mathcal{O}_K$ is such that*

$$c = \left| \frac{f(a_0)}{f'(a_0)^2} \right| < 1.$$

Then f has a root $a \in \mathcal{O}_K$ such that $|a - a_0| \le c$.

Proof. Define a sequence of $a_n \in K$ by

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

We will show that a_n converges to a root. In fact we will show by induction that

$$|a_n| \leq 1 \quad \text{and} \quad |f(a_n)/f'(a_n)^2| \leq c^{2^n} \tag{1.1.9.2}$$

for all $n \geq 0$. Then

$$|a_{n+1} - a_n| \leq c^{2^n} \tag{1.1.9.3}$$

which implies that the method converges rather rapidly, say $\lim_n a_n = a$. Since $|a_n| \leq 1$ for all n we have $|a| \leq 1$, and then 1.1.9.3 implies $|a_n - a_0| \leq c$ for all n and thus $|a - a_0| \leq c$. Finally 1.1.9.2 implies $|f(a_n)| \leq c^{2^n}$ and thus $f(a) = 0$.

The first inequality in 1.1.9.2 and 1.1.9.3 imply $|a_{n+1}| \leq 1$. The second implies that $h = -f(a_n)/f'(a_n)$ satisfies

$$|h| < c^{2^n}|f'(a_n)|.$$

Taylor's formula 1.1.9.1 yields

$$f(a_{n+1}) = f(a_n) + f'(a_n)h + h^2 g(a_n, h) = h^2 g(a_n, h)$$

and thus

$$|f(a_{n+1})| \leq |h^2|$$

since $g(X, Y) \in \mathcal{O}_K[X, Y]$ and $|a_n| \leq 1$. Again by Taylor's formula, $f'(a_{n+1}) - f'(a_n)$ is a multiple of h, which has absolute value less than $|f'(a_n)|$, so that

$$|f'(a_{n+1})| = |f'(a_n)|.$$

Putting it all together, we find

$$\left|\frac{f(a_{n+1})}{f'(a_{n+1})^2}\right| < \frac{|h|^2}{|f'(a_n)|^2} < \frac{c^{2^{n+1}}|f'(a_n)|^2}{|f'(a_n)^2|} = c^{2^{n+1}}$$

as required. ■

1.1.9.7 Roots yet again. We saw in section 1.1.9.4 that for any nonarchimedean field K of mixed characteristic $p > 0$ and integer n prime to p, an element $a \in \mathcal{O}_K^\times$ is an nth power if and only if it is an nth power residue, i.e. an nth-power modulo $\mathfrak{m}$. We now inquire about p^nth roots. We will see later that the question reduces to the existence of p^nth roots of $a \in \mathcal{O}_K$ such that $|a - 1| < 1$. For such a, $a_0 = 1$ is a root modulo $\mathfrak{m}$ of the polynomial $f(X) = X^{p^n} - a$, and Newton's method shows that $f(X)$ has a root in K if $|f(1)/f'(1)| < 1$. This says that $|(1 - a)/p^{2n}| < 1$, so a has a p^nth root if $|a - 1| < |p|^{2n}$. For $K = \mathbb{Q}_p$ this says that a is a p^nth power if $a \equiv 1 \mod p^{2n+1}$.

1.1.10 Zeroes of power series. If K is a nonarchimedean field and $f \in \mathcal{O}_K[[X]]$, the root test for the convergence of power series shows that the series $f(x)$ converges for any $x \in \mathfrak{m}$. In this section we show that the problem of finding solutions of $f(x) = 0$ reduces to solving a polynomial equation. We start with a version of the division algorithm.

1.1.10.1 Proposition *Suppose R is a complete local ring with maximal ideal $\mathfrak{m}$. Let $f = \sum_{n\geq 0} a_n X^n \in R[[X]]$ be such that $\bar{f} \neq 0$ and let n be the smallest natural number such that $a_n \in R^\times$. For any $g \in R[[X]]$ there are unique elements $q \in R[[X]]$ and $r \in R[X]$ such that*

$$g = qf + r, \quad \textit{and} \quad \deg r < n.$$

Proof. (Manin) We first prove uniqueness. Denote by $h : R[[X]] \to R[X]$, $t : R[[X]] \to R[[X]]$ the R-linear maps

$$g = \sum_{k\geq 0} b_k X^k \quad \Rightarrow \quad h(g) = \sum_{0\leq k<n} b_k X^k, \quad t(g) = \sum_{k\geq 0} a_{n+k} X^k.$$

Then $t(X^n g) = g$ for any $g \in R[[X]]$, and $h(g) = g$ if g is a polynomial of degree less than n. For f as in the proposition, $t(f) \in R[[X]]^\times$ and the coefficients of $h(f)$ generate a principal ideal (π). Therefore the map

$$m_f(h) = \left(\frac{h(f)}{t(f)}\right) h$$

is well-defined and takes its values in $\pi R[[X]]$.

There are q, r satisfying the conditions of the proposition if and only if $t(g) = t(qf)$. Since $f = h(f) + X^n t(f)$, finding q and r is equivalent to solving

$$t(g) = t(q(h(f)) + X^n t(f)) = t(q(h(f))) + qt(f)$$

for q. If we put $u = qt(f)$ this is is the same as

$$t(g) = t\left(u\frac{h(f)}{t(f)}\right) + u = (I + t \circ m_f)(u).$$

Since π is topologically nilpotent, so is the linear operator m_f and the operator $I+m_f$ is invertible. We find that $u = (I+m_f)^{-1}(g)$ and $q = t(f)^{-1}u$; this proves uniqueness, and conversely if we set $q = t(f)^{-1}(I + m_f)^{-1}(g)$ and $r = g - qf$ then q and r satisify the conditions of the proposition. ■

1.1.10.2 Theorem *(Weierstrass factorization) Suppose R is a complete local ring with maximal ideal $\mathfrak{m}$. Let $f = \sum_{n\geq 0} a_n X^n \in R[[X]]$ be such that $\bar{f} \neq 0$ and let n be the smallest natural number such that $a_n \in R^\times$. Then $f = gh$ where g is a monic polynomial of degree n whose coefficients of degree less than n lie in $\mathfrak{m}$, and $g \in R[[X]]^\times$.*

Proof. Apply proposition 1.1.10.1 with f and $g = X^n$, so that $X^n = qf + r$ with $\deg r < n$. If $q = \sum_{n \geq 0} c_n X^n$ then comparing the coefficients of both sides of $X^n = qf + r$ shows that the coefficients of r all lie in $\mathfrak{m}$, and that

$$1 = \sum_{i+j=n} a_i c_j \equiv a_n c_0 \mod \mathfrak{m}.$$

Then $q \in R[[X]]^\times$ and $f = (X^n - r)q^{-1}$, and we may take $g = X^n - r$ and $h = q^{-1}$. ■

1.1.10.3 Corollary *Suppose K is a discretely valued nonarchimedean field and $f \in \mathcal{O}_K[[X]]$. Then f has at most finitely many zeroes in $\mathfrak{m}$.*

Proof. By dividing f by a power of a uniformizer we may assume that $\bar{f} \neq 0$. If $f = gh$ is the factorization of f given by the theorem, any zero of f is a zero of g and conversely. ■

1.1.11 Exercises.

1.1.11.1 Let R be a ring with a nonarchimedean absolute value. Show that if two closed balls in R intersect then one is contained in the other. Specifically, show that if $r_1 \leq r_2$ and $B(a_1, r_1) \cap B(a_2, r_2) \neq \emptyset$ then $B(a_1, r_1) \subseteq B(a_2, r_2)$.

1.1.11.2 Show that for any prime p and $n \in \mathbb{N}$

$$v_p(n!) = \sum_{k \geq 1} \left[\frac{n}{p^k} \right] = \frac{n - s(n)}{p - 1}$$

where v_p is the p-adic valuation of $\mathbb{Q}$ and $s(n)$ is the sum of the base p digits of n. In other words, if

$$n = a_0 + a_1 p + a_2 p^2 + \cdots + a_r p^r$$

then

$$s(n) = a_0 + a_1 + a_2 + \cdots + a_r.$$

Conclude from this that

$$v_p\left(\binom{n+m}{m}\right) = \frac{s(n) + s(m) - s(m+n)}{p - 1}.$$

1.1.11.3 Find a formula for $v_p\left(\binom{a}{n}\right)$ when $a \in \mathbb{Q}_p \setminus \mathbb{Z}_p$.

1.1.11.4 Prove lemma 1.1.3.2.

1.1.11.5 Show that the polynomial

$$f(X) = X^3 + X^2 - 2X + 8$$

is irreducible in $\mathbb{Q}[X]$ but has three roots in $\mathbb{Q}_2$. Find the 2-adic valuations of these roots and compute their 2-adic expansions through the term in 2^6. (Compute $f(1)$, $f(2)$ and $f(4)$).

1.1.11.6 The Cartesian equation for the lemniscate $r^2 + \cos 2\theta = 0$ is

$$(x^2 + y^2)^2 - y^2 + x^2 = 0.$$

Let k be any field of characteristic not equal to 2. Set $K = k((x))$ and write the above equation as $F(y) = 0$ with $F \in K[y]$. Show that F has four solutions in K, with leading terms ± 1, $\pm x$, and compute these through the term in x^3. When $k = \mathbb{R}$, interpret this in terms of the graph of the lemniscate.

1.2 Extensions of nonarchimedean fields

1.2.1 Extensions. Let K be a valued field. A *valued extension* of K is a K-algebra R with an absolute value that extends that of K. If K is nonarchimedean, a *nonarchimedean extension* of K is valued extension that is complete for its absolute value. In this chapter we are mainly interested in field extensions, but the case where R is a division ring will be important later.

If K is a valued field with residue field k and R is a valued K-algebra, the structure homomorphism $R \to K$ induces a homomorphism $\mathcal{O}_K \subseteq \mathcal{O}_L$. As this homomorphism sends $\mathfrak{m}_K \to \mathfrak{m}_R$, it induces a homomorphism $k \to k_R$, where k_R is the residue field of R. In the case where R is a division ring we call k_R/k the *residual* extension of R/K.

An *extension* of discrete valuation rings is an injective homomorphism $A \to B$ of discrete valuation rings such that if $\mathfrak{m}_A \subset A$, $\mathfrak{m}_B \subset B$ are the maximal ideals then $A \cap \mathfrak{m}_B = \mathfrak{m}_A$. Thus if L/K is an extension of discretely valued fields then $\mathcal{O}_K \to \mathcal{O}_L$ is an extension of discrete valuation rings. Conversely of $A \to B$ is an extension of discrete valuation rings and K (resp. L) is the fraction field of A (resp. B), the valuations of A and B induce valuations on K and L. Multiplying the valuation of L by a suitable factor makes it an extension of the valuation of K, and then L/K is an extension of valued fields in the above sense.

If K is a valued field and L/K is an field extension, the valuation of K extends to L under fairly general circumstances. We will be particularly concerned with the case when K is nonarchimedean (i.e. complete) and L/K is finite.

1.2.2 Normed spaces. Let K be a field with a nonarchimedean absolute value $|\ \ |$ and let V be a K-vector space. A *norm* for V is a map $V \to \mathbb{R}$,

written $v \mapsto ||v||$ such that

$$||v|| = 0 \text{ if and only if } v = 0 \tag{1.2.2.1}$$
$$||av|| = |a|\,||v|| \text{ for all } a \in K,\ v \in V. \tag{1.2.2.2}$$
$$||v + w|| \leq \max(||v||, ||w||) \text{ for all } v,\ w \in V. \tag{1.2.2.3}$$

As is the case for the absolute value of K, a norm on a K-vector space defines a metric for which the operations of addition and scalar multiplication are continuous. In particular for any $v \in V$, the function $x \mapsto x + v$ (translation by v) is a homeomorphism.

A *Banach space* over K is a K-vector space V with a norm such that V is complete for the metric defined by the norm.

A K-vector space of finite dimension always has a norm. For example if V has dimension n and $v_1, \ldots, v_n$ is a basis for V it is easily checked that

$$||v|| = \max(|a_1|, \ldots, |a_n|) \quad \text{if} \quad v = a_1 v_1 + \cdots + a_n v_n \tag{1.2.2.4}$$

defines a norm on V. We will call 1.2.2.4 the *standard norm* associated to the basis $v_1, \ldots, v_n$. If K is a nonarchimedean field then V is a Banach space for this norm.

Two norms on a K-vector space V are *equivalent* if they define the same topology. This will be the case in particular if the norms $||\quad||$, $||\quad||_1$ satisfy the inequalities

$$C||v||_1 \leq ||v|| \leq D||v||_1 \tag{1.2.2.5}$$

for some nonzero constants and all $v \in V$.

1.2.2.1 Proposition *Suppose K is a nonarchimedean field and V is a K-vector space of finite dimension. Any norm on V is equivalent to the norm defined by a basis, and V is complete for this norm.*

Proof. The assertion is vacuous if V has dimension zero. If V has dimension one with basis v_1 then V 1.2.2.5 holds with $C = D = ||v_1||$, and V is evidently complete.

Suppose V has dimension $n > 1$ with basis $v_1, \ldots, v_n$ and the lemma has been proven for K-vector spaces of dimension $n - 1$. Let $||\quad||$ be a norm on V and denote by $||\quad||_1$ the norm associated to the basis $v_1, \ldots, v_n$. For $v \in V$ we write $v = \sum_i a_i v_i$; then

$$||v|| = ||\sum_i a_i v_i|| \leq \max_i(|a_i|\,||v_i||) \leq \max_i(|a_i|) \max_i(||v_i||) = ||v||_1 \max_i(||v_i||)$$

and we can take $D = \max_i(||v_i||)$ in 1.2.2.5. For the other inequality we denote by V_i for $1 \leq i \leq n$ the span of the v_j for all $j \neq i$; then $v_i \notin V_i$ implies $0 \notin v_i + V_i$. For the rest of the argument, topological assertions are relative to the topology defined by $||\quad||$. By induction V_i is complete for the induced

metric and therefore closed in V. Since translation is a homeomorphism $v_i + V_i$ is closed for all i, and

$$\bigcup_{1 \le i \le n} (v_i + V_i)$$

is a closed subset of V not containing 0. It is therefore disjoint from some open ball, say $||x|| < C$. Let $v \in V$ be any nonzero element and write $v = \sum_i a_i v_i$. Choose i such that $||v||_1 = |a_i|$; then $a_i^{-1} v \in v_i + V_i$ and consequently $|a_i|^{-1}||v|| \ge C$, i.e.

$$||v|| \ge C|a_i| = C||v||_1$$

as required. ■

1.2.2.2 Corollary *Suppose K is a nonarchimedean field and V is a K-vector space of finite dimension. Then any two norms on V are equivalent, and for the metric defined by any norm, V is complete.*

1.2.2.3 Lemma *Let K be a field and D a division K-algebra. Any $x \in D$ is contained in a subfield of D containing K.*

Proof. Consider the K-algebra homomorphism $f : K[X] \to D$ sending $g(X)$ to $g(x)$. If x is algebraic over K then the minimal polynomial g of x is irreducible (same proof as for fields) and the image of f is isomorphic to the field $K[X]/(g)$. Otherwise x is transcendental and f is injective. Then f extends to a K-algebra homomorphism $K(X) \to D$, whose image is a field containing K and x. ■

The lemma shows that for any element x of a division K-algebra D it makes sense to speak of the subfield of D generated by x.

1.2.2.4 Theorem *Suppose K is a nonarchimedean field and D is a division K-algebra of finite degree over K. the absolute value of K extends uniquely to D, and D is complete for topology defined by the extension. Thus D is naturally a nonarchimedean division ring.*

Proof. We first show that the extension is unique if it exists. Suppose $|\ \ |_1$, $|\ \ |_2$ are two extensions of the absolute value $|\ \ |$ of K. Since they are norms on D when viewed as a K-vector space the last corollary says they induce the same topology and D is complete. Then $|\ \ |_2 = |\ \ |_2^\alpha$ for some $\alpha > 0$, and since $|\ \ |_1, |\ \ |_2$ coincide on $K \subseteq D$ we must have $\alpha = 1$.

For the proof of existence we set $n = [L : K]$ and denote by $N_{D/K} : D^\times \to K^\times$ the norm for the finite-dimensional K-algebra D (i.e. $N_{D/K}(x)$ is the determinant of the K-linear endomorphism of D induced by left multiplication by x. will show that

$$|x|_D = |N_{D/K}(x)|^{1/n} \tag{1.2.2.6}$$

defines an absolute value on D. Corollary 1.2.2.2 shows that D will be complete for the metric defined by $|\ |_D$.

It is clear that $|x| = 0$ if and only if $x = 0$, and the multiplicative property of the norm shows that $|xy|_D = |x|_D|y|_D$. To prove 1.1.1.4 it suffices by lemma 1.1.1.1 to show that $|x+1|_D \leq 1$ whenever $|x|_D \leq 1$.

We first consider the case where $D = L$ is a field. Pick $x \in L$ and let $f(X) = X^n + a_1X^{n-1} + \cdots + a_n \in K[X]$ be the minimal polynomial of x over K. Up to a sign the characteristic polynomial of multiplication by x is a power of $f(X)$, and by definition $N_{L/K}(x)$ is the constant term of the characteristic polynomial. We therefore have $N_{L/K}(x) = \pm(a_n)^d$ for some d (in fact the degree of $L/K(x)$. Thus if $|x|_D \leq 1$, $|a_n| \leq 1$ as well and by corollary 1.1.9.5, $f(X) \in \mathcal{O}_K[X]$.

Since $f(X)$ is monic irreducible in $K[X]$, $g(X) = f(X-1)$ is monic irreducible as well and belongs to $\mathcal{O}_K[X]$ since $f(X)$ does. In fact $g(X)$ is the minimal polynomial of $x+1$ over K, and reversing the above argument shows that $N_{L/K}(x+1) \in \mathcal{O}_K$, whence $|x+1|_D \leq 1$. The theorem is now proven in the case of a finite extension of fields.

In the general case D lemma 1.2.2.3 says that D is a union of fields of finite degree over K. Suppose $x \in D$ and $F = K(x)$ be the subfield of D generated by x. Then

$$N_{D/K}(x) = N_{F/K}(N_{D/F}(x)) = (N_{F/K})^{[D:F]}$$

and therefore

$$|x|_D = |N_{F/K}|^{1/[F:K]} = |x|_F$$

where $|x|_F$ denotes the unique extension of the absolute value of K to F. Since we have shown that $|\ |_F$ is an absolute value on F, $|x+1|_D \leq |x|_D$ and $|\ |_D$ is an absolute value on D. ■

For later use we record the formula for the corresponding valuation v_D:

$$v_D(x) = \frac{v(x)}{[D:K]}. \tag{1.2.2.7}$$

1.2.2.5 Corollary *If L/K is an algebraic extension of a nonarchimedean field K, the absolute value of K extends uniquely to L/K.*

Proof. The theorem says that the absolute value extends uniquely to every finite extension M/K where $M \subseteq L$. For any $x \in L$, the absolute value extends to $K(x)$ and serves to define $|x|$. To check the axioms it's enough to note that for all x, $y \in L$, $M = K(x,y)$ is a finite extension of K, so the absolute value extends to M. ■

It corollary 1.2.2.5 is *not* asserted that L is complete or that L is a nonarchimedean field; in fact this is frequently false. For example the algebraic closure $\bar{\mathbb{Q}}_p$ of $\mathbb{Q}_p$ has a unique absolute value extending the p-adic absolute value of $\mathbb{Q}_p$; it is not complete for this absolute value (exercise 1.2.9.2).

The completion of $\bar{\mathbb{Q}}_p$ is denoted by $\mathbb{C}_p$. We will see later that $\mathbb{C}_p$ is algebrabraically closed (corollary 1.2.8.50.

The valuation of $\bar{\mathbb{Q}}_p$ or $\mathbb{C}_p$ is not discrete. In fact for any $n > 1$ the polynomial $f(X) = X^n - p$ is irreducible in $\mathbb{Q}[X]$. Denote by v the extension of the

p-adic valuation of $\mathbb{Q}$ to $\bar{\mathbb{Q}}_p$ and let α be a root of f in $\bar{\mathbb{Q}}_p$. Then $v(\alpha) = 1/n$, and we conclude that the value group of v contains $\mathbb{Q} \subset \mathbb{R}$. Then formula 1.2.2.7 shows that the value group is exactly $\mathbb{Q}$. Note that a similar argument can be made for any discretely valued nonarchimedean field.

Because of corollary 1.2.2.5 we may for any extension L/K speak of the absolute value of any $x \in L$ that is algebraic over K.

1.2.2.6 Corollary *If K^{alg}/K is an algebraic closure of K and $x \in K^{alg}$ then all the conjugates of x have the same valuation.*

Proof. If $x' \in K^{alg}$ is conjugate to x, there is an automorphism $\sigma : K^{alg} \to K^{alg}$ such that $\sigma(x) = x'$. Since $x \mapsto |x|$ and $x \mapsto |\sigma(x)|$ are both absolute values of K^{alg} extending that of K, we must have $|\sigma(x)| = |x|$ and therefore $|x'| = |x|$. ■

1.2.2.7 Proposition *If L/K is an algebraic extension of nonarchimedean fields, $\mathcal{O}_L$ is the integral closure of $\mathcal{O}_K$ in L.*

Proof. Denote the integral closure by A. If $x \in A$ satisfies $|x| > 1$, $|x|^{n+1} > |x|^n$ for all $n \geq 0$. On the other hand if x is a root of a monic equation of degree d with coefficients in $\mathcal{O}_K$ then $|x|^d \leq \max_{0 \leq i < d} |x|^i$. Therefore $A \subseteq \mathcal{O}_L$.

Suppose now $x \in \mathcal{O}_L$ and let $f(X) = X^d + \cdots + a_1 X + a_0$ be the minimal polynomial of x over K. If $M = K(x)$, $|x| = |a_0|^{1/d}$ and consequently $a_0 \in \mathcal{O}_K$. Then $f(X) \in \mathcal{O}_K[X]$ by corollary 1.1.9.5 and x is integral over $\mathcal{O}_K$. ■

1.2.3 Residual degree and ramification index. Suppose L/K is an extension of valued fields. The degree of the residual extension is called the *residual degree* of L/K and is denoted by $f_{L/K}$. Furthermore Γ_K is a subgroup of Γ_L and the index $[\Gamma_L : \Gamma_K]$ is called the *ramification index* of L/K and is denoted by $e_{L/K}$ If L/K and M/L are extensions of nonarchimedean fields the formulas

$$e_{M/K} = e_{M/L} e_{L/K}, \qquad f_{M/K} = f_{M/L} f_{L/K}. \tag{1.2.3.1}$$

follow immediately from the definitions.

1.2.3.1 Proposition *If L/K is a finite extension of valued fields, $e_{L/K}$ and $f_{L/K}$ are finite and*

$$e_{L/K} f_{L/K} \leq [L : K]. \tag{1.2.3.2}$$

Proof. Pick integers $r \leq e_{L/K}$ and $s \leq f_{L/K}$; it is enough to show $rs \leq [L : K]$. By hypothesis there are $x_1, \ldots, x_r \in L^\times$ such that $|x_i|$ have distinct images in Γ_L/Γ_K, and $y_1, \ldots, y_s \in \mathcal{O}_L$ with linearly independent images in k_L. Note that this implies that $y_i \in \mathcal{O}_K^\times$ for $1 \leq i \leq s$. We will show that the $x_i y_j$ are linearly independent over K.

Suppose to the contrary that

$$\sum_{i,j} a_{i,j} x_i y_j = 0 \tag{1.2.3.3}$$

with $a_{i,j} \in K$. Choose (k, ℓ) such that

$$|a_{i,j}x_iy_j| \leq |a_{k,\ell}x_ky_\ell|$$

for all i, j. For $i \neq k$ it cannot happen that $|a_{i,j}x_iy_j| = |a_{k,\ell}x_ky_\ell|$; in fact since $|y_j| = |y_\ell| = 1$, this would imply $|x_i/x_k| \in \Gamma_K$ contrary to the choice of x_i.

We now move the terms in 1.2.6.2 with $i \neq k$ to the right hand side and divide by $a_{k,\ell}x_k$. The result is an equality

$$\sum_j b_jy_j = c$$

with $b_j \in \mathcal{O}_K$, $b_\ell = 1$ and $|c| < 1$. Reducing mod $\mathfrak{m}_L$ yields a nontrivial dependence relation among the $\bar{y}_j$ with coefficients in k, contrary to the choice of y_j. ■

We shall see that equality holds when K and L are complete and discretely valued. Nonetheless strict inequality in 1.2.6.2 is possible even when K and L are complete; see exercise 1.2.9.5.

1.2.3.2 Corollary *If L/K is a finite extension of valued fields, the valuation of L is discrete (resp. trivial) if and only if the valuation of K is discrete (resp. trivial).*

Proof. Since Γ_L/Γ_K is finite the assertion is clear in the discrete case. In the case of trivial valuations it suffices to observe that the value group cannot be a nontrivial finite group. ■

1.2.4 Unramified extensions. For the rest of this chapter we will be concerned with finite extensions of valued fields. A finite extension L/K of valued fields is *residually separable* if the residual extension is separable. A finite extension L/K of valued fields is *unramified* if it is residually separable and $f_{L/K} = [L : K]$. The definition implies $e_{L/K} = 1$, but in general the condition $f_{L/K} = [L : K]$ is stronger.

1.2.4.1 Lemma *Let K be a valued field and $f \in \mathcal{O}_K[X]$ a monic polynomial whose reduction $\bar{f}$ is irreducible and separable. Then $L = K[X]/(f)$ is an unramified extension of K and if $x \in L$ is a root of f in L, $\mathcal{O}_L = \mathcal{O}_K[x]$ and $L = K(x)$.*

Proof. Observe first that f is irreducible in $K[X]$ by Gauss's lemma, so L/K is a field extension of degree $\deg f$. We can assume that x is the image if $X \in K[X]$ in L, and it suffices to show that $\mathcal{O}_L = \mathcal{O}_K[x]$. In fact if this is true, the residual field k_L of L is $k[X]/(\bar{f})$ where as usual k is the residue field of K; then k_L/k is separable since $\bar{f}$ is, and $[L : K] = \deg f = \deg \bar{f} = [k_L : k]$.

Since K is complete, $\mathcal{O}_L$ is the integral closure of $\mathcal{O}_K$ in L; therefore $x \in \mathcal{O}_L$ and $\mathcal{O}_K[x] \subseteq \mathcal{O}_L$. Conversely if $y \in \mathcal{O}_L$ we can write

$$y = a_{n-1}x^{n-1} + \cdots + a_1x + a_0$$

with $a_i \in K$ and $n = \deg(f) = [L : K]$. We must show that $|a_i| \leq 1$. If not the suppose the maximum of $|a_0|, \ldots, |a_{n-1}|$ is attained by $|a_i| > 1$; then dividing the equation by a_i and reducing modulo $\mathfrak{m}$ yields a nontrivial dependence relation among the $\bar{x}^i$ with $0 \leq i < n$. This is impossible since $\bar{x}$ has degree n over k, and it follows that $\mathcal{O}_L = \mathcal{O}_K[x]$. ■

1.2.4.2 Theorem *Suppose K is a nonarchimedean field with residue field k and k'/k is a finite separable extension of k.*

(i). There is an unramified extension L/K, unique up to K-isomorphism such whose residual extension is k'/k.

(ii). If $x \in L$ is such that $\bar{x} \in k'$ generates k'/k then $L = K(x)$ and $\mathcal{O}_L = \mathcal{O}_K[x]$. If $f \in \mathcal{O}_K[X]$ is the minimal polynomial of x then $\bar{f}$ is the minimal polynomial of $\bar{x}$. Conversely if f is any monic lifting of the minimal polynomial of $\bar{f}$ then f has a root $x \in \mathcal{O}_L$ such that $\bar{x}$ generates k'/k.

(iii). Suppose E/K is an algebraic extension with residue field k_E. Any k-homomorphism $k' \to k_E$ extends uniquely to a K-homomorphism $L \to E$.

Proof. Suppose $\bar{x} \in k'$ generates k' as an extension of k, $\bar{f}$ is the minimal polynomial of x' over k and choose a monic lifting $f \in \mathcal{O}_K[X]$ of $\bar{f}$. By construction f is separable, and it is irreducible by Gauss. The existence of L/K then follows from lemma 1.2.4.1, as does assertion (ii).

The uniqueness assertion in (i) follows from (iii), applied to a pair of unramified finite extensions L/K, L'/K with isomorphic residual extensions k'/k and the identity of k'. Suppose then that E/K is an algebraic extension with with residual extension k_E/k, and recall that the absolute value of K extends uniquely to E. If $\bar{x}$, $\bar{f}$ and f are as before, we can identify L with $K[X]/(f)$. Let $\bar{y}$ be the image of $\bar{x}$ under the k-homomorphism $k' \to k_E$ and let $y' \in \mathcal{O}_E$ be an element lifting $\bar{y}$. Since E/K is algebraic, $K(y)$ is a finite extension of K and is therefore complete for the absolute value of $K(y')$ induced by that of E. The residue field of $K(y')$ is a subfield of k_E containing $\bar{y}$, so by the corollary to Hensel's lemma the separable polynomial f has a root $y \in K(y')$ The map $K[X] \to L$ sending $X \mapsto y$ induces an injective homomorphism $K[X]/(f) \to L$ since f is irreducible. This is the desired homomorphism $L \to E$; it is evidently unique, since it is determined by the image of $x \in L$, which is in turn determined by the k-homomorphism $k' \to k_E$. ■

1.2.4.3 Corollary *Two unramified extensions of K are isomorphic if and only if their residual extensions are isomorphic.*

1.2.4.4 Corollary *Suppose L/K is a finite unramified extension of nonarchimdean fields with residual extension k_L/k. Then any k-automorphism of k_L is the reduction of a unique K-automorphism of L.*

1.2.4.5 Corollary *A local field has up to isomorphism exactly one unramified extension of any given degree.*

Proof. Since the residue field of a local field is finite, this follows from the corresponding assertion for finite fields. ■

1.2.4.6 Proposition *Suppose L/K is an finite unramified extension of nonarchimedean fields and F/K is an extension of nonarchimedean fields. Then $L \otimes_K F$ is a direct sum of unramified extensions of K.*

Proof. By theorem 1.2.4.2 we can write $L = K(x)$ with $x \in \mathcal{O}_L$ integral over K, and if $f \in \mathcal{O}_K[X]$ is the minimal polynomial of x then $\bar{f} \in kX$ is irreducible and separable. Let f/k be the residual extension of F/K and let $\bar{f} = \prod_i \bar{g}_i$ the factorization of $\bar{f}$ in $f[X]$ into irreducible monic polynomials. Since $\bar{f} \in k[X]$ is separable, the $\bar{g}_i$ are separable and relatively prime to each other. By Hensel's lemma we have $f = \prod_i g_i$ with $g_i \in \mathcal{O}_F[X]$, g_i irreducible and separable and reducing modulo $\mathfrak{m}_F$ to $\bar{g}_i$. If we set $L_i = F[X]/(g_i)$ then $L \otimes_K F \simeq \bigoplus_i L_i$, and lemma 1.2.4.1 shows that each L_i is an unramified extension of F. ■

1.2.4.7 Corollary *Suppose K is a nonarchimedean field, E/K is an extension and L, F are finite extensions of K contained in E.*

(i). If E/L and L/K are finite then E/K is unramified if and only if E/L and L/K are unramified.

(ii). If L/K is unramified then so is LF/F.

(iii). If L/K and F/K are unramified, so is LF/K.

Proof. The first assertion follows from the transitivity of separability and the multiplicative properties of the degree and the residual degree 1.2.3.1. The third assertion follows from the second. As to the second, LF is the image of the natural map $L \otimes_K F \to E$, which must be one of the direct summands of $L \otimes_K F$. ■

We will say that an algebraic extension L/K of nonarchimedean fields is unramified if every finite extension of K contained in L is unramified in the previous sense. The first part of corollary 1.2.4.7 shows that this definition is consistent with the previous one.

Corollary 1.2.4.7 implies that if L/K is any algebraic extension, the compositum of all finite unramified extensions of K contained in L is unramified; it is called the *maximal unramified extension of K in L*. If L is an algebraic closure of K it is called "the" maximal unramified extension of K since any two such extensions are isomorphic.

1.2.4.8 Corollary *Suppose K is a nonarchimedean field, L/K is an unramified finite extension and F is the maximal unramified extension of K in L. If $f_{L/K}$ is finite then $f_{L/K} = [F : K]$*

Proof. It suffices to observe that F and L have the same residue field. ■

1.2.5 Totally ramified extensions. An extension L/K of valued fields is *tamely ramified* if $e_{L/K}$ is finite and not divisible by the residual characteristic, and *totally ramified* if $f_{L/K} = 1$.

1.2.5.1 Proposition *Suppose K is a discretely valued nonarchimedean field and L/K is a finite totally ramified extension. If $\tau \in L$ is a uniformizer, $\mathcal{O}_L = \mathcal{O}_K[\tau]$ and τ is a root of an Eisenstein polynomial in $\mathcal{O}_K[X]$ of degree $e_{L/K} = [L : K]$. In particular $\mathcal{O}_L$ is a free $\mathcal{O}_K$-module of rank $[L : K]$.*

Proof. Observe first that a system of representatives of K is also one for L. If π be a uniformizer of K and v is the normalized valuation of L, $v(\tau^i\pi^j) = je_{L/K}+i$ and it follows from proposition 1.1.8.1 and the remark following it that any $x \in \mathcal{O}_L$ has a unique expansion in the form

$$x = \sum_{i\geq 0} \sum_{0\leq j<e} s(a_{i,j})\pi^i\tau^j$$

with $a_{i,j} \in k$ and $e = e_{L/K}$. It follows that $1, \tau, \ldots, \tau^{e-1}$ is a basis of $\mathcal{O}_L$ as $\mathcal{O}_K$-module. In particular $\mathcal{O}_L = \mathcal{O}_K[\tau]$, $L = K(\tau)$ and $[L : K] = e_{L/K}$. The minimal polynomial f of τ over K is a monic polynomial in $\mathcal{O}_K[X]$; since all conjugates of τ have absolute less than one, the coefficients of f lie in $\mathfrak{m}$. The constant term is up to a sign the product of the conjugates; there are e of them and they all have the same absolute value, namely $|\tau| = |\pi|^{1/e}$. The constant term thus has absolute value $|\pi|$, so it is a uniformizer in K, and f is an Eisenstein polynomial. ■

Corollary 1.2.4.7 has no analogue for totally ramified extensions: there are totally ramified extensions L/K, F/K with L, $F \subset E$ such that LF/K is not totally ramified (c.f. exercise 1.2.9.6).

Let M/K be any extension of fields and suppose L, F are subfields of M containing K. Recall that L and F are *linearly disjoint* if the canonical map $L \otimes_K F \to M$ is injective; if so its image is the compositum LF of L and F.

1.2.5.2 Proposition *Suppose K is a discretely valued nonarchimedean field and L, F are extensions of K contained is some algebraic closure of K. If L/K is unramified an F/K is totally ramified, L and F are linearly disjoint over K.*

Proof. Since tensor products commute with inductive limits we may assume that L and F are finite extensions of K. It suffices to show that $L \otimes_K F$ is a field. By proposition 1.2.5.1 there is an isomorphism $F \simeq K[X]/(f)$ for some Eisenstein polynomial $f \in K[X]$. Then

$$L \otimes_K F \simeq L[X]/(f)$$

and since L/K is unramified, f is an Eisenstein polynomial in $L[X]$. Therefore $L \otimes_K F$ is a field. ■

1.2.5.3 Example: cyclotomic fields. Denote by μ_{p^n} the set of p^nth roots of 1 in $\bar{\mathbb{Q}}_p$ and let $\mathbb{Q}_p(\mu_{p^n})$ be the field obtained by adjoining the elements of μ_{p^n} to $\mathbb{Q}_p$. If ζ is a primitive p^nth root of 1, i.e. a generator of μ_{p^n} then $\mathbb{Q}_p(\mu_{p^n}) = \mathbb{Q}_p(\zeta)$, and ζ is a root of the polynomial

$$\begin{aligned} f(X) &= \frac{X^{p^n} - 1}{X^{p^{n-1}} - 1} \\ &= X^{(p-1)p^{n-1}} + X^{(p-2)p^{n-1}} + \cdots + X^{p^{n-1}} + 1 \end{aligned} \tag{1.2.5.1}$$

Since $f(X+1)$ is an Eisenstein polynomial in $\mathbb{Z}_p[X]$ $f(X)$ is irreducible, $\mathbb{Q}_p(\mu_{p^n})$ is totally ramified of degree $(p-1)p^{n-1}$ over $\mathbb{Q}_p$, and $\zeta - 1$ is a uniformizer of $\mathbb{Q}_p(\zeta)$. Furthermore $\eta = \zeta^{p^{n-1}}$ is a primitive pth root of 1, so that $\mathbb{Q}_p(\eta)$ is an extension of degree $p-1$ contained in $\mathbb{Q}_p(\mu_{p^n})$. Thus $\mathbb{Q}_p(\eta)$ is the maximal tamely ramified extension of $\mathbb{Q}_p$ in $\mathbb{Q}_p(\mu_{p^n})$.

1.2.6 Separable extensions. When L/K is a separable extension of nonarchimedean fields, equality in 1.2.3.3 follows from standard commutative algebra, as we now explain.

Let A be any Dedekind domain with fraction field K, L/K a finite separable extension of K and B the integral closure of A in L. Since L/K is separable, B is a finite A-algebra. Let us recall the proof: the relative trace $\mathrm{Tr}_{L/K} : L \to K$ induces a K-valued bilinear form $\langle x, y\rangle = \mathrm{Tr}_{L/K}(xy)$ which is nondegenerate when L/K is separable. If we choose a basis of L/K contained in B, B is contained in the span of the dual basis, and is therefore finitely generated.

Suppose now $\mathfrak{m}$ is a maximal ideal of A, and recall that the localization $A_\mathfrak{m}$ is a discrete valuation ring, K is the fraction field of $A_\mathfrak{m}$ and the valuation of $A_\mathfrak{m}$ induces a discrete nonarchimedian valuation of K with integer ring $A_\mathfrak{m}$. The localization $B_\mathfrak{m}$ has finitely many maximal ideals $\mathfrak{p}_1, \ldots \mathfrak{p}_r$ lying above $\mathfrak{m}$; as before to each $\mathfrak{p}_i$ is associated a discrete valuation of L whose integer ring is the localization $B_{\mathfrak{p}_i}$. Denote by e_i and f_i the ramification index and residual degre of $B_{\mathfrak{p}_i}/A_\mathfrak{m}$; the *Dedekind degree formula* asserts that

$$[L : K] = \sum_i e_i f_i. \tag{1.2.6.1}$$

We see from this how strict inequality can obtain in 1.2.6.2: since e_i, $f_i \geq 1$ we must have $e_i f_i < [L : K]$ if there is more than one prime ideal of B above $\mathfrak{m}$.

1.2.6.1 Theorem *If L/K is a separable extension of discretely valued nonarchimedean fields,*

$$e_{L/K} f_{L/K} = [L : K]. \tag{1.2.6.2}$$

Proof. The preceding discussion applies to $A = \mathcal{O}_K$ and $B = \mathcal{O}_L$ since the latter is the integral closure of the former in L. Since K is complete the valuation of K has a unique extension to L. This implies that $\mathcal{O}_L$ has only one maximal ideal above $\mathfrak{m}$, and the equality follows from 1.2.6.1. ■

In section 1.3.2 we will determine all local fields of positive characteristic. For characteristic zero we have:

1.2.6.2 Theorem *A local field of characteristic zero is a finite extension of* $\mathbb{Q}_p$.

Proof. A local field K is discretely valued and the residue field k has characteristic $p > 0$ for some p. Since K has characteristic 0 it is an extension of $\mathbb{Q}_p$ by proposition 1.1.6.2. Since K is discretely valued it has finite ramification index over $\mathbb{Q}_p$, and since k is finite the residue degree is finite. Since $K/\mathbb{Q}_p$ is separable, 1.2.6.2 shows that $[K : \mathbb{Q}_p]$ is finite. ■

1.2.7 Residually separable extensions. The inequality 1.2.6.2 is also an equality if L/K is a finite residually separable extension of nonarchimedean fields. This condition is automatic if the residue field of K is perfect, and in particular if K is a local field.

1.2.7.1 Theorem *Suppose K is a discretely valued nonarchimedean field, L/K is a finite residually separable extension and F is the maximal unramified extension of K in L. Then L/F is totally ramified, $[F : K] = f_{L/K}$ and $e_{L/K} = [L : F]$. In particular*

$$[L : K] = e_{L/K} f_{L/K} \tag{1.2.7.1}$$

and L/K is unramified if and only if $e_{L/K} = 1$. Finally, $\mathcal{O}_L$ is a free $\mathcal{O}_K$-module of rank $[L : K]$.

Proof. By corollary 1.2.4.8 we know that $[F : K] = f_{L/K}$, and since $[F : K] = f_{F/K}$ as well we deduce that $f_{L/F} = 1$, i.e. L/F is totally ramified. By proposition 1.2.5.1, $e_{L/F} = [L : F]$, and since $e_{F/K} = 1$ we conclude that $e_{L/K} = [L : F]$. The formula 1.2.7.1 then follows from the multiplicativity of the degree.

We know that $\mathcal{O}_L$ is a free $\mathcal{O}_F$-module of rank $[L : F]$ by proposition 1.2.5.1 while $\mathcal{O}_F$ is a free $\mathcal{O}_K$-module of rank $[F : K]$ by part (ii) of theorem 1.2.4.2. It follows that $\mathcal{O}_L$ is a free $\mathcal{O}_K$-module of rank $[L : K]$. ■

We can improve the last assertion of theorem 1.2.7.1.

1.2.7.2 Corollary *If L/K satisifies the condition of the theorem, there is an $x \in \mathcal{O}_L$ such that $\mathcal{O}_L = \mathcal{O}_K[x]$ and $L = K(x)$.*

Proof. Let F be the maximal unramified extension of K in L. We have seen that $F = K(y)$ and $\mathcal{O}_F = \mathcal{O}_K[y]$ for any $y \in \mathcal{O}_F$ reducing to a generator $\bar{y}$ of the residual extension k_F/k. Furthermore if τ is any uniformizer of $\mathcal{O}_L$ then $\mathcal{O}_L = \mathcal{O}_F[\tau]$. Setting $e = e_{L/K}$ and $f = f_{L/K}$ we see that the ef products $y^i\tau^j$ for $0 \le i < f$ and $0 \le j < e$ are basis of $\mathcal{O}_L$ as an $\mathcal{O}_K$-algebra. From this it is easily seen that if x is any element of $\mathcal{O}_L$ with the same reduction as y, then the $x^i\tau^j$ for $0 \le i < f$ and $0 \le j < e$ form a basis of $\mathcal{O}_L$ as an $\mathcal{O}_K$-algebra; by Nakayama it suffices to check that this is so modulo $\mathfrak{m}_K$.

Let f be the minimal polynomial of y over K. Since f reduces to the minimal polynomial of $\bar{y}$, $f'(y)$ is a unit in $\mathcal{O}_F$. Then if τ is any uniformizer of L,

$$f(y+\tau) = f(y) + f'(y)\tau + b\tau^2 = f'(y)\tau + b\tau^2$$

for some $b \in \mathcal{O}_L$, i.e. $f(y+\tau)$ is a uniformizer in $\mathcal{O}_L$. If we set $x = y+\tau$ then x and y have the same reduction modulo $\mathfrak{m}_L$, and the $x^i f(x)^j$ for $0 \le i < f$ and $0 \le j < e$ form an $\mathcal{O}_K$-basis of $\mathcal{O}_L$. ■

The assertion of the corollary can fail if K is not complete (c.f. exercise 1.2.9.7).

1.2.8 Krasner's lemma. Fix a nonarchimedean field K and an algebraic closure K^{alg} of K. For $x \in K^{alg}$ we define

$$\kappa_x = \min_{i \neq j} |x_i - x_j| \tag{1.2.8.1}$$

where the x_i are the distinct conjugates of x over K.

1.2.8.1 Theorem *(Krasner's lemma) With the above notation, if $y \in K^{alg}$ is such that $|x-y| < \kappa_x$ and x is separable over $K(y)$ then $x \in K(y)$.*

Proof. For all $s \in \mathrm{Gal}(K^{alg}/K(y))$ we have

$$|s(x) - y| = |s(x) - s(y)| = |x - y|$$

and therefore

$$|s(x) - x| = |s(x) - y + y - x| \le |x - y| < \kappa_x.$$

Since $s(x)$ and x are conjugate over K, $s(x) = x$ for all s and consequently $x \in K(y)$. ■

1.2.8.2 Corollary *Suppose L/K is a separable algebraic extension of the nonarchimedean field K and x, $y \in L$ have the same degree over K. If $|y-x| < \kappa_x$ then $K(y) = K(x)$.*

Proof. Here it is automatic that x is separable over $K(y)$. Since $K(x)$ and $K(y)$ have the same degree over K and $K(x) \subseteq K(y)$, we have $K(x) = K(y)$. ■

1.2.8.3 Proposition *If L/K is a totally and tamely ramified extension of nonarchimedean fields of degree e, there is a uniformizer $\pi \in \mathcal{O}_K$ and a root $x \in L$ of $X^e - \pi$ such that $L = K(x)$.*

Proof. Observe first that L/K is necessarily separable. If τ (resp. π) is a uniformizer of $\mathcal{O}_L$ (resp. $\mathcal{O}_K$) then $\tau^e/\pi \in \mathcal{O}_L^\times$. Since the residual extension is trivial, we can change π by a unit in $\mathcal{O}_K$ so as to have $\tau^e/\pi \equiv 1 \mod \mathfrak{m}_L$, or

$|\tau^e/\pi - 1| < 1$. Set $f(X) = X^e - \pi$, so that $|f(\tau)| < |\pi|$. If $a_1, \ldots, a_e$ are the roots of f in some algebraic closure of L, the last inequality says that

$$\prod_{1 \le i \le e} |\tau - a_i| < |\pi|. \tag{1.2.8.2}$$

The quantities a_i/a_j are all roots of $X^e - 1 = 0$, and since e is not divisible by the residue characteristic, $X^e - 1$ is separable modulo $\mathfrak{m}$. Then the residue of a_i/a_j mod $\mathfrak{m}$ is not 1, so that $|a_i/a_j - 1| = 1$ for all $i \neq j$, i.e. $|a_i - a_j| = |a_i|$ for $i \neq j$. If $|\tau - a_i| = |a_i|$ for all i then $\prod_i |\tau - a_i| = |a_i|^e = |\pi|$, contradicting 1.2.8.2. Therefore there is an i such that $|\tau - a_i| < |a_i - a_j|$ for all $j \neq i$. Since both τ and a_i have degree e over K, corollary 1.2.8.2 shows that $K(\tau) = K(a_i)$ and we may take $x = a_i$. ■

If K is any field with a nonarchimedean valuation. For

$$f = \sum_n a_n X^n \in K[X]$$

the *Gauss norm* of f is

$$|f|_{\text{Gauss}} = \max(|a_0|, \ldots, |a_n|). \tag{1.2.8.3}$$

This is a vector space norm in the sense of section 1.2.2.

1.2.8.4 Proposition *Let K be a nonarchimedean field, $f \in K[X]$ and let x be a simple root of f in some algebraic closure K^{alg} of K. For all sufficiently small $\epsilon > 0$ there is a $\delta > 0$ satisyfing the following property: for all $g \in K[X]$ of the same degree as f such that $|f - g|_{\text{Gauss}} < \delta$, there is a unique root y of g such that $|y - x| < \epsilon$. For these roots x, y we have $K(x) \subseteq K(y)$. If f is irreducible, so is g, and then $K(x) = K(y)$.*

Proof. Let $x_1 = x, x_2, \ldots, x_d$ be the distinct roots of f in K^{alg} and replace ϵ by a quantity that is smaller than 1, ϵ and the $|x_i - x_j|$ for all $i \neq j$. Then $\epsilon < \kappa_x$ since the conjugates of x are all to be found among the $x_1, \ldots, x_d$. Since the expression $g(x)/g'(x)^2$ defines a continuous function of the coefficients of g, there is a $\delta > 0$ such that $|f - g|_{\text{Gauss}} < \delta$ implies $g'(x) \neq 0$ and

$$\left| \frac{g(x)}{g'(x)^2} \right| < \epsilon$$

for all i. By Newton's method g has root y such that $|x - y| < \epsilon$. Since $\epsilon < |x - x_i|$ for all $i > 1$ we cannot have $|x_i - y| < \epsilon$ if $i > 1$. This establishes the first statement. Since x is a simple root of f it is separable over K, and the containment $K(x) \subseteq K(y)$ follows from Krasner's lemma. Finally if f is irreducible,

$$\deg(f) = [K(x) : K] \le [K(y) : K] \le \deg(g) = \deg(f)$$

and it follows that g is irreducible and that $K(x) = K(y)$. ■

The constant ϵ can be made effective, c.f. exercise 2.1.7.7.

The hypothesis that x is a simple root of f cannot be dropped. Suppose for example that K is a nonarchimedean field of characteristic $p > 0$ and $f_a(X) = X^p + aX + \pi$ where π is a uniformizer in K and $a \in K$. A root of f_0 generates an inseparable extension L of K, while for any nonzero a however small, f_a has p distinct roots any one of which generates a separable extension L' of K; in particular $L' \neq L$.

1.2.8.5 Corollary *The completion of an algebraically closed valued field is algebraically closed.*

Proof. Suppose K is an algebraically closed valued field and let $\hat{K}$ be the completion of K. Let $f \in \hat{K}[X]$ be an irreducible polynomial; since K is algebraically closed it is perfect, so f is separable. Let x be a root of f in some finite extension of $\hat{K}$, choose ϵ and δ as in proposition 1.2.8.4. Finally, choose $g \in K[X]$ so that $|f - g|_{\text{Gauss}} < \delta$. Since f is irreducible, so is g, and g has a root y such that $\hat{K}(x) = \hat{K}(y)$. Since $g \in K[X]$, y is algebraic over K and so $y \in K$. Therefore $\hat{K}(x) = \hat{K}$, and $x \in \hat{K}$, i.e. f has degree one. ■

For example $\mathbb{C}_p$, the algebraic closure of $\bar{\mathbb{Q}}_p$, is algebraically closed.

1.2.8.6 Corollary *Suppose k is a field of characteristic 0 with algebraic closure k^{alg}, and set $K = k((T))$. The algebraic closure of K is the union of the fields $k^{alg}((T^{1/n}))$ for all $n \geq 1$.*

Proof. Any unramified extension of $k((T))$ has the form $\ell((T))$ for some algebraic extension of k. Thus the maximal unramified extension of K is $k^{alg}((T))$. Any finite extension of $k^{alg}((T))$ is tame, and the result follows. ■

1.2.8.7 Theorem *For any $n > 0$, a local field of characteristic zero has a finite number of extensions of degree n.*

Proof. Let K be a local field of characteristic 0. The residue field field of K has exactly one extension of any given degree, so K has exactly one unramified extension of any given degree. It is therefore enough to show that the number of totally ramified extensions of degree n is finite.

We write degree n Eisenstein polynomials in $K[X]$ in the form

$$X^n + a_1 X^{n-1} \cdots + a_{n-1} X + \pi u$$

where $a_i \in \mathfrak{m}$ and $u \in \mathcal{O}_K^\times$, and identify them with points of the space

$$(a_1, \ldots, a_{n-1}, u) \in \mathfrak{m}^{n-1} \times \mathcal{O}_K^\times = \mathfrak{X}$$

The Gauss norm on $K[X]$ induces the natural topology on $\mathfrak{X}$, and in particular X is compact. If $f \in \mathfrak{X}$, a root of f generates a totally ramified extension of

degree n, and this extension is separable since K has characteristic 0. Conversely we have seen that every totally ramified extension of K arises in this way.

We now apply proposition 1.2.8.4 to each $f \in \mathfrak{X}$ with $\epsilon = \kappa_x$, where x is any root of f in an algebraic extension of K. If δ_x is the corresponding quantity from the proposition we choose an open ball B_f around $f \in \mathfrak{X}$ of radius δ_x. Since X is compact it is covered by finitely many $B_{f_1}, \ldots, B_{f_r}$. If a root of some Eisenstein polynomial f generates a totally ramified extension of K of degree n, $f \in B_{f_i}$ for some i, and then $K(x) = K(x_i)$ by the proposition; thus K has at most r totally ramified extensions of degree n. ■

We will see in section 2.1.5 that a local field of characteristic $p > 0$ has infinitely many separable extensions of degree p.

1.2.8.8 Quadratic extensions of $\mathbb{Q}_p$. As an example, let's find all quadratic extensions of $\mathbb{Q}_p$. By Kummer theory they all have the form $\mathbb{Q}_p(\sqrt{a})$ and the distinct fields of this type correspond bijectively to the nontrivial elements of $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$. So it is enough to work out the structure of $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$.

Suppose first p is odd. As groups $\mathbb{Q}_p^\times \simeq \mathbb{Z}_p^\times \times \mathbb{Z}$ the second factor is generated by a uniformizer. Furthermore $\mathbb{Z}_p^\times \simeq \mathbb{F}_p^\times \times U$ where U is the cyclic subgroup generated by $1 + p \in \mathbb{Z}_p^\times$. Since p does not divide 2, every element of U is a square by the results of section 1.1.6.5. We conclude that

$$\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2} \simeq (\mathbb{F}_p^\times/\mathbb{F}_p^{\times 2}) \times (\mathbb{Z}/2\mathbb{Z})$$

where the first factor is cyclic of order two, generated by the image of any $u \in \mathbb{Z}_p^\times$ that is not a square modulo p, and second factor is generated by the class of p. The elements of $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$ are represented by 1 ,u, p and up, and so $\mathbb{Q}_p$ has three quadratic extensions when p is odd, namely $\mathbb{Q}_p(\sqrt{u})$, $\mathbb{Q}_p(\sqrt{p})$ and $\mathbb{Q}_p(\sqrt{up})$.

The analysis for $p = 2$ is similar except for the structure of $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$. By the results of section 1.1.9.7, $x \in \mathbb{Z}_2^\times$ has a square root if $x \equiv 1 \mod 8$. On the other hand $(\mathbb{Z}_2/8\mathbb{Z}_2)^\times = \{1, 3, 5, 7\}$ is the noncyclic group of order 4. It follows that $x \in \mathbb{Z}_2^\times$ is a square if and only if $x \equiv 1 \mod 8$, and $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$ is a product of three cyclic groups of order 2. Thus $\mathbb{Q}_2$ has seven quadratic extensions, namely $\mathbb{Q}_2(\sqrt{3})$, $\mathbb{Q}_2(\sqrt{5})$, $\mathbb{Q}_2(\sqrt{7})$, $\mathbb{Q}_2(\sqrt{2})$, $\mathbb{Q}_2(\sqrt{6})$, $\mathbb{Q}_2(\sqrt{10})$ and $\mathbb{Q}_2(\sqrt{14})$.

1.2.9 Exercises

1.2.9.1 (i) Show that any two algebraically closed fields of the same cardinality are isomorphic. (ii) Deduce from this that $\mathbb{C}$ is isomorphic to $\bar{\mathbb{Q}}_p$ for any p. In particular, $\mathbb{C}$ has a nonarchimedean absolute value extending the p-adic absolute value on $\mathbb{Q}$ for any p. (iii) Do you still believe in the axiom of choice?

1.2.9.2 Show that $\bar{\mathbb{Q}}_p$ is not complete for the absolute value extending that of $\mathbb{Q}_p$ (construct an element of $\mathbb{C}_p$ that is not fixed by any open subgroup of $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$).

1.2.9.3 A nonarchimedean field is *spherically complete* if any nested sequence $B_1 \supseteq B_2 \supseteq B_3 \ldots$ of closed balls has nonempty intersection. (i) Show that any discretely valued nonarchimedean field is spherically complete. (ii) Show that $\mathbb{C}_p$ is *not* spherically complete.

1.2.9.4 Let K be a nonarchimedean field and L/K an algebraic extension. Show that the conclusion of Hensel's lemma is valid for L. Likewise for Newton's method.

1.2.9.5 Let β_n be a sequence of elements of $\bar{\mathbb{Q}}_2$ such that $\beta_0 = 2$ and $\beta_{n+1}^2 = \beta_n$ for all $n \geq 0$. Let $K_0 = \mathbb{Q}_2(\beta_1, \beta_2, \ldots)$ and and let K be the completion of K_0 with respect to the unique absolute value of K_0 extending the 2-adic valuation of $\mathbb{Q}_2$. (i) Show that $X^2 - 3$ is irreducible in $K[X]$. (ii) If $L = K(\alpha)$ where α is a root of $X^2 - 3$ in $\bar{\mathbb{Q}}_2$, show that $[L : K] = 2$ but $e_{L/K} = f_{L/K} = 1$. (use the previous exercise).

1.2.9.6 Show that a compositum of totally ramified extensions is not necessarily totally ramified (consider the extensions in section 1.2.8.8: which are unramified? totally ramified?)

1.2.9.7 Let $R = \mathbb{Z}_{(2)}$, the localization of $\mathbb{Z}$ at the maximal ideal (2), so that the fraction field R is $\mathbb{Q}$. Let $K = \mathbb{Q}(\alpha)$ where α is a root of the polynomial $f(X) = X^3 + X^2 - 2X + 8$ (c.f. exercise 1.1.11.5). (i) Show that the 2-adic absolute value of $\mathbb{Q}$ has exactly 3 inequivalent extensions v_0, v_1, v_2 to K. (ii) Show that the integral closure S of R in K is the set of $x \in K$ such that $v_i(x) \geq 0$ for $i = 0, 1, 2$. (observe that S is a Dedekind domain). (iii) Show that there is no $x \in S$ such that $S = R[x]$ (first show that if this were so, the prime ideals of S above (2) would be in a one-to-one correspondence with the distinct irreducible factors of f modulo 2).

1.3 Existence and Uniqueness theorems.

In this section we will determine the structure of equicharacteristic nonarchimedean fields, and show that for any perfect field k of characteristic p there is an absolutely unramified, mixed characteristic nonarchimedean field with residue field k, which is furthermore unique up to canonical isomorphism.

1.3.1 ***p*-rings** A *p-ring* is a pair (A, I) consisting of a commutative ring A with an ideal I such that A is I-adically complete and separated and the quotient ring A/I is a perfect ring of characteristic $p > 0$. A morphism $f : (A, I) \to (A', I')$ of p-rings is a ring homomorphism $A \to A'$ sending I into I'. If $(A, I) \to (A', I')$ is a morphism of p-rings, the *reduction* of f is the homomorphism $A/I \to A'/I'$.

If (A, I) is a p-ring then $p \in I$ and A is p-adically complete and separated.

Then $p \in I$ implies that

$$x \equiv y \mod I^n \Rightarrow x^p \equiv y^p \mod I^{n+1} \tag{1.3.1.1}$$

for all x, $y \in A$ and $n > 0$.

A p-ring is *strict* if $I = (p)$ and p is not a divisor of zero in A. The argument of proposition 1.1.8.1 can be used with almost no change to show that if (A, I) is strict, any element of A has a unique p-adic expansion

$$a = \sum_{n \geq 0} [a_n] p^n$$

with $a_n \in A/I$ for all n.

As before a *system of representatives* of (A, I) is a section $s : A/I \to A$ the canonical projection. A system of representatives s is *additive* if $s(a + b) = s(a) + s(b)$ and *multiplicative* if $s(ab) = s(a)s(b)$. If s is both additive and multiplicative, the image of s is a subring of A. We will shows that any p-ring has a multiplicative system of representatives. We will need the following general result whose proof is left as an exercise:

1.3.1.1 Lemma *Let A be a commutative ring $I \subset A$ an ideal and suppose that A is I-adically complete and separated. Let $U_n \subseteq A$ for $n > 0$ be a sequence of nonempty subsets such that $U_{n+1} \subseteq U_n$ for all $n > 0$, and if x, $y \in U_n$ then $x \equiv y \mod I^{n+1}$. The intersection $\bigcap_{n>0} U_n$ is a singleton.*

As usual we denote the canonical surjection $A \to A/I$ by $x \mapsto \bar{x}$. For $a \in A/I$ and $n > 0$ let $U_n(a) \subset A$ be the subset defined by

$$x \in U_n(a) \iff \bar{x} = a \quad \text{and } x \text{ is a } p^n\text{th power.} \tag{1.3.1.2}$$

Evidently $U_{n+1}(a) \subseteq U_n(a)$ for all n. The next lemma shows that we can apply lemma 1.3.1.1 to the sets $U_n(a)$:

1.3.1.2 Lemma *For all $a \in A/I$ and $n > 0$, $U_n(a)$ is nonempty, and if x, $y \in U_n(a)$ then $x \equiv y \mod I^{n+1}$.*

Proof. Since A/I is perfect there is a $b \in A/I$ such that $b^{p^n} = a$. Then if $u \in A$ is such that $\bar{u} = b$, $u^{p^n} \in U_n(a)$.

Suppose now x and y are elements of $U_n(a)$ and write $x = u^{p^n}$, $y = v^{p^n}$. Since $\bar{x} = \bar{y} = a$, $\bar{u}^{p^n} = \bar{v}^{p^n}$ and thus $\bar{u} = \bar{v}$. This says $u \equiv v \mod I$, and repeated application of 1.3.1.1 yields $u^{p^n} \equiv v^{p^n} \mod I^{n+1}$, i.e. $x \equiv y \mod I^{n+1}$. ■

1.3.1.3 Proposition *Any p-ring (A, I) has a unique system of representatives $s : A/I \to A$ which commutes with the pth power map: $s(a^p) = s(a)^p$. This s is multiplicative, and $x \in A$ is in the image of s if and only if it is a p^nth power for all $n > 0$. If A has characteristic p, s is additive as well.*

Proof. By lemmas 1.3.1.1 and 1.3.1.2 we can define a function $s : A/I \to A$ by

$$\{s(a)\} = \bigcap_{n>0} U_n(a).$$

By construction $s(a)$ reduces to a modulo I, i.e. s is a system of representatives. From the definition 1.3.1.2 we see that the pth power map sends $U_n(a)$ into $U_{n+1}(a^p)$, from which it follows that $s(a)^p = s(a^p)$.

We next show that $x \in A$ is in the image of s if and only if it is a p^nth power for all $n > 0$. Since A/I is perfect the condition is clearly necessary; on the other hand if x is a p^nth power for all $n > 0$ and $a = \bar{x}$ then $x \in U_n(a)$ for all n and thus $x = s(a)$.

From this it follows that $s : A/I \to A$ is the unique system of representatives such that $s(a^p) = s(a)^p$: if s' is another such map then $s'(a)$ is a p^nth power for all n, hence $s'(a) = s(b)$ for some $b \in A/I$. Reducing modulo I yields $a = b$ and then $s'(a) = s(a)$.

For any a, $b \in A/I$ the elements $s(ab)$ and $s(a)s(b)$ are p^nth powers for all n, and have the same reduction, namely ab. Therefore $s(ab) = s(a)s(b)$ for all a and b in A/I, so s is multiplicative.

Suppose finally A has characteristic p. Then

$$s(a) + s(b) = s(a^{p^{-n}})^{p^n} + s(b^{p^{-n}})^{p^n} = (s(a^{p^{-n}}) + s(b^{p^{-n}}))^{p^n}$$

is a p^nth power for all n, so that $s(a)+s(b) = s(c)$ for some c. Reducing modulo I yields $c = a + b$ and then $s(a) + s(b) = s(a + b)$, so s is additive. ■

The $s(a)$ in the proposition is called the *Teichmüller lift* of a, and we will denote it by $[a]$. Teichmuller lifts are functorial in the following sense:

1.3.1.4 Corollary *If $f : (A, I) \to (A', I')$ is a morphism of p-rings with residue fields k, k', the diagram*

$$\begin{tikzcd} k \arrow[r, "{[\ ]}"] \arrow[d, "\bar{f}"'] & A \arrow[d, "f"] \\ k' \arrow[r, "{[\ ]}"] & A' \end{tikzcd}$$

commutes.

Proof. In fact for all $x \in k$, $f([x])$ is a p^nth power for all $n > 0$ and reduces to $f(x) \in k'$. ■

1.3.1.5 Remark. The commutative diagram in the corollary says that $f([a]) = [f(a)]$, so if (A, I) is a strict p-ring the morphism f is

$$f(\sum_{n\geq 0}[a_n]p^n) = \sum_{n\geq 0}[\bar{f}(a_n)]p^n. \tag{1.3.1.3}$$

In particular, f is the unique morphism lifting $\bar{f}$.

1.3.2 Equicharacteristic nonarchimedean fields. As a first application we show that any complete equicharacteristic nonarchimedean field is a field of Laurent series.

1.3.2.1 Theorem *Suppose K is a discretely valued equicharacteristic nonarchimedean field. If the residue field of K is perfect, K has a field of representatives, and there is an isomorphism $K \simeq k((T))$ for which the splitting $s : k \to \mathcal{O}_K$ is the identity on k.*

Proof. We first show that K has a field of representatives. When K and k have positive characteristic this follows from proposition 1.3.1.3, so we suppose K and k have characteristic zero. Then $\mathbb{Q}$ maps injectively to K and k, and thus into $\mathcal{O}_K$. In particular any subfield of $\mathcal{O}_K$ must map injectively to k. By Zorn's lemma there is a maximal subfield $F \subseteq \mathcal{O}_K$, and we denote by $\bar{F}$ its image in k, so that $F \to \bar{F}$ is an isomorphism.

We claim that k is algebraic over $\bar{F}$. If for example $t \in k$ is transcendental over $\bar{F}$, it is the image under reduction of some $x \in \mathcal{O}_K$ which must itself be transcendental over F since $F \to \bar{F}$ is an isomorphism. Then $F(x)$ is a a proper extension field of F, contradicting the maximality of F.

Suppose now $t \in k$ and $\bar{f}(X) \in \bar{F}[X]$ is the minimal polynomial of t. Since $\bar{F}$ has characteristic zero, $\bar{f}$ is separable. If $f \in F[X]$ is monic and reduces to $\bar{f}$, it is irreducible and has a root $x \in \mathcal{O}_K$ reducing to t by the corollary to Hensel's lemma. Since F is a maximal subfield of $\mathcal{O}_K$, $F(x) = F$, whence $\bar{F}(t) = \bar{F}$ and $t \in \bar{F}$. We conclude that $\bar{F} = k$ and F is a field of representatives.

If π is a uniformizer of K, any element of $\mathcal{O}_K$ has a unique series representation of the form $\sum_k s(a_k)\pi^k$. It follows that the map $f : k[[T]] \to \mathcal{O}_K$ defined by

$$\sum_k a_k T^k \mapsto \sum_k s(a_k)\pi^k$$

is an isomorphism of rings, and passing to the quotient field yields a isomorphism $k((T)) \to K$ of nonarchimedean fields. ■

If K has characteristic $p > 0$ and k is not perfect it is still true, although much more difficult to prove, that $K \simeq k((T))$. In fact there is no canonical isomorphism of this sort, or canonical identification of k with a subfield of $\mathcal{O}_K$.

1.3.3 The universal p-ring on a set. Let S be a set and $\mathbb{Z}[S]$ the polynomial ring on the elements of S. For $n \in \mathbb{N}$ we set $R_n = \mathbb{Z}[S]$ and define

$$\mathbb{Z}[S^{p^{-\infty}}] = \varinjlim_n R_n$$

where $R_n \to R_{n+1}$ is the homomorphism induced by $X \mapsto X^p$ for all $X \in S$. We can think of $\mathbb{Z}[S^{p^{-\infty}}]$ as the polynomial ring in the variables $X^{p^{-n}}$ for all $n \geq 0$ and $X \in S$; $X^{p^{-n}}$ can be identified with the image if $X \in S \subset R_n$ in $\mathbb{Z}[S^{p^{-\infty}}]$. We denote by $i_S : S \to \mathbb{Z}[S^{p^{-\infty}}]$ the composite map $S \to \mathbb{Z}[S] \to \mathbb{Z}[S^{p^{-\infty}}]$ where

the first map is the canonical one for a polynomial ring, and $\mathbb{Z}[S] \to \mathbb{Z}[S^{p^{-\infty}}]$ uses the identification $\mathbb{Z}[S] = R_0$.

Since inductive limits commute with quotients

$$\mathbb{F}_p[S^{p^{-\infty}}] = \mathbb{Z}[S^{p^{-\infty}}]/p\mathbb{Z}[S^{p^{-\infty}}] \tag{1.3.3.1}$$

is the inductive limit of the polynomial rings $\bar{R}_n = \mathbb{F}_p[S]$ where again $\bar{R}_n \to \bar{R}_{n+1}$ is induced by $X \mapsto X^p$ for $X \in S$. Since the pth power homomorphism is the identity on $\mathbb{F}_p$, $\bar{R}_n \to \bar{R}_{n+1}$ is the pth power homomorphism on $\mathbb{F}_p[S]$, and it follows that $\mathbb{F}_p[S^{p^{-\infty}}]$ is the perfection of $\mathbb{F}_p[S]$.

Finally, we define $\mathbb{Z}_p\{S^{p^{-\infty}}\}$ to be the p-adic completion of $\mathbb{Z}[S^{p^{-\infty}}]$. Since p is not a zero-divisor in $\mathbb{Z}_p[S^{p^{-\infty}}]$ it is not a zero-divisor in $\mathbb{Z}_p\{S^{p^{-\infty}}\}$. Since

$$\mathbb{F}_p[S^{p^{-\infty}}] = \mathbb{Z}\{S^{p^{-\infty}}\}/p\mathbb{Z}\{S^{p^{-\infty}}\}.$$

it follows that $\mathbb{Z}\{S^{p^{-\infty}}\}$ is a strict p-ring.

The map i_S induces maps $S \to \mathbb{F}_p[S^{p^{-\infty}}]$, $S \to \mathbb{Z}\{S^{p^{-\infty}}\}$ which we also denote by i_S, as they are all compatible in the obvious sense.

1.3.3.1 Proposition *Let S be a set.*

(i). Let A be a perfect ring of characteristic p. Any map of sets $f : S \to A$ of S extends uniquely to a homomorphism $f^\flat : \mathbb{F}_p[S^{p^{-\infty}}] \to A$ such that

$$\begin{tikzcd} S \arrow[r, "i_S"] \arrow[dr, "f"'] & \mathbb{F}_p[S^{p^{-\infty}}] \arrow[d, "f^\flat"] \\ & A \end{tikzcd} \tag{1.3.3.2}$$

commutes.

(ii). Let (A, I) be a p-ring. Any map of sets $f : S \to A/I$ extends uniquely to a homomorphism $f^\sharp : \mathbb{Z}_p\{S^{p^{-\infty}}\} \to A$ such that $\overline{f^\sharp} = f^\flat$.

Proof. If A is perfect of characteristic p we set $R_n = \mathbb{F}_p[S]$ and identify $\mathbb{F}_p[S^{p^{-\infty}}]$ with $\varinjlim_n R_n$. Then $f^\sharp$ is homomorphism induced by the homomorphisms sending $X \in S \subset R_n$ to $f(X)^{p^{-n}}$. The uniqueness of $f^\sharp$ is a general property of inductive limits.

If (A, I) is a p-ring we set $R_n = \mathbb{Z}[S]$ and identify $\mathbb{Z}[S^{p^{-\infty}}]$ with $\varinjlim_n R_n$. The homomorphisms $R_n \to A$ which send $X \in S \subset R_n$ to $[f(X)]^{p^{-n}}$ yield a homomorphism $\mathbb{Z}[S^{p^{-\infty}}] \to A$ whose reduction is the one constructed previously. Since $p \in I$ the completion of $\mathbb{Z}[S^{p^{-\infty}}] \to A$ is a homomorphism $f^\sharp : \mathbb{Z}_p\{S^{p^{-\infty}}\} \to A$. The uniqueness of the lifting $f^\sharp$ follows from remark 1.3.1.5. ∎

1.3.3.2 Corollary *The constructions $\mathbb{F}_p[S^{p^{-\infty}}]$, $\mathbb{Z}_p\{S^{p^{-\infty}}\}$ are functorial in S.*

Proof. This is easily checked directly, but in any case the functoriality of $\mathbb{F}_p[S^{p^{-\infty}}]$ is a general property of free objects, and that of $\mathbb{Z}_p\{S^{p^{-\infty}}\}$ follows from its universal property. ■

1.3.3.3 Corollary *If $g : A \to B$ is a homomorphism of perfect rings of characteristic p and $f : S \to A$ is a map of sets then $(gf)^\flat = gf^\flat$.*

Proof. The uniqueness part of proposition 1.3.3.1 shows that the right hand diagonal arrow in the commutative diagram

$$\begin{tikzcd} S \arrow[r, "i_S"] \arrow[dr, "f"'] & \mathbb{F}_p[S^{p^{-\infty}}] \arrow[d, "f^\flat"] \arrow[dr, "gf^\flat"] & \\ & A \arrow[r, "g"] & B \end{tikzcd}$$

is equal to $(gf)^\flat$. ■

The first part of proposition 1.3.3.1 asserts that $\mathbb{F}_p[S^{p^{-\infty}}]$ and the map $i_S : S \to \mathbb{F}_p[S^{p^{-\infty}}]$ is a free object in the category of perfect rings. We will accordingly call $\mathbb{F}_p[S^{p^{-\infty}}]$ the *free perfect ring on S*. The ring $\mathbb{Z}_p\{S^{p^{-\infty}}\}$ is not a free object in this precisely this sense and we will call it instead the *universal p-ring on S*.

Since elements of $\mathbb{F}_p[S^{p^{-\infty}}]$ may be thought of as polynomials in the $X^{p^{-n}}$ there is an obvious sense in which one can substitute elements of a perfect ring A for the various $X \in S$ appearing in f. This is precisely what the homomorphism $f^\sharp$ in part (i) of proposition 1.3.3.1 does: $f : S \to A$ can viewed as an assignment of values to the various $X \in S$; then for any $g \in \mathbb{F}_p[S^{p^{-\infty}}]$, $f^\sharp(g)$ is the result of substituting these values into g.

1.3.4 The Uniqueness Theorem The next theorem shows that part (ii) of proposition 1.3.3.1 is a consequence of part (i).

1.3.4.1 Theorem *Let (A, I) be a strict p-ring and (A', I') a p-ring. For any homomorphism $f_0 : A/I \to A'/I'$ there is a unique morphism of p-rings $f : (A, I) \to (A', I')$ such that $\bar{f} = f_0$.*

Proof. Uniqueness follows for the formula of equation 1.3.1.3, given that f exists. As for existence we set $S = A/I$; for $a \in A/I$ it will be convenient to denote the corresponding element of S by X_a. The maps $g : S \to A/I$, $g' : S \to A'/I'$ given by $g(X_a) = a$, $g(X_a) = f(a)$ induce homomorphisms of p-rings $g^\sharp$, $(g')^\sharp$

sitting in a diagram

$$\begin{tikzcd} \mathbb{Z}_p\{S^{p^{-\infty}}\} \arrow[d, "g^\sharp"'] \arrow[dr, "(g')^\sharp"] & \\ A \arrow[r, dotted] & A' \end{tikzcd}$$

and we want to fill in the dotted arrow with a homomorphism. The homomorphism g is surjective since $g^\sharp$ maps $\sum_{n\geq 0}[X_{a_n}]p^n$ to $\sum_{n\geq 0}[a_n]p^n$, so it suffices to show that $\mathrm{Ker}(g) \subseteq \mathrm{Ker}(g')$. Suppose $h = \sum_{i\geq 0}[h_i]p^i \in \mathrm{Ker}(g^\sharp)$; since $g^\sharp(h) = \sum_{i\geq 0}[g^\flat(h_i)]p^i$, $h \in \mathrm{Ker}(g^\sharp)$ says that $g^\flat(h_i) = 0$ in A/I for all i. Then $g' = fg$ implies that $(g')^\flat(h_i) = f(g^\flat(h_i)) = 0$ for all i, so that $h \in \mathrm{Ker}((g')^\sharp)$. ■

The uniqueness theorem follows by taking $(A', I') = (A, I)$:

1.3.4.2 Corollary *Let k be a perfect ring of characteristic $p > 0$. If A and A' are strict p-rings with residue ring k there is a unique isomorphism $A \xrightarrow{\sim} A'$ reducing modulo p to the identity of k.*

1.3.5 The existence theorem. We now apply the universal p-ring construction to

$$S = \{X_0, X_1, X_2, \ldots Y_0, Y_1, Y_2, \ldots\}. \tag{1.3.5.1}$$

If we set

$$x = \sum_{n\geq 0}[X_n]p^n, \quad y = \sum_{n\geq 0}[Y_n]p^n$$

then for any polynomial $F \in \mathbb{Z}[X, Y]$,

$$F(x, y) = \sum_{n\geq 0}[h_n^F(X., Y.)]p^n \tag{1.3.5.2}$$

for some sequence of $h_n^F(X., Y.) \in \mathbb{F}_p[S^{p^{-\infty}}]$. Similar considerations apply to polynomials in any number of variables.

The polynomials h_n^F so define give a "universal" method of computing F in any strict p-ring (A, I). As we observed earlier, any $a \in A$ has a unique series expansion

$$a = \sum_n [a_n]p^n \tag{1.3.5.3}$$

with $a_n \in A/I$. We can use 1.3.5.3 to identify the $a \in A$ with the sequence $(a_n)_{n\in\mathbb{N}} \in (A/I)^{\mathbb{N}}$. Thus any strict p-ring has a canonical "coordinate system" in which the coordinates are elements of A/I.

1.3.5.1 Proposition *Suppose (A, I) is a p-ring and $a = (a_i)$, $b = (b_i) \in A$. For any $F \in \mathbb{Z}[X, Y]$, $F(a, b) = (h_i^F(a., b.))$ where the h_i^F are defined by 1.3.5.2.*

Proof. Apply proposition 1.3.3.1 with S as in 1.3.5.1 and f sends $X_i \mapsto a_i$ and $Y_i \mapsto b_i$. Then $f^\flat((X.)) = a$, $f^\flat((Y.)) = b$, and since $f^\flat$ is a homomorphism $f^\flat(F((X.),(Y.))) = F(a,b)$. On the other hand $F((X.),(Y.)) = (h_i(X.,Y.))$ by definition, so $f^\flat(F((X.),(Y.))) = (h_i(a.,b.)$. ■

If we take $F(X,Y) = X+Y$, $F(X,Y) = XY$ or $F(X) = -X$ the proposition yields S_n, P_n, $M_n \in \mathbb{F}_p[S^{p^{-\infty}}]$ such that

$$(a_i) + (b_i) = (S_i(a.,b.)), \quad (a_i)(b_i) = (P_i(a.,b.)), \quad -(a_i) = (M_i(a.) \quad (1.3.5.4)$$

for any strict p-ring A and (a_i), $(b_i) \in A$. In other words the ring operations in a strict p-ring can be computed by means of "universal" formulas in the coordinates. The commutative and associative laws for addition are expressed by the formulas

$$S_i(X.,Y.) = S_i(Y.,X.), \quad S_i(X.,S.(Y.,Z.)) = S_i(S.(X.,Y.),Z.)) \qquad (1.3.5.5)$$

and similarly for the remaining ring axioms. Note also that

$$p(a_0,a_1,\ldots) = (0,a_0,a_1,\ldots) \qquad (1.3.5.6)$$

in this notation.

1.3.5.2 Theorem *For any perfect ring k of characteristic $p > 0$ there exists a strict p-ring with residue ring k, which is unique up to unique isomorphism.*

Proof. We have already proven uniqueness. For existence we consider the ring $\mathbb{Z}_p\{S^{-p^{-\infty}}\}$ with $S = k$, let $g : S \to k$ be the identity and $g^\flat : \mathbb{F}_p[k^{-p^{-\infty}}] \to k$ is the universal homomorphism. As before we identify elements of $\mathbb{Z}_p\{k^{-p^{-\infty}}\}$ with vectors of elements of $\mathbb{F}_p[k^{-p^{-\infty}}]$. Define a relation on $\mathbb{Z}_p\{k^{-p^{-\infty}}\}$ by

$$(a_i) \sim (b_i) \quad \text{if and only if } g^\flat(a_i) = g^\flat(b_i) \text{ for all } i \geq 0.$$

This is evidently an equivalence relation and we define A to be the quotient of $\mathbb{Z}_p\{k^{-p^{-\infty}}\}$ by this relation. By construction we can identify elements of A vectors of elements of k.

If $(a_i) \sim (a'_i)$ and $(b_i) \sim (b'_i)$ then

$$(a_i) + (b_i) = (S_i(a.,b.)), \quad (a'_i) + (b'_i) = (S_i(a'.,b'.))$$

and

$$g^\flat(S_i(a.,b.)) = S_i(g^\flat(a.),g^\flat(b.)) = S_i(g^\flat(a'.),g^\flat(b'.)) = g^\flat(S_i(a'.,b'.))$$

which show that $(a_i)+(b_i) \sim (a'_i)+(b'_i)$. Similar calculations show that $(a_i)(b_i) \sim (a'_i)(b'_i)$ and $-(a_i) \sim -(a'_i)$.

It follows that the ring operations in $\mathbb{Z}_p\{k^{-p^{-\infty}}\}$ descend to A. The ring axioms hold for these operations since they hold in $\mathbb{Z}_p\{k^{-p^{-\infty}}\}$ and $\mathbb{Z}_p\{k^{-p^{-\infty}}\} \to$

A is surjective. The relation 1.3.5.6 and the above description of A show that A is p-adically separated and complete. We also see from 1.3.5.6 that p is not a divisor of zero in A and that the map sending the class of (a_n) to a_0 identifies $A/pA \simeq k$. Thus $(A, (p))$ is a strict p-ring with residue ring k. ■

We denote the unique strict p-ring with residue ring k by $W(k)$; it is called the *ring of Witt vectors of* k. Taking k to be a perfect field, we find:

1.3.5.3 Corollary *For any perfect field k of characteristic $p > 0$ there is a complete, absolutely unramified mixed characteristic discrete valuation ring $W(k)$ with residue field k, and a nonarchimedean field $K(k)$ with integer ring $W(k)$. The ring $W(k)$ and the field $K(k)$ are unique up to unique isomorphism.*

Proof. By construction $W(k)$ is a local ring whose maximal ideal is generated by p, so $W(k)$ is a discrete valuation ring; the other assertions are evident. ■

To be sure, uniqueness must be understood as the assertion that if A is any complete absolutely unramified discrete valuation ring of mixed characterstic $p > 0$ there is a unique isomorphism $W(k) \to A$ reducing to the identity of k.

1.3.5.4 Corollary *If A is a complete discrete valuation ring of mixed characteristic $p > 0$ with perfect residue field k, there is a unique injective homomorphism $W(k) \to A$ reducing to the identity of k. If e is the ramification index of $W(k) \to A$ then A is a free $W(k)$-module of rank e.*

1.3.5.5 Corollary *Suppose A is a complete discrete valuation ring with perfect residue field k, and that k'/k is a perfect extension of k. There is an extension $A \to A'$ of discrete valuation rings such that A' is complete and the reduction of $A \to A'$ modulo p is $k \to k'$.*

Proof. If the fraction field K of A is equicharacteristic p then $A \simeq k[[T]]$ and we may take $A' = k'[[T]]$. In the mixed characteristic case we know that $A \simeq W(k)[X]/(f)$ for some Eisenstein polynomial f. Then f is irreducible and $W(k')$ and $A' = W(k')[X]/(f)$ is a complete discrete valuation ring with residue field k'. ■

1.3.6 Lifts of Frobenius. If k is a perfect ring we can apply theorem 1.3.4.1 to the Frobenius homomorphism $k \to k$, i.e. the map $x \mapsto x^p$. The resulting isomorphism is usually denoted by $\sigma : W(k) \to W(k)$. In terms of vectors, it is

$$\sigma(a_n) = (a_n^p) \tag{1.3.6.1}$$

as is easily checked. We also use σ to denote the obvious (and unique) extension to $K(k)$. Finally, we will use the same notation σ for lifts of the qth power map $x \mapsto x^q$ for any (fixed) power q of p.

If A is any commutative ring and $I \subset$ is an ideal such that A/I has characteristic $p > 0$, a *lift of the qth power Frobensius* to A is a homomorphism $\sigma : A \to A$ reducing modulo I to the qth power map.

1.3.6.1 Proposition *Let A be a complete discrete valuation ring of mixed characteristic $p > 0$ with perfect residue field k. If the fraction field of A is a normal extension of the fraction field of $W(k)$, the map $\sigma : W(k) \to W(k)$ extends to an automorphism of A.*

Proof. If K is the fraction field of A, the map $\sigma : K(k) \to K(k)$ extends to an automorphism of K by Galois theory. Since A is the integral closure of $W(k)$ in K, this σ induces an isomorphism of A. ■

Note that no claim is made concerning uniqueness.

If K is a nonarchimedean field of equicharacteristic $p > 0$ with perfect residue field k, the existence of lifts of Frobenius is evident: we know that $K \simeq k((T))$, and thus

$$\sigma(\sum_n a_n T^n) = \sum_n a_n^p T^n \tag{1.3.6.2}$$

is a lift of Frobenius. Note that we can not use the Frobenius of K itself here, since this is not an automorphism of K or $\mathcal{O}_K$. Furthermore we will in the sequel need lifts of Frobenius that fix a given uniformizer of K.

1.3.6.2 Lemma *Suppose K is a discretely valued nonarchimedean field with algebraically closed residue field k of characteristic $p > 0$. If $\sigma : K \to K$ is a lift of the qth power Frobenius, then for any $a_1, \ldots, a_n \in \mathcal{O}_K$ there is a $v \in \mathcal{O}_K$ such that*

$$v^{\sigma^n} + a_0 v^{\sigma^{n-1}} + \cdots + a_{n-1} v + a_n = 0. \tag{1.3.6.3}$$

If one of the a_i is a unit, v can be taken to be a unit.

Proof. Let π be a uniformizer of K. Dividing 1.3.6.3 by a suitable power of π^{σ^n} shows that we can assume one of the a_i is a unit. We solve 1.3.6.3 by successive approximations. Modulo π it says that

$$v^{q^n} + a_0 v^{q^{n-1}} + \cdots + a_{n-1} v + a_n = 0$$

which can be solved since k is algebraically closed, and the solution is nonzero in k. Suppose now v has been found modulo π^k and set

$$v^{\sigma^n} + a_0 v^{\sigma^{n-1}} + \cdots + a_{n-1} v + a_n = \pi^k b.$$

If we put $v = u + \pi^k w$ then u will be a solution modulo π^{k+1} if

$$(v^{\sigma^n} + \pi^k w^{p^n}) + a_0(v^{\sigma^{n-1}} + \pi^k w^{p^{n-1}}) + \cdots + a_{n-1}(v + \pi^k w) + a_n = \pi^k b$$

modulo π^{k+1}, or in other words if w satisfies

$$w^{p^n} + a_1 w^{p^{n-1}} + \cdots + a_{n-1} w + a_1 = b$$

modulo π. Since k is algebraically closed this has a solution. ■

1.3.6.3 Corollary *For any lift $\sigma : K \to K$ of the qth power Frobenius, there is a uniformizer π of $\mathcal{O}_K$ fixed by σ.*

Proof. If π is any uniformizer, $\pi^\sigma = u\pi$ for some $u \in \mathcal{O}_K^\times$. By the lemma there is a $v \in \mathcal{O}_K^\times$ such that $v^\sigma = uv$, and then $v^{-1}\pi$ is fixed by σ. ■

1.3.6.4 Corollary *If $a \in K^\times$ the endomorphism $x \mapsto ax^{\sigma^n} - x$ of K is surjective if a has positive valuation, or if a has negative valuation and σ is an isomorphism, or if k is algebraically closed.*

Proof. If a has positive valuation,

$$ax^{\sigma^n} - x = -y \tag{1.3.6.4}$$

can be solved for x by recursive substitution:

$$x = \sum_{i \geq 0} a^i y^{\sigma^{in}}.$$

If a has negative valuation and σ is an isomorphism we rewrite 1.3.6.4 as

$$(ax^{\sigma^n}) - a^{-\sigma^{-n}}(ax^{\sigma^n})^{\sigma^{-n}} = -y$$

which is solvable by the previous case. Finally when k is algebraically closed and $a \in \mathcal{O}_K^\times$ we can rescale x so as to have $y \in \mathcal{O}_K$, which requires changing a by a unit. Then equation 1.3.6.4 is solvable by lemma 1.3.6.2. ■

1.3.6.5 Theorem *Suppose K is a discretely valued nonarchimedean field with residue field k of characteristic $p > 0$. If σ is a lift of the qth power Frobenius of k to K, the fixed field K^σ of σ is a local field.*

Proof. If k^{alg} is the algebraic closure of k then K has an unramified extension K' with residual extension k^{alg}/k, and σ extends to a lift of Frobenius to K'. It suffices to show that $(K')^\sigma$ is a local field; in other words we may reduce to the case when k is algebraically closed. In particular we may assume that K has a uniformizer π fixed by σ.

Suppose first that K is equicharacteristic $p > 0$; then $K \simeq k((T))$ where T is any uniformizer of K. We may assume T is fixed by σ; since σ is continuous this means that $K^\sigma = \mathbb{F}_q((T))$, which is a local field.

Suppose now that K has mixed characteristic $p > 0$ and let π be a uniformizer fixed by σ. Then $\mathcal{O}_K \simeq W(k)[\pi]$ and the minimial polynomial of π is an Eisenstein polynomial f. If the coefficients of f do not belong to $W(\mathbb{F}_q)$ then $f - f^\sigma$ would be a polynomial of degree less than $\deg(f)$, of which π is a root since it is fixed by σ. Thus $f \in W(\mathbb{F}_q)[X]$ and

$$\mathcal{O}_K^\sigma \simeq (W(k)[X]/(f))^\sigma \simeq W(\mathbb{F}_q)[X]/(f) \simeq W(\mathbb{F}_q)[\pi]$$

and it follows that K is a local field. ■

Chapter 2

Ramification Theory

2.1 The Different and Discriminant

2.1.1 Derivations. Let A be a commutative ring, B a commutative A-algebra and let M be a B-module. An *A-derivation of B into M* is an additive map $D : B \to M$ such that $D(A) = 0$ and

$$D(xy) = xD(y) + yD(x) \tag{2.1.1.1}$$

for all x, $y \in B$. If D and D' are derivations of B into M then so are $D + D'$ and bD for all $b \in B$, so the derivations form a B-module, which we denote $\mathrm{Der}_A(B)$.

Let $D(M)$ be the B-algebra $B \oplus M$ with the evident addition and multiplication defined by

$$(b \oplus m)(b' \oplus m') = bb' \oplus bm' + b'm$$

(the algebra of "dual numbers" on M). It is an augmented B-algebra via the homomorphisms $b \mapsto b \oplus 0$, $b \oplus m \mapsto b$ and we may identify M with a B-submodule of $D(M)$ such that $M^2 = 0$ for this ring structure.

If D is an A-derivation $B \to M$, the map

$$v : B \to D(M) \qquad v(b) = b \oplus D(b) \tag{2.1.1.2}$$

is an A-algebra homomorphism for the A-algebra structure of $D(M)$ induced by the B-module structure. Denote by $\mathrm{Hom}_{B/A}(B, D(M)) \subset \mathrm{Hom}_A(B, D(M))$ the set of A-algebra homomorphisms whose composition with the augmentation is the identity. Then for any $D \in \mathrm{Der}_A(B, M)$ the map 2.1.1.2 is in $\mathrm{Hom}_{B/A}(B, D(M))$, and we have defined a map

$$\mathrm{Der}_A(B, M) \to \mathrm{Hom}_{B/A}(B, D(M)) \tag{2.1.1.3}$$

of sets which is evidently functorial in M.

2.1.1.1 Lemma *The map 2.1.1.3 is a bijection.*

Proof. Any $v : B \to D(M)$ in $\mathrm{Hom}_{B/A}(B, D(M))$ has the form $v(b) = b \oplus D_v(b)$ for some A-linear map $D_v : B \to M$. If $a \in A$ then $D_v(a) = 0$, since the A-algebra structure of $B(M)$ comes from the B-algebra structure which is $b \mapsto b \oplus 0$. The condition that v is a ring homomorphism implies that $D_v(bb') = bD_v(b') + b'D_v(b)$. Thus D_v is an A-derivation, and the map $v \mapsto D_v$ is inverse to 2.1.1.3. ■

2.1.2 Differentials. There is a "universal" A-derivation of B into a B-module. Denote by I the kernel of the multiplication map $B \otimes_A B \to B$. The module of *differentials* of B/A is the B-module

$$\Omega^1_{B/A} = I/I^2. \tag{2.1.2.1}$$

If $\sum_i a_i \otimes b_i \in I$ then $\sum_i a_i b_i = 0$ and then

$$\sum_i a_a \otimes b_i = \sum_i a_i(1 \otimes b_i - b_i \otimes 1)$$

and it follows the $\Omega^1_{B/A}$ is generated by elements of the form

$$dx = 1 \otimes x - x \otimes 1 + I^2. \tag{2.1.2.2}$$

Easy calculations show that

$$d(x + y) = dx + dy, \qquad d(xy) = xdy + ydx \tag{2.1.2.3}$$

and $da = 0$ for any $a \in A$. It follows that d is an A-derivation $d : B \to \Omega^1_{B/A}$. If $u : M \to \Omega^1_{B/A}$ is any B-module homomorphism the composition $u \circ d$ is a A-derivation of B into M. We will show that every A-derivation $B \to M$ has this form; this is the sense in which $d : B \to \Omega^1_{B/A}$ is the "universal A-derivation" of B into a B-module.

2.1.2.1 Proposition *The map*

$$\mathrm{Hom}_B(\Omega^1_{B/A}, M) \to \mathrm{Der}_A(B, M) \qquad f \mapsto f \circ d \tag{2.1.2.4}$$

is an isomorphism.

Proof. It suffices to show that the composite of this map with 2.1.1.3 is a bijection. The structure morphism $v_0 : B \to D(M)$ is the image of the zero map $\Omega^1_{B/A} \to M$. If $v : B \to D(M)$ is any element of $\mathrm{Hom}_{B/A}(B, D(M))$, v and v_0 coincide on A and thus

$$\alpha : B \otimes_A B \to D(M) \qquad b \otimes b' \mapsto v_0(b)v(b')$$

defines an A-algebra homomorphism. Since the composition of v and v_0 with the augmentation $D(M) \to B$ is the identity,

$$\alpha(1 \otimes x - x \otimes 1) = 0 \oplus D(x)$$

and thus $\alpha(I) \in M$; furthermore $M^2 = 0$ implies $\alpha(I^2) = 0$. Therefore α induces a B-module map $\Omega^1_{B/A} = I/I^2 \to M$, and one checks easily that this an inverse to 2.1.2.4. ■

2.1.2.2 Corollary *If $B = A[X_1, \ldots, X_n]$ then $\Omega^1_{B/A}$ is the free B-module on $dX_1, \ldots, dX_n$.*

Proof. Homomorphisms $B \to D(M)$ are in a bijective correspondence with maps of the set $\{X_1, \ldots, X_n\}$ to $D(M)$, and the homomorphisms in $\mathrm{Hom}_{B/A}(B, D(M))$ correspond to those who take their values in $M \subset D(M)$. If $X_i \mapsto m_i \in M$, the corresponding map $\Omega^1_{B/A} \to M$ sends $dX_i \to m_i$, and for any choice of $m_i \in M$ there is exactly one such map. It follows that $\Omega^1_{B/A}$ is free on the dX_i. ■

2.1.2.3 Functoriality. The construction $\Omega^1_{B/A}$ is functorial in the following sense. If

$$\begin{tikzcd} A \arrow[r] \arrow[d] & A' \arrow[d] \\ B \arrow[r, "f"] & B' \end{tikzcd}$$

is a commutative diagram, the ring homomorphism $B \otimes_A B \to B' \otimes_{A'} B'$ induces a B-linear map $\Omega^1_{B/A} \to \Omega^1_{B'/A'}$, or equivalently a B'-linear map

$$B' \otimes_B \Omega^1_{B/A} \to \Omega^1_{B'/A'}. \tag{2.1.2.5}$$

which sends $1 \otimes db \mapsto df(b)$. An important special case is when $A' = A$ and $S \subset B$ is a multiplicative system and $B' = S^{-1}B$; then 2.1.2.5 is an isomorphism

$$S^{-1}\Omega^1_{B/A} \xrightarrow{\sim} \Omega^1_{S^{-1}B/A}. \tag{2.1.2.6}$$

If $S \subset A$ is a multiplicative system this leads to an isomorphism

$$S^{-1}\Omega^1_{B/A} \xrightarrow{\sim} \Omega^1_{S^{-1}B/S^{-1}A}. \tag{2.1.2.7}$$

Suppose now $A \to B \to C$ are homomorphisms of commutative rings. For any C-module M the sequence

$$0 \to \mathrm{Der}_B(C, M) \to \mathrm{Der}_A(C, M) \to \mathrm{Der}_A(B, M)$$

is easily seen to be exact. By proposition 2.1.2.1 we can rewrite this as

$$0 \to \mathrm{Hom}_C(\Omega^1_{C/B}, M) \to \mathrm{Hom}_C(\Omega^1_{C/A}, M) \to \mathrm{Hom}_C(C \otimes_B \Omega^1_{B/A}, M).$$

It is easily checked that this exact sequence is obtained by applying $\mathrm{Hom}_C(\ , M)$ to the exact sequence

$$C \otimes_B \Omega^1_{B/A} \to \Omega^1_{C/A} \to \Omega^1_{C/B} \to 0 \tag{2.1.2.8}$$

and that the maps in 2.1.2.8 are the ones induced by functoriality.

Suppose now $B \to C$ is surjective ring homomorphism with kernel J. Then $\mathrm{Der}_B(C, M) = 0$ for any C-module M and it follows that $\Omega^1_{C/B} = 0$. On the other hand if M is a C-module and $D : B \to M$ is an A-derivation, $D(J^2) = 0$. When viewed as a B-module, $JM = 0$ and from this one deduces that the map $J \to M$ induced by D is B-linear and vanishes on J^2 (use the Leibnitz rule in both cases). Therefore D induces a B-linear map $\mathrm{Der}_A(B, M) \to \mathrm{Hom}_B(J/J^2, M)$, and the resulting sequence

$$0 \to \mathrm{Der}_A(C, M) \to \mathrm{Der}_A(B, M) \to \mathrm{Hom}_B(J/J^2, M)$$

is exact. As before this comes from an exact sequence

$$J/J^2 \to C \otimes_B \Omega^1_{B/A} \to \Omega^1_{C/A} \to 0 \tag{2.1.2.9}$$

when $B \to C$ is a surjective A-algebra map with kernel J. The map $J/J^2 \to C \otimes_B \Omega^1_{B/A}$ sends $f \in J/J^2$ to $1 \otimes df$ (note that this is well-defined).

2.1.2.4 Computation of $\Omega^1_{B/A}$. The exact sequence 2.1.2.9 provides a useful method of computing $\Omega^1_{B/A}$ when B is realized as a quotient of a polynomial ring $C = A[X_1, \ldots, X_n]$ by an ideal $I = (f_1, \ldots, f_r)$. In fact $\Omega^1_{C/A}$ is the free C-module on $dX_1, \ldots, dX_n$ and therefore $\Omega^1_{B/A}$ is the quotient of the free B-module with basis $1 \otimes dX_1, \ldots, 1 \otimes dX_n$ by the submodule generated by $1 \otimes df_1, \ldots, 1 \otimes df_r$. The next lemma is a simple example of this procedure, which we will use repeatedly is the following:

2.1.2.5 Lemma *Suppose A is a commutative ring and $B = A[X]/(f)$ where $f \in A[X]$ is a monic irreducible polynomial. If $x \in B$ is the image of $X \in A[X]$ in B then $\Omega^1_{B/A} \simeq B/(f'(x))$.*

Proof. We use the exact sequence

$$(f)/(f)^2 \to B \otimes_{A[X]} \Omega^1_{A[X]/A} \to \Omega^1_{B/A} \to 0$$

and recall that $\Omega^1_{A[X]/A}$ is the free $A[X]$-module on dX. Therefore $B \otimes_{A[X]} \Omega^1_{A[X]/A}$ a free B-module of rank one, and we may write any element of it as $b \otimes dX$. Then the image of $f \in (f)$ in $B \otimes_{A[X]} \Omega^1_{A[X]/A}$ is

$$1 \otimes df = 1 \otimes f'(X)dX = f'(x) \otimes dX$$

and the assertion follows. ■

2.1.2.6 Proposition *Suppose L/K is a finite extension of fields. Then $\Omega^1_{L/K} = 0$ if and only if L/K is separable.*

Proof. Suppose $L = K[x]$ is a simple extension and f is the minimal polynomial of x. The lemma shows that $\Omega^1_{L/K} \simeq L/(f'(x))$.

If L/K is separable it is simple, so that $f'(x) \neq 0$ and $\Omega^1_{L/K} = 0$. If L/K is purely inseparable of degree p it is also simple, but this time $f'(x) = 0$ and $\Omega^1_{L/K}$ has dimension one. Finally if L/K is inseparable of any degree there is an intermediate extension $K \subset K' \subset L$ such that L/K' is purely inseparable of degree p. We can then apply the exact sequence 2.1.2.8 to $K \to K' \to L$ and we see that $\Omega^1_{L/K'}$ is a quotient of $\Omega^1_{L/K}$. It follows that $\Omega^1_{L/K} \neq 0$. ■

2.1.2.7 Corollary *Suppose A is an integral domain and B is a finite A-algebra that is also an integral domain. Let K and L be the fraction fields of A and B respectively. The extension L/K is separable if and only if $\Omega^1_{B/A}$ is a torsion B-module.*

Proof. Since B is a finite A-algebra, L/K is a finite extension and thus L/K is separable if and only if $\Omega^1_{L/K} = 0$. To conclude it suffices to observe that $\Omega^1_{L/K} = L \otimes_B \Omega^1_{B/A}$. ■

2.1.2.8 Proposition *Suppose $A \to B$ is a local homomorphism of discrete valuation rings making B a finite A-module. The residual extension $k \to k_B$ of $A \to B$ is residually separable if and only if $\Omega^1_{B/A}$ is generated by $d\pi$ for some uniformizer π of B. If so, it is generated by $d\pi$ for any uniformizer π.*

Proof. We first remark that $\Omega^1_{k_B/k} \simeq \Omega^1_{k_B/A}$. If $\pi \in B$ is any uniformizer, $k_B \simeq B/\pi B$ and the exact sequence 2.1.2.9 with $J = (\pi)$ can be written

$$\pi B/\pi^2 B \xrightarrow{d} k_B \otimes_B \Omega^1_{B/A} \to \Omega^1_{k_B/k} \to 0.$$

If $A \to B$ is residually separable, $\Omega^1_{k_B/k} = 0$. Then $\pi B/\pi^2 B \to k_B \otimes_B \Omega^1_{B/A}$ is surjective, and $\Omega^1_{B/A}$ is generated by $d\pi$ by Nakayama. Conversely if π is a uniformizer and $d\pi$ generates $\Omega^1_{B/A}$, $\pi B/\pi^2 B \to k_B \otimes_B \Omega^1_{B/A}$ is surjective. Therefore $\Omega^1_{k_B/k} = 0$ and $A \to B$ is residually separable. ■

2.1.3 The Different. Suppose A is a commutative ring and B is a commutative A-algebra. The *different* of B/A is the annihilator of $\Omega^1_{B/A}$:

$$\mathcal{D}_{B/A} = \mathrm{Ann}_B(\Omega^1_{B/A}). \tag{2.1.3.1}$$

2.1.3.1 Proposition *Suppose A is an integral domain with fraction field K, B is a finitely generated A-algebra that is also an integral domain, and L is the fraction field of B. If L/K is finite, then L/K is separable if and only if $\mathcal{D}_{B/A} \neq 0$.*

Proof. Since B is finitely generated, $\Omega^1_{B/A}$ is a finitely generated B-module, say with generators $dx_1, \ldots, dx_s$. If L/K is separable, $\Omega^1_{B/A}$ is torsion, and the annihilator of a finitely generated torsion module over an integral domain is nonzero. If L/K is not separable we have seen that $L \otimes_B \Omega^1_{B/A} \neq 0$. If $\omega \in \Omega^1_{B/A}$ is such that $1 \otimes \omega \neq 0$ in $L \otimes_B \Omega^1_{B/A}$ then $b\omega = 0$ implies $b = 0$. Consequently $\mathcal{D}_{B/A} = 0$. ■

2.1.3.2 Proposition *Suppose A is a commutative ring and $B = A[X]/(f)$ where $f \in A[X]$ is a monic irreducible polynomial. If $x \in B$ is the image of $X \in A[X]$ in B then $\mathcal{D}_{B/A} = (f'(x))$.*

Proof. This follows from lemma 2.1.2.5 and the definition. ■

2.1.3.3 Corollary *With the hypotheses of the proposition, $\Omega^1_{B/A}$ is a cyclic B-module.*

2.1.4 Nonarchimedean Fields. When L/K is a finite separable extension of nonarchimedean fields we will write $\mathcal{D}_{L/K}$ for $\mathcal{D}_{\mathcal{O}_L/\mathcal{O}_K}$. We will improve on the following lemma later:

2.1.4.1 Lemma *If L/K is a totally ramiified extension of discretely valued nonarchimedean fields then*

$$v_L(\mathcal{D}_{L/K}) \geq e_{L/K} - 1 \tag{2.1.4.1}$$

with equality if and only if L/K is tamely ramified.

Proof. We know $\mathcal{O}_L = \mathcal{O}_K[x]$ where x is a root of some Eisenstein polynomial

$$f(X) = X^e + a_1 X^{e-1} + \cdots + a_e.$$

Then $\mathcal{D}_{L/K}$ is generated by

$$f'(x) = ex^{e-1} + \cdots + a_{e-1}.$$

Since $v_L((i-1)a_i e^{i-1}) \geq e$,

$$v_L(f'(x)) \geq v_L(ex^{e-1}) \geq e - 1$$

with equality only when $v_L(e) = 0$, i.e. when L/K is tamely ramified. ■

2.1.4.2 Theorem *For any finite extension L/K of discretely valued nonarchimedean fields the following are equivalent:*

(i). L/K is unramified.

(ii). $\Omega^1_{\mathcal{O}_L/\mathcal{O}_K} = 0$.

(iii). $\mathcal{D}_{L/K}$ is the unit ideal.

Proof. The last two statements are clearly equivalent. We will show that the first two are as well. Suppose first that L/K is unramified. Then L/K is residually separable, i.e. $\mathcal{O}_K \to \mathcal{O}_L$ is a finite residually separable extension of discrete valuation rings. By proposition 2.1.2.8, $\Omega^1_{\mathcal{O}_L/\mathcal{O}_K}$ is generated by $d\pi$ for any uniformizer π of L. Since L/K is unramified we may take $\pi \in K$, in which case $d\pi = 0$ and thus $\Omega^1_{\mathcal{O}_L/\mathcal{O}_K} = 0$.

Suppose conversely that $\Omega^1_{\mathcal{O}_L/\mathcal{O}_K} = 0$ and let ℓ/k be the residual extension. Since $\Omega^1_{\mathcal{O}_L/\mathcal{O}_K} \to \Omega^1_{\ell/\mathcal{O}_K} = \Omega^1_{\ell/k}$ is surjective, $\Omega^1_{\ell/k} = 0$ and $\mathcal{O}_K \to \mathcal{O}_L$ is residually separable. Let K'/K be the maximal unramified extension of K in L. Then $\Omega^1_{\mathcal{O}_L/\mathcal{O}'_K}$ is a quotient of $\Omega^1_{\mathcal{O}_L/\mathcal{O}_K} = 0$, and thus $\Omega^1_{\mathcal{O}_L/\mathcal{O}'_K} = 0$. By the lemma,

$$0 = v_L(\mathcal{D}_{L/K'}) \geq e_{L/K'} - 1 = [L : K'] - 1$$

from which we see that $K' = L$ and L/K is unramified. ■

2.1.4.3 Corollary *Suppose L/K is a residually separable finite extension of nonarchimedean fields. If K'/K is the maximal unramified extension of K in L, $\Omega^1_{L/K'} \simeq \Omega^1_{L/K}$ and $\mathcal{D}_{L/K'} = \mathcal{D}_{L/K}$.*

Proof. Apply the exact sequence 2.1.2.8 to $\mathcal{O}_K \to \mathcal{O}_{K'} \to \mathcal{O}_L$. ■

2.1.4.4 Theorem *For any residually separable finite extension of discretely valued nonarchimedean fields L/K,*

$$v_L(\mathcal{D}_{L/K}) \geq e_{L/K} - 1 \tag{2.1.4.2}$$

with equality if and only if L/K is tamely ramified.

Proof. This follows from corollary 2.1.4.3 and lemma 2.1.4.1. ■

We include the following for the sake of tradition; it will not really be used.

2.1.4.5 Proposition *Suppose E/L and L/K is are finite, residually separable extensions of nonarchimedean fields. Then*

$$\mathcal{D}_{E/K} = \mathcal{D}_{E/L}\mathcal{D}_{L/K}. \tag{2.1.4.3}$$

Proof. We can assume E/K is separable since otherwise both sides are 0. Since $\Omega^1_{E/K}$ is a cyclic $\mathcal{O}_E$-module it suffices to show that

$$v_E(\Omega^1_{\mathcal{O}_E/\mathcal{O}_K}) = v_E(\Omega^1_{\mathcal{O}_E/\mathcal{O}_L}) + v_E(\mathcal{O}_E \otimes_{\mathcal{O}_L} \Omega^1_{\mathcal{O}_L/\mathcal{O}_K}). \tag{2.1.4.4}$$

Find $x \in \mathcal{O}_L$ such that $\mathcal{O}_L = \mathcal{O}_K[x]$ and $y \in \mathcal{O}_E$ such that $\mathcal{O}_E = \mathcal{O}_L[y]$. Let f (resp. g) be the minimal polynomial of x over K (resp. y over L). There is a polynomial $h \in K[X, Y]$ such that $h(x, Y) = g(Y)$. Then $\mathcal{O}_E \simeq$

$\mathcal{O}_K[X,Y]/(f(X),h(X,Y))$, and applying the method of section 2.1.2.4 shows that $\Omega^1_{\mathcal{O}_E/\mathcal{O}_K}$ is the quotient of the free $\mathcal{O}_E$-module with basis $1\otimes dX$, $1\otimes dY$ by the submodule generated by $1\otimes df = f'(x)\otimes dX$ and $1\otimes dh = h_x(x,y)\otimes dX + h_y(x,y)\otimes dY$. Since $h_y(x,Y) = g'(Y)$, $1\otimes dh = h_x(x,y)\otimes dX + g'(y)\otimes dY$ and the length of $\Omega^1_{\mathcal{O}_E/\mathcal{O}_K}$ is $v_E(f'(x)g'(y))$, which is the right hand side of 2.1.4.4. ■

2.1.4.6 Corollary *With the notation of the proposition, the sequence*

$$0 \to \mathcal{O}_E \otimes_{\mathcal{O}_L} \Omega^1_{\mathcal{O}_L/\mathcal{O}_K} \to \Omega^1_{\mathcal{O}_E/\mathcal{O}_K} \to \Omega^1_{\mathcal{O}_E/\mathcal{O}_L} \to 0$$

is exact.

Proof. This is the exact sequence 2.1.2.8 except for the assertion of exactness at the first term. However if $\mathcal{O}_E \otimes_{\mathcal{O}_L} \Omega^1_{\mathcal{O}_L/\mathcal{O}_K} \to \Omega^1_{\mathcal{O}_E/\mathcal{O}_K}$ is not injective, the relation 2.1.4.4 would not hold. ■

In fact the exactness of this sequence is not evident from the proof of proposition 2.1.4.5. The calculation of $\Omega^1_{\mathcal{O}_E/\mathcal{O}_K}$ in the proof shows that the injectivity of $\mathcal{O}_E \otimes_{\mathcal{O}_L} \Omega^1_{\mathcal{O}_L/\mathcal{O}_K} \to \Omega^1_{\mathcal{O}_E/\mathcal{O}_K}$ is equivalent to $h_x(x,y)$ being a unit.

2.1.5 The Discriminant. If K is any valued field we denote by I_K the group of fractional ideals of K, i.e. $\mathcal{O}_K$-submodules of K that are free of rank one. When K is discretely valued, $I_K \simeq \mathbb{Z}$, the isomorphism being given by $(x) \mapsto v_K(x)$. When L/K is a finite extension of valued fields we extend the norm map $N_{L/K} : L^\times \to K^\times$ by

$$I = (x) \Rightarrow N_{L/K}(I) = (N_{L/K}(x)). \tag{2.1.5.1}$$

This is well-defined since the norm of a unit is a unit. Like the usual norm, the norm on fractional ideals is transitive for successive extensions.

If L/K is a finite separable extension of discretely valued fields the *discriminant* of L/K is the ideal

$$\mathfrak{d}_{L/K} = N_{L/K}(\mathcal{D}_{L/K}). \tag{2.1.5.2}$$

If L/K and E/L are both finite separable extensions of discretely valued fields, the transitivity formula 2.1.4.3 and the transitivity of the norm imply that

$$\mathfrak{d}_{E/K} = \mathfrak{d}_{L/K}^{[E:L]}\mathfrak{d}_{E/L}. \tag{2.1.5.3}$$

2.1.5.1 Example: cyclotomic fields. Recall the situation of Example 1.2.5.3: $\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p$ is the extension generated by a root ζ of the polynomial

$$f(X) = \frac{X^{p^n} - 1}{X^{p^{n-1}} - 1}$$

and $\eta = \zeta^{p^{n-1}}$. Since

$$f'(X) = \frac{p^n X^{p^n-1}}{X^{p^{n-1}}-1} - \frac{X^{p^n}-1}{(X^{p^{n-1}}-1)^2} p^{n-1} X^{p^{n-1}-1}$$

the different $\mathcal{D}_{\mathbb{Q}_p(\zeta)/\mathbb{Q}_p}$ is generated by $p^n/(\eta-1)$. If v is the normalized valuation of $\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p$, $v(p) = (p-1)p^{n-1}$ and $v(\eta-1) = p^{n-1}$, so that

$$v(\mathcal{D}_{\mathbb{Q}_p(\zeta)/\mathbb{Q}_p}) = (np-n-1)p^{n-1}. \tag{2.1.5.4}$$

From theorem 2.1.4.2 we deduce:

2.1.5.2 Proposition *A finite separable extension L/K of discretely valued nonarchimedean fields is unramified if and only if $\mathfrak{d}_{L/K} = (1)$.*

Suppose $L = K(x)$ for some $x \in \mathcal{O}_L$ such that $\mathcal{O}_L = \mathcal{O}_K[x]$. If f is the minimal polynomial of x over K then $\mathcal{D}_{L/K} = (f'(x))$ and therefore $fd_{L/K} = (N_{L/K}(f'(x)))$. If $x = x_1, \ldots, x_n$ are the conjugates of x in K^{alg} then $f(X) = \prod_i (X - x_i)$, and we find $f'(x) = \prod_{i>1}(x_1 - x_i)$, and

$$\mathfrak{d}_{L/K} = (D) \qquad D = \prod_{i \neq j} (x_i - x_j)^2. \tag{2.1.5.5}$$

The expression defining D is a symmetric polynomial in the x_i and can therefore be written as a polynomial in the coefficients of f.

The discriminant $\mathfrak{d}_{L/K}$ is an isomorphism invariant of the extension L/K. Using it we can show, for example that any local field K of characteristic $p > 0$ has infinitely many nonisomorphic separable extensions of degree p. It suffices to recall the Eisenstein polynomial

$$f_a(X) = X^p + aX + \pi \tag{2.1.5.6}$$

where π is a uniformizer of K. If $L = K(x)$ where x is a root of f_a, $f_a'(x) = a$ and thus $\mathfrak{d}_{L/K} = (a^p)$. Letting $a \to 0$ in K produces an infinite series of separable extensions of degree p with distinct discriminants, and thus mutually nonisomorphic. Note that the "limiting extension" in which $a = 0$ is inseparable.

This example shows how the proof of theorem 1.2.8.7 breaks down for a local field of characteristic $p > 0$. In the notation of the proof take $n = p$; then all points of X of the form $(0, \ldots, 0, u)$ correspond to inseparable polynomials. They have to be removed in order to use proposition 1.2.8.4, but this results in a noncompact set. Nonetheless the example suggests that the number of finite separable extensions of given degree will be finite if one bounds the discriminant away from zero, and in fact this is true:

2.1.5.3 Theorem *Let K be a local field of characteristic $p > 0$. For all positive integers n, m there are only finitely many separable extensions L/K such that $[L : K] = n$ and $v(\mathfrak{d}_{L/K}) \leq m$.*

Proof. We reuse the setup and notation of the proof if theorem 1.2.8.7. Since the quantity D in 2.1.5.5 is a polynomial function of the coefficients of f, the subset $Y \subset X$ defined by $v(D) \leq m$ is closed, and therefore compact. Since every polynomial corresponding to a point of Y is separable, the argument of theorem 1.2.8.7 can therefore be applied to Y, and the result follows. ■

2.1.6 The Trace form. The different is usually defined in terms of the trace form of the extension L/K. In this section we compare this definition with the one given above. We first recall part of the proof that a finite extension L/K of fields is separable if and only if the trace $\mathrm{Tr}_{L/K} : L \to K$ is not identically zero. When L/K is separable, say of degree n we may write $L = K(x)$. Then if f is the minimal polynomial of x,

$$\mathrm{Tr}_{L/K}(x^i/f'(x)) = \begin{cases} 0 & 0 \leq i < n-1 \\ 1 & i = n-1 \end{cases}. \tag{2.1.6.1}$$

This equality is most easily seen from the partial fraction expansion

$$\frac{1}{f(T)} = \sum_{1 \leq i \leq n} \frac{1}{f'(x_i)(T - x_i)} \tag{2.1.6.2}$$

in which $x_1, \ldots, x_n$ are the roots of f. If both sides are expanded in powers of $1/T$, the left hand side starts with $1/T^n$, while on the right hand side the coefficient of $1/T^i$ is $\mathrm{Tr}_{L/K}(x^{i-1}/f'(x))$. The formula 2.1.6.1 implies that the trace form $\langle x, y \rangle = \mathrm{Tr}_{L/K}(xy)$ is nondegenerate; we will repeat the argument below.

Suppose now L/K is a finite separable extension of nonarchimedean fields, and choose $x \in \mathcal{O}_L$ such that $\mathcal{O}_L = \mathcal{O}_K[x]$. Denote by $\mathcal{O}_L^\vee$ the set of $y \in L$ such that $\mathrm{Tr}_{L/K}(xy) \in \mathcal{O}_K$ for all $x \in \mathcal{O}_L$; since $\mathrm{Tr}_{L/K}$ is nondegenerate this is a fractional ideal of L, and thus free $\mathcal{O}_K$-submodule of L of rank $n = [L : K]$. In fact if we put $y_i = x^i/f'(x)$ for all $i \geq 0$, 2.1.6.1 implies first that $\mathrm{Tr}_{L/K}(x_i y_j) \in \mathcal{O}_K$ for all i, $j \geq 0$, and second that

$$\left(\mathrm{Tr}_{L/K}(x_i y_j)\right)_{0 \leq i,j < n} = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 1 & * \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 1 & \cdots & * & * \\ 1 & * & \cdots & * & * \end{pmatrix}$$

where the entries below the antidiagonal are in $\mathcal{O}_K$. Since this matrix has determinant ± 1 the y_i for $0 \leq i < n$ are a basis of $\mathcal{O}_L^\vee$. Since $\mathcal{D}_{L/K} = (f'(x))$, we have shown that

$$\mathcal{O}_L^\vee = \mathcal{D}_{L/K}^{-1}. \tag{2.1.6.3}$$

If $\mathfrak{a}$ is any fractional ideal of L, the K-linearity of $\mathrm{Tr}_{L/K}$ shows that $\mathrm{Tr}_{L/K}(\mathfrak{a})$ is a fractional ideal of K.

2.1.6.1 Proposition *For any fractional ideals* $\mathfrak{a} \subseteq \mathcal{O}_L$, $\mathfrak{b} \subseteq \mathcal{O}_K$, $\mathrm{Tr}_{L/K}(\mathfrak{a}) \subseteq \mathfrak{b}$ *if and only if* $\mathfrak{a} \subseteq \mathfrak{b}\mathcal{D}_{L/K}^{-1}$.

Proof. By 2.1.6.3 and the K-linearity of $\mathrm{Tr}_{L/K}$,

$$\begin{aligned}
\mathrm{Tr}_{L/K}(\mathfrak{a}) \subseteq \mathfrak{b} &\iff \mathfrak{b}^{-1}\mathrm{Tr}_{L/K}(\mathfrak{a}) \subseteq \mathcal{O}_K \\
&\iff \mathrm{Tr}_{L/K}(\mathfrak{b}^{-1}\mathfrak{a}) \subseteq \mathcal{O}_K \\
&\iff \mathfrak{b}^{-1}\mathfrak{a} \subseteq \mathcal{O}_K^{\vee} = \mathcal{D}_{L/K}^{-1} \\
&\iff \mathfrak{a} \subseteq \mathfrak{b}\mathcal{D}_{L/K}^{-1}.
\end{aligned}$$

■

2.1.7 Exercises.

2.1.7.1 Suppose L/K is a finite separable extension. (i) Show that $L \otimes_K L$ is isomorphic to a direct sum of fields. (ii) Use this to give another proof that $\Omega^1_{L/K} = 0$ when L/K is finite and separable.

2.1.7.2 Suppose L/K is a finite purely inseparable extension. (i) Show that the kernel of the multiplication map $L \otimes_K L \to L$ is a nonzero nilpotent maximal ideal of $L \otimes_K L$. In particular $L \otimes_K L$ is an Artin local ring. (ii) Deduce from this that $\Omega^1_{L/K} \neq 0$. (iii) Use the last result to show that $\Omega^1_{L/K} \neq 0$ for any finite inseparable extension.

2.1.7.3 Suppose A is a commutative ring and $\{B_i\}$ is a filtered system of commutative A-algebras. Show that if $B = \varinjlim_i B_i$ then

$$\Omega^1_{B/A} \simeq \varinjlim_i \Omega^1_{B_i/A}.$$

Deduce from this that if L/K is a separable algebraic extension then $\Omega^1_{L/K} = 0$.

2.1.7.4 Suppose A is a commutative ring of characteristic $p > 0$ and denote by A^{perf} the perfection of A. Show that $\Omega^1_{A^{perf}/A} = 0$. Compare with exercise 2.1.7.2.

2.1.7.5 Suppose K is a field of characteristic $p > 0$ and L/K is an extension such that $L^p \subseteq K$. A set $S \subset L$ is a *p-base* of L/K if L is generated as an K-vector space by monomials of the form $\prod_{x \in S} x^{n(x)}$ where $n(x) = 0$ for all but finitely many $x \in S$ and $0 \leq n(x) < p$ for all x. Show that S is a p-base if and only if the dx for all $x \in S$ form a basis of the L-vector space $\Omega^1_{L/K}$. (use exercise 2.1.7.2 to show sufficiency).

2.1.7.6 Suppose K and L are as in the last problem A subset $S \subset L$ is *p-independent* if the monomials $\prod_{x \in S} x^{n(x)}$ are linearly independent over K. (i)

Show that a singleton set $S = \{x\}$ is p-independent if and only if $x \notin K$. (ii) Show that any p-indepedent set extends to a p-base.

2.1.7.7 Let K be a nonarchimedean field and $f \in \mathcal{O}_K[X]$ is irreducible and separable. If x is a root of f in some algebraic closure of K and $L = K(x)$, show that the constant ϵ in proposition 1.2.8.4 can be taken to be $|D|^{1/2}$ where $\mathfrak{d}_{L/K} = (D)$.

2.2 The Ramification Filtration

For the rest of this chapter we assume unless otherwise stated that all fields are nonarchimedean with *separable* residue field and all field extensions are separable (they are also residually separable by the previous hypothesis.

2.2.1 The Inertia Group. Suppose first that L/K is a finite Galois extension with residual extension k_L/k. Then k_L/k is a Galois extension too, since a k-embedding of k_L into k^{alg} must lift to a K-embedding of L into K^{alg} by theorem 1.2.4.2. But any two K-embeddings $L \to K^{alg}$ have the same image, so the same must be true for any two k-embeddings of k_L into k^{alg}. By corollary 1.2.4.4 any element of $\mathrm{Gal}(k_L/k)$ lifts to a unique element of $\mathrm{Gal}(L/K)$, or in other words the natural homomorphism $\mathrm{Gal}(L/K) \to \mathrm{Gal}(k_L/k)$ is an isomorphism.

If L/K is any finite Galois extension, the maximal unramified extension F of K in L is stable under the action of $\mathrm{Gal}(L/k)$ since F is the unique unramified extension of K in L with residue field k_L. The argument of the last paragraph applies to F/K, resulting in an isomorphism $\mathrm{Gal}(F/K) \to \mathrm{Gal}(k_L/k)$. By Galois theory this produces a surjective homomorphism $\mathrm{Gal}(L/K) \to \mathrm{Gal}(k_L/k)$ whose kernel is the *inertia group* $I_{L/K}$ of the extension L/K.

Finally if L/K is any Galois extension of K (not necessarily finite) L is the union of its subfields L'/K that are finite and Galois over K, and then $\mathrm{Gal}(L/K) = \varprojlim_{L'} \mathrm{Gal}(L'/K)$ where L' runs over the set of such subfields. One can then show that the inverse limit $\mathrm{Gal}(L/K) \to \mathrm{Gal}(k_L/k)$ of the homomorphisms $\mathrm{Gal}(L'/K) \to \mathrm{Gal}(k_{L'}/k)$ is still surjective and its kernel $I_{L/K}$ is the projective limit of the $I_{L'/K}$. In the special case $L = K^{sep}$ we write $I_{K^{sep}/K} = I_K$, so that there is an exact sequence

$$0 \to I_K \to \mathrm{Gal}(K^{sep}/K) \to \mathrm{Gal}(k^{alg}/k) \to 0 \tag{2.2.1.1}$$

that is the projective limit of the exact sequences

$$0 \to I_{L/K} \to \mathrm{Gal}(L/K) \to \mathrm{Gal}(k_L/k) \to 0 \tag{2.2.1.2}$$

for all finite Galois L/K.

2.2.2 The ramification groups. When L/K is a finite Galois extension the inertia subgroup is the first term in a series of subgroups of $G = \mathrm{Gal}(L/K)$,

the *ramification filtration*. Since the action of G stabilizes $\mathcal{O}_L$ and $\mathfrak{m}_L$ it stabilizes the $\mathfrak{m}_L^i$ for all $i \geq 0$. Thus G acts on $\mathcal{O}_L/\mathfrak{m}_L^{n+1}$ for all $n \geq 0$ and we define

$$G_n = \mathrm{Ker}(G \to \mathrm{Aut}(\mathcal{O}_L/\mathfrak{m}_L^{n+1}). \tag{2.2.2.1}$$

The inertia subgroup is G_0, and the G_n are all normal subgroups of G. They are variously called the *ramification groups* or *higher inertia groups*. The integers n such that $G_n \neq G_{n+1}$ are the *breaks* of the ramification filtration.

Evidently $s \in G_n$ if and only if $v_L(s(a) - a) \geq n + 1$ for all $a \in \mathcal{O}_K$. Since L/K is residually separable we have $\mathcal{O}_L = \mathcal{O}_K[x]$ for some $x \in \mathcal{O}_L$. It is then clear that $s \in G_n$ if and only if $v_L(s(x) - x) \geq n + 1$. We are then led to introduce the function

$$i_G(s) = v_L(s(x) - x) \tag{2.2.2.2}$$

where $x \in \mathcal{O}_L$ is any element such that $\mathcal{O}_L = \mathcal{O}_K[x]$. Note that $i_G(1) = \infty$ by definition. It is clear from the above that the right hand side of 2.2.2.2 is independent of the choice of x satisfying this condition, and in fact that

$$s \in G_n \iff i_G(s) \geq n + 1. \tag{2.2.2.3}$$

From this we see that

$$G_n = 1 \quad \text{for any} \quad n \geq \max_{s \neq 1} i_G(s). \tag{2.2.2.4}$$

Since $t(x)$ may be used in place of x for any $t \in G$,

$$i_G(tst^{-1}) = i_G(s) \tag{2.2.2.5}$$

for all s, $t \in G$. Applying the nonarchimedean triangle equality to $st(x) - x = (st(x) - s(x)) + (s(x) - x)$ shows that

$$i_G(st) \geq \min(i_G(s), i_G(t)) \quad \text{with equality if} \quad i_G(s) \neq i_G(t). \tag{2.2.2.6}$$

If $H \subseteq G$ is a subgroup corresponding to the field $F \subseteq L$ then $\mathcal{O}_L = \mathcal{O}_F[x]$, and it follows that

$$H_n = H \cap G_n \quad \text{and} \quad i_H(s) = i_G(s). \tag{2.2.2.7}$$

The ramification filtration of a quotient of G is more problematic and will be dealt with later.

2.2.3 The different. We saw earlier that that $v_L(\mathcal{D}_{L/K})$ is bounded below by $e_{L/K} - 1$. We can get an exact formula for $v_L(\mathcal{D}_{L/K})$ using the ramification filtration. Recall first that if $\mathcal{O}_L = \mathcal{O}_K[x]$ and f is the minimal polynomial of x then $\mathcal{D}_{L/K} = (f'(x))$. Now the conjugates of x over K are the $s(x)$ for all $s \in G$, so $f(X) = \prod_{s \in G}(X - s(x))$ and then

$$f'(x) = \prod_{s \neq 1}(x - s(x)).$$

It follows that

$$v_L(\mathcal{D}_{L/K}) = \sum_{s \neq 1} i_G(s). \tag{2.2.3.1}$$

Now $i_G(s)$ has the value n on the set $G_{n-1} \setminus G_n$, so the sum on the right hand side of 2.2.3.1 is

$$\sum_{n \geq 0} n(|G_{n-1}| - |G_n|) = \sum_{n \geq 0} n(r_{n-1} - r_n)$$

if we set $r_n = |G_n| - 1$ (note that almost all terms of the sum are zero). But the sum on the right hand side above collapses to $\sum_{n \geq 0} r_n$, so

$$v_L(\mathcal{D}_{L/K}) = \sum_{n \geq 0} (|G_n| - 1). \tag{2.2.3.2}$$

Since the inertia group is G_0, $|G_0| = e_{L/K}$ and thus 2.2.3.2 strengthens theorem 2.1.4.4 in the present case.

2.2.3.1 Example: cyclotomic fields again. Picking up from examples 1.2.5.3 and 2.1.5.1, we first identify $G = \mathrm{Gal}(\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p$ with $(\mathbb{Z}/p^n\mathbb{Z})^\times$, where the $a \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ acts as $\zeta \mapsto \zeta^a$. If v is the normalized valuation on $\mathbb{Q}_p(\mu_{p^n})$ then

$$i_G(a) = v(\zeta^a - \zeta) = v(\zeta^{a-1} - 1).$$

Denote by $U^i \subseteq (\mathbb{Z}/p^n\mathbb{Z})^\times$ the set of $u \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ congruent to 1 modulo p^i. If $a \in U^i \setminus U^{i+1}$, ζ^{a-1} is a primitive p^{n-i}th root of 1, and

$$v_p(\zeta^{a-1} - 1) = \frac{1}{(p-1)p^{n-i-1}}$$

where v_p is the extension to $\mathbb{Q}_p(\mu_{p^n})$of the normalized valuation of $\mathbb{Q}_p$. Since $v(x) = (p-1)p^{n-1}v_p(x)$ for any $x \in \mathbb{Q}_p(\mu_{p^n})$, $i_G(a) = p^i$ and the ramification filtration of G is

$$\begin{aligned} G_0 &= G \\ G_1 = \cdots = G_{p-1} &= U^1 \\ G_p = \cdots = G_{p^2-1} &= U^2 \\ &\vdots \\ G_{p^{n-1}} &= U^n = 1. \end{aligned} \tag{2.2.3.3}$$

Since $|U^i| = p^{n-i}$ the right hand side of equation 2.2.3.2 is

$$\begin{aligned} &(p-1)p^{n-1} - 1 + \sum_{0<i<n} (p^i - p^{i-1})(p^{n-i} - 1) \\ &\quad = (p-1)p^{n-1} - 1 + \sum_{0<i<n} (p^n - p^{n-1} - p^i + p^{i-1}) \\ &\quad = (p-1)p^{n-1} - 1 + (n-1)(p-1)p^{n-1} - p^{n-1} + 1 \\ &\quad = (np - n - 1)p^{n-1} \end{aligned}$$

which agrees with our earlier result 2.1.5.4 for the different of $\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p$.

2.2.4 The quotients G_n/G_{n+1}. We may apply the equality 2.2.2.7 to the case where $H = G_0$ is the inertia subgroup, and $K' = F$ is the maximal unramified extension of K in L. Then $\mathcal{O}_L = \mathcal{O}_F[\pi]$ where π is any uniformizer of L. The formula for i_G then yields

$$i_G(s) = v_L(s(\pi) - \pi) = 1 + v_L(s(\pi)/\pi - 1)$$

and 2.2.2.3 then shows that for $s \in G_0$,

$$s \in G_n \iff \frac{s(\pi)}{\pi} \equiv 1 \mod \pi^n. \tag{2.2.4.1}$$

We are therefore led to study the filtration $U^n \subset \mathcal{O}_L^\times$ defined by $U^0 = \mathcal{O}_L^\times$ and

$$U^n = 1 + (\pi^n) \subseteq \mathcal{O}_L^\times \quad \text{for} \quad n > 0. \tag{2.2.4.2}$$

Evidently

$$U^0/U^1 \simeq k_L^\times \tag{2.2.4.3}$$

and

$$U^n/U^{n+1} \simeq k_L \quad \text{for} \quad n > 0 \tag{2.2.4.4}$$

where the latter isomorphism identifies the class of $1 + \pi^n x$ with the class of x in k_L (the reader to whom this is new should check these assertions!)

From 2.2.4.1 we see that for $n \geq 0$ there is a map

$$\theta_n : G_n/G_{n+1} \to U^n/U^{n+1} \tag{2.2.4.5}$$

which to $s \in G_n$ assigns the class of $s(\pi)/\pi$ in U^n. This map is independent of the choice of π: in π' is another uniformizer, $\pi' = u\pi$ with $u \in \mathcal{O}_L^\times$. Then if $s \in G_n$, $s(u) \equiv u \mod \pi^{n+1}$ and therefore $s(u)/u \equiv 1 \mod \pi^{n+1}$. Consequently

$$\frac{s(\pi')}{\pi'} = \frac{s(\pi)}{\pi}\frac{s(u)}{u} \equiv \frac{s(\pi)}{\pi} \mod \pi^{n+1}$$

and the assertion follows.

2.2.4.1 Lemma *The map 2.2.4.5 is an injective homomorphism.*

Proof. For $s, t \in G_n$, $t(\pi)$ is a uniformizer and thus

$$\frac{st(\pi)}{\pi} = \frac{st(\pi)}{t(\pi)}\frac{t(\pi)}{\pi} \equiv \frac{s(\pi)}{\pi}\frac{t(\pi)}{\pi} \mod \pi^{n+1}$$

by the previous discussion. Then θ_n is a homomorphism, and its kernel is clearly trivial. ■

2.2.4.2 Proposition *Suppose K is a discretely valued nonarchimedean field of equicharacteristic 0. If L/K is a finite Galois extension with group G then $G_1 = 1$ and G_0/G_1 is cyclic. In particular if the residue field is algebraically closed, G is cyclic.*

Proof. If the residual extension is k_L/k we know that G_0/G_1 is isomorphic to a subgroup of $k_L^\times$, and a finite subgroup of the mulitiplicative group of a field is cyclic. For $n > 0$, G_n/G_{n+1} is isomorphic to a subgroup of the additive group k, which has no elements of finite order; therefore $G_n/G_{n+1} = 1$ for all $n > 0$ and thus $G_1 = 1$. The last statement is clear since G/G_0 is the Galois group of the residual extension. ■

2.2.4.3 Corollary *If $K = k((T))$ is a discretely valued nonarchimedean field of equicharacteristic 0 with algebraically closed residue field, the algebraic closure of K is the union of the $K(T^{1/n})$ for all $n > 0$.*

Proof. The proposition shows that any finite extension of K is cyclic. By Kummer theory a cyclic extension of degree n is generated by a root of $X^n - a$, with the distinct extensions corresponding to the nontrivial classes in $K^\times/K^{\times n}$. Since the residue field is algebraically closed, the latter group is cyclic of order n, generated by the class of $T \in K^\times$. ■

2.2.4.4 Proposition *Suppose K is a discretely valued nonarchimedean field with residue field of characteristic $p > 0$. If L/K is a finite Galois extension with group G then G_0/G_1 is cyclic, G_1 is a p-group and $G_0 \simeq G_1 \rtimes (G_0/G_1)$.*

Proof. As in the last proposition G_0/G_1 is isomorphic to a subgroup of $k_L^\times$, and in this case a finite subgroup of $k_L^\times$ cannot have order divisible by p. Similarly for $n > 0$, G_n/G_{n+1} is isomorphic to a finite subgroup of the additive group k_L, and in this case every nonidentity element of k_L has order p. Thus G_n/G_{n+1} is an elementary p-group for $n > 0$, and G_1 is a p-group.

If $e = |G_0/G_1$, $p^n \equiv 1 \mod e$ for some n, and by replacing n by a multiple we may assume that $|G_0|$ divides ep^n. Choose a $y \in G_0$ whose image in G_0/G_1 is a generator. Then $x = y^{p^n}$ satisfies $x^e = y^{ep^n} = 1$. On the other hand the image of x in G_0/G_1 has order e since p^n is relatively prime to e. Therefore the subgroup generated by x maps isomorphically to G_0/G_1. ■

2.2.4.5 Corollary *If L/K is a Galois extension of local fields, the Galois group is solvable.*

Proof. We already know that the inertia group G_0 is solvable, and G/G_0 is isomorphic the the Galois group of the residual extension. Since the latter is an extension of finite fields, G/G_0 is cyclic. ■

2.3 Herbrand's Theorem

Suppose now $H \subseteq G$ is a normal subgroup corresponding to a normal extension F of K in L. Our aim is to relate the ramification filtration of G with that of the quotient G/H.

2.3.1 The Herbrand function. If $u \geq -1$ is real we define

$$G_u = G_n \quad n = \lceil u \rceil \tag{2.3.1.1}$$

where $\lceil u \rceil$ is the least integer not less than u. For $-1 \leq u \leq 0$ we define $[G_0 : G_u] = [G_u : G_0]^{-1}$ (it equals 1, except for $u = -1$), so that $[G_0 : G_u]$ is piecwise constant function of u for $u \geq -1$. We next define

$$\varphi_{L/K}(u) = \int_0^u \frac{dt}{[G_0 : G_t]}.g \tag{2.3.1.2}$$

Because of our definition of $[G_0 : G_t]$ for $-1 \leq t \leq 0$ we have $\varphi_{L/K}(u) = u$ in that interval. We will write $\varphi(u)$ for $\varphi_{L/K}(u)$ if the extension L/K is understood. The following should be clear:

2.3.1.1 Lemma *The function $\varphi_{L/K}(u)$ is the unique real-valued function on $[-1, \infty)$ such that*

(i). $\varphi_{L/K}(u)$ is continuous and piecewise linear for all $u \geq -1$;

(ii). $\varphi_{L/K}(u)$ is differentiable for all nonintegral u and

$$\varphi_{L/K}(u)' = \frac{1}{[G_0 : G_u]}.$$

(iii). $\varphi_{L/K}(0) = 0$

The equality

$$\varphi_{L/K}(u) = \frac{1}{|G_0|}\left(\sum_{s \in G_0} \min(i_G(s), u+1)\right) - 1 \tag{2.3.1.3}$$

follows from the lemma. In fact the right hand side clearly satisfies (i) and (iii). If $m < u < m+1$, the derivative of the right hand side is the number of $s \in G_0$ such that $i_G(s) \geq m+2$, divided by $|G_0|$. This is $[G_0 : G_{m+1}]^{-1} = [G_0 : G_u]^{-1}$, so (ii) holds as well.

2.3.2 The upper numbering. Clearly $\varphi_{L/K}(t)$ is an increasing function of u and we denote the inverse function by $\psi_{L/K}(t)$. The *upper numbering* of the ramification groups is defined by

$$G^v = G_{\psi(v)} \quad \text{or equivalently} \quad G^{\varphi(u)} = G_u. \tag{2.3.2.1}$$

It is clear that $\psi_{L/K}$ is characterized by the following properties: it is continuous, piecewise linear, $\psi_{L/K}(0) = 0$, and $\psi_{L/K}$ is differentiable in any interval of the form $(\varphi_{L/K}(n), \varphi_{L/K}(n+1))$, the derivative being $[G_0 : G_n]$. From this we get the formula

$$\psi_{L/K}(u) = \int_0^u [G^0 : G^v] dv \tag{2.3.2.2}$$

(note the upper numbering in the integral).

Our goal in this section is an analogue of the formula 2.2.2.7 relative to the quotient map $G \to G/H$, in which the upper numbering replaces the original "lower numbering."

2.3.2.1 Proposition *For all $\sigma \in G/H$,*

$$i_{G/H}(\sigma) = \frac{1}{e_{L/F}} \sum_{s \in \sigma} i_G(s). \tag{2.3.2.3}$$

Proof. (Tate) The sum is over elements of the coset $\sigma \in G/H$. If $\sigma = 1$, both sides are $+\infty$, so we assume $\sigma \neq 1$ and pick an $s \in G$ mapping to σ. Choose $x \in \mathcal{O}_L$, $y \in \mathcal{O}_F$ such that $\mathcal{O}_L = \mathcal{O}_K[x]$, $\mathcal{O}_F = \mathcal{O}_K[y]$. If we set

$$a = s(y) - y, \qquad b = \prod_{t \in H} (st(x) - x)$$

then

$$v_L(a) = e_{L/F} i_{G/H}(\sigma), \qquad v_L(b) = \sum_{s \in \sigma} i_G(s)$$

and so it suffices to show that $v_L(a) = v_L(b)$, i.e a and b generate the same ideal of $\mathcal{O}_L$.

The minimal polynomial of x over F is

$$f(X) = \prod_{t \in H} (X - t(x))$$

and thus if we write ${}^s f$ for the result of applying s to the coefficients of f,

$${}^s f(x) = \prod_{t \in H} (x - st(x)) = \pm b.$$

Since y generates $\mathcal{O}_F$, the coefficients of ${}^s f(X) - f(X)$ are divisible by $s(y) - y$. Then ${}^s f(x) = {}^s f(x) - f(x)$ is divisible by $s(y) - y$, or in other words a divides b.

There is a $g \in \mathcal{O}_K[X]$ such that $y = g(x)$. Then x is a root of $g(X) - y$, which must therefore be divisible by f:

$$g(X) - y = f(X)h(X).$$

Apply s to this equation and then substitute x for X; the result is

$$y - s(y) = {}^s f(x) {}^s h(x)$$

and it follows that b divides a. ■

For $\sigma \in G/H$ we define

$$j(\sigma) = \max_{s \in \sigma} i_G(s). \tag{2.3.2.4}$$

If the maximum in 2.3.2.4 is acheived for $s \in \sigma$ the triangle inequality 2.2.2.6 shows that

$$i_G(st) = \min(i_G(s), i_G(t)) = \min(j(\sigma), i_H(t)) \quad \text{if} \quad i_G(s) = \max_{t \in H} i_G(st). \tag{2.3.2.5}$$

From this we see that

$$\sigma \in G_n H/H \iff j(\sigma) \geq n+1 \tag{2.3.2.6}$$

and thus j plays the same role for $G_n H/H$ as $i_{G/H}$ does for $(G/H)_n$.

2.3.2.2 Lemma

$$i_{G/H}(\sigma) - 1 = \varphi_{L/F}(j(\sigma) - 1) \tag{2.3.2.7}$$

Proof. Let $s \in G$ be the element of σ for which $i_G(s)$ has the maximum value $j(\sigma)$, and rewrite the equality 2.3.2.3 as

$$i_{G/H}(\sigma) = \frac{1}{e_{L/F}} \sum_{t \in H} i_G(st). \tag{2.3.2.8}$$

By 2.3.2.5 this is the same as

$$i_{G/H}(\sigma) = \frac{1}{|H_0|} \sum_{t \in H} \min(j(\sigma), i_H(t)) \tag{2.3.2.9}$$

since $e_{L/F} = |H_0|$. The equality 2.3.1.3 applied to L/F and H then yields

$$i_{G/H}(\sigma) = \varphi_{L/F}(j(\sigma) - 1) + 1 \tag{2.3.2.10}$$

and we are done. ■

2.3.2.3 Theorem *(Herbrand) If $v = \varphi_{L/F}(u)$ then*

$$(G/H)_v = G_u H/H \simeq G_u/H_u. \tag{2.3.2.11}$$

Proof. Combining 2.3.2.6 and 2.3.2.7 we see that

$$\begin{aligned} \sigma \in G_u H/H &\iff j(\sigma) \geq u+1 \\ &\iff \varphi_{L/F}(j(\sigma) - 1) \geq \varphi_{L/F}(u) = v \\ &\iff i_{G/H}(\sigma) - 1 \geq v \\ &\iff \sigma \in (G/H)_v \end{aligned}$$

whence the equality on the left. The isomorphism on the right follows from this and 2.2.2.7. ■

2.3.2.4 Proposition *If $H \subseteq G$ is a normal subgroup corresponding to the Galois extension F/K,*

$$\varphi_{L/K} = \varphi_{F/K} \circ \varphi_{L/F}, \quad \psi_{L/K} = \psi_{L/F} \circ \psi_{F/K}. \tag{2.3.2.12}$$

Proof. If we set $v = \varphi_{L/F}(u)$, the derivative of $\varphi_{F/K}(\varphi_{L/F}(u))$ is

$$\varphi'_{F/K}(v)\varphi'_{L/F}(u) = \frac{|(G/H)_v|}{e_{F/K}}\frac{|H_u|}{e_{L/F}}.$$

Herbrand's theorem shows that this is the same as

$$\frac{|(G_u/H_u)|}{e_{F/K}}\frac{|H_u|}{e_{L/F}} = \frac{|G_u|}{e_{L/K}} = \varphi'_{L/K}(u)$$

and the characterization of the φ function (lemma 2.3.1.1) then yields the first equality in the proposition. The second formula follows from the first. ■

The formula

$$G^v H/H = (G/H)^v \tag{2.3.2.13}$$

follows from Herbrand's theorem 2.3.2.3 and proposition 2.3.2.4. In fact

$$(G/H)^v = (G/H)_{\psi_{F/K}(v)}$$

by definition, and this is the same as

$$G_{\psi_{L/F}(\psi_{F/K}(v))}H/H = G_{\psi_{L/K}(v)}H = G^v H/H.$$

The equality 2.3.2.13 shows that the upper numbering extends to a filtration on the Galois group of an *infinite* Galois extensions. If we denote the Galois group of a finite extension L/K by G_L, then for successive Galois extensions L/K, E/L the canonical projection $G_E \to G_L$ maps $G_E^v \to G_L^v$ surjectively. Thus if L/K is a (possibly infinite) algebraic extension with Galois group G,

$$G = \varprojlim_L G_L$$

where L runs through the set of finite Galois extensions of K in L, and $G^v \subseteq G$ is defined by

$$G^v = \varprojlim_L G_L^v. \tag{2.3.2.14}$$

This filtration is "left continuous" in the sense that

$$G^v = \bigcap_{w<v} G^w. \tag{2.3.2.15}$$

The *breaks* of the filtration G^v are the values of v for which $G^v \neq G^{v+\epsilon}$ for all $\epsilon > 0$; they are not necessarily integers, even in the case of a finite extension.

2.3.2.5 Cyclotomic fields yet again. The calculation in section 2.2.3.1 of the ramification filtration for $\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p$ shows that

$$G_u = \begin{cases} G & u \leq 0 \\ U^i & 1 \leq i \leq n-1 \text{ and } p^{i-1}-1 < u \leq p^i - 1 \\ 1 & u > p^{n-1}-1. \end{cases}$$

The Herbrand function φ for $\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p$ is then

$$\begin{aligned}
\varphi(u) &= u && \text{for} \quad u \in [-1, 0] \\
&= i + \frac{u - (p^{i-1} - 1)}{(p-1)p^{i-1}} && \text{for} \quad 1 \le i \le n-1 \text{ and } u \in (p^{i-1} - 1, p^i - 1] \\
&= n + \frac{u - (p^{n-1} - 1)}{(p-1)p^{n-1}} && \text{for} \quad u \ge p^{n-1} - 1
\end{aligned}$$

It follows that the breaks of the ramification filtration in the upper numbering are integral and that

$$G^v = U^v$$

for integral $0 \le v \le n$.

The field $\mathbb{Q}_p(\mu^{p^\infty})$ is the colimit of the finite extensions $\mathbb{Q}_p(\mu^{p^n})$ for $n \to \infty$. The Galois group is $G = \varprojlim_n (\mathbb{Z}/p^n\mathbb{Z})^\times = \mathbb{Z}_p^\times$ and the previous results show that $G^v = U^v$ where now $U^v \subset \mathbb{Z}_p^\times$ is the subgroup of p-adic integers congruent to 1 modulo p^v and v ranges through all natural numbers.

The Hasse-Arf theorem states that the breaks of the ramification filtration in the upper numbering are integral for any abelian extension of discretely valued nonarchimedean fields with perfect residue fields. We will see more examples.

2.3.2.6 A Kummer extension. Suppose now $K = \mathbb{Q}_p(\mu_{p^n})$, π is a uniformizer of K and $L = K(x)$ where x is a root of $f(X) = X^{p^n} - \pi$ in $\bar{\mathbb{Q}}_p$. Since f is an Eisenstein polynomial L/K is a totally ramified extension of degree p^n and x is a uniformizer of L. Since K contains the p^nth roots of unity L/K is Galois. The Galois group is isomorphic to $G = \mu_{p^n}$ with $\alpha \in \mu_{p^n}$ acting on L via $x \mapsto \alpha x$. We may use x to compute the function i_G:

$$i_G(\alpha) = v_L(\alpha x - x) = v_L(\alpha - 1) + 1.$$

If $\alpha - 1$ is a primitive p^ith root of unity,

$$v_L(\alpha - 1) = p^n v_K(\alpha - 1) = p^{2n-i}$$

and thus

$$s \in G_m \iff p^{2n-i} \ge m.$$

The ramification filtration is then

$$\begin{aligned}
G_u &= G && \text{for} \quad u \in [-1, p^n] \\
&= \mu_{p^{n-i}} && \text{for} \quad 0 < i < n, \text{ and } u \in (p^{n+i-1}, p^{n+i}] \\
&= 1 && \text{for} \quad u > p^{2n-1}
\end{aligned}$$

and the Herbrand function is

$$\begin{aligned}
\varphi_{L/K}(u) &= u && \text{for} \quad u \in [-1, p^n] \\
&= (i+1)p^n - ip^{n-1} + \frac{u - p^{n+i}}{p^{i+1}} && \text{for} \quad 0 < i < n-1 \text{ and } u \in [p^{n+i}, p^{n+i+1}] \\
&= np^n - (n-1)p^{n-1} + \frac{u - p^{2n-1}}{p^n} && \text{for} \quad u \ge p^{2n-1}.
\end{aligned}$$

The breakpoints of the ramification filtration for the upper numbering are the integers $(i+1)p^n - ip^{n-1}$ for $0 < i < n-1$ (as predicted by Hasse-Arf).

2.4 The Norm

The main result of this section is that the norm $N_{L/K} : L^\times \to K^\times$ is surjective if L/K is a finite extension of discretely valued nonarchimedean fields with algebraically closed residual fields (note that L/K is then totally ramified). This is one of the key points in our treatment of local class field theory.

2.4.1 Unramified extensions. Of course the norm can never be surjective for a nontrivial extension since the image of the induced map $\Gamma_L \to \Gamma_K$ has index $[L:K]$. In this section we study the homomorphism $\mathcal{O}_L^\times \to \mathcal{O}_K^\times$ induced by the norm.

We denote by U_L^n the groups that were designated U^n is section 2.2.4: the elements $\mathcal{O}_L^\times$ congruent to 1 modulo π^n, where π is any uniformizer of L, and similarly for $U_K^n \subseteq \mathcal{O}_K^\times$. By definition $U_L^0 = \mathcal{O}_L^\times$ and $U_K^0 = \mathcal{O}_K^\times$.

2.4.1.1 Lemma *Let $f : A \to B$ be a homomorphism of abelian groups, and let $A_n \subseteq A$, $B_n \subseteq B$ be filtrations such that $f(A_n) \subseteq B_n$ for all $n \geq 0$ and the natural maps*

$$A \to \varprojlim_n A/A_n, \qquad B \to \varprojlim_n B/B_n$$

are isomorphisms. If the maps $A_n/A_{n+1} \to B_n/B_{n+1}$ induced by f are injective (resp. surjective, bijective) then so is f.

Proof.

■

Note that the second condition in the lemma applies to the filtrations $U_K^n \subseteq \mathcal{O}_K^\times$ and $U_L^n \subseteq \mathcal{O}_L^\times$.

If $x \in U_L^n$ we may write $x = 1 + \pi^n u$ with $u \in \mathcal{O}_L$ and π a uniformizer of K; then

$$N_{L/K}(x) = \prod_{s \in G}(1 + \pi^{ns}u) \equiv 1 + \pi^n \mathrm{Tr}_{L/K}(u) \mod \pi^{2n}. \tag{2.4.1.1}$$

This shows that $N_{L/K}(U_L^n) \subseteq U_K^n$, and the norm induces maps

$$N_n : U_L^n/U_L^{n+1} \to U_K^n/U_K^{n+1} \tag{2.4.1.2}$$

for all $n \geq 0$. Evidently N_0 is the norm on the residual extensions, and if we fix a choice of π to identify $U_K^n/U_K^{n+1} \simeq k$ and $U_L^n/U_L^{n+1} \simeq k_L$ then N_n for $n > 0$ is the trace.

2.4.1.2 Proposition *Suppose L/K is finite and unramified. For any $n > 0$, $N_{L/K}$ induces a surjective map $U_L^n \to U_K^n$, and the canonical projection induces an isomorphism*

$$\mathcal{O}_K^\times/N_{L/K}(\mathcal{O}_L^\times) \xrightarrow{\sim} k^\times/N_{k_L/k}(k_L^\times). \tag{2.4.1.3}$$

Proof. Since the trace is surjective for any finite separable extension, 2.4.1.2 is surjective for all $n > 0$ and it follows that the induced map $U_L^n \to U_K^n$ is also surjective. In particular this is so for $n = 1$, and applying the snake lemma to the diagram

$$\begin{tikzcd} 0 \arrow[r] & U_L^1 \arrow[r] \arrow[d] & \mathcal{O}_L^\times \arrow[r] \arrow[d] & k_L^\times \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & U_K^1 \arrow[r] & \mathcal{O}_K^\times \arrow[r] & k^\times \arrow[r] & 0 \end{tikzcd}$$

yields the isomorphism 2.4.1.3, since all vertical arrows are induced by the appropriate norm. ■

2.4.1.3 Corollary *The norm map $\mathcal{O}_L^\times \to \mathcal{O}_K^\times$ is surjective if and only if the residual norm map $k_L^\times \to k^\times$ is surjective.*

2.4.1.4 Lemma *If k'/k is an extension of finite fields, the norm $N_{k'/k} : (k')^\times \to k^\times$ is surjective.*

Proof. Suppose $|k| = q$ and $|k'| = q^f$. Since the qth power Frobenius generates the Galois group of k'/k, the norm map is $x \mapsto x^n$ where

$$n = 1 + q + \cdots + q^{f-1} = \frac{q^f - 1}{q - 1}.$$

The kernel of norm has at most n elements, so the image has at least $(q^f - 1)/n = q - 1$ elements. Since the image has at most that many elements, $N_{k'/k}$ is surjective. ■

Combining the lemma with , we find:

2.4.1.5 Proposition *Suppose L/K is unramified Galois extension of local fields.*

(i). The norm map $\mathcal{O}_L^\times \to \mathcal{O}_K^\times$ is surjective.

(ii). The group $K^\times / N_{L/K} L^\times$ is cyclic of order n, generated by any uniformizer of K.

Proof. The first assertion follows from the lemma and proposition 2.4.1.2. For the second, let v_K, v_L be the normalized valuations of K and L; since L/K is unramified v_L is an extension of v_K. In the commutative diagram

$$\begin{tikzcd} 0 \arrow[r] & \mathcal{O}_L^\times \arrow[r] \arrow[d, "N"'] & L^\times \arrow[r, "v_L"] \arrow[d, "N"'] & \mathbb{Z} \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & \mathcal{O}_K^\times \arrow[r] & K^\times \arrow[r, "v_K"] & \mathbb{Z} \arrow[r] & 0 \end{tikzcd}$$

the left hand is surjective, and since L/K is unramified the image of the right hand arrow is $n\mathbb{Z}$, whence the second assertion. ■

2.4.2 Some totally ramified cases. We now suppose L/K is cyclic of prime degree ℓ and we fix a generator $s \in G$. The filtrations $U_K^n \subset \mathcal{O}_K^\times$ and $U_L^n \subset \mathcal{O}_L^\times$ are defined as in the last section. We also choose uniformizers $\pi \in \mathcal{O}_K$ and $\tau \in \mathcal{O}_L$ and use these to identify $U_L^n/U_L^{n+1} \simeq k_L$ and $U_K^n/U_K^{n+1} \simeq k$ for $n > 0$. More precisely, the class of $1 + \tau^n u \in U_L^n$ is identified with the image of u in k_L, and similarly the class of $1 + \pi^n u \in U_L^n$ is identified with the image of u in k.

Since G is cyclic of prime order the ramification groups G_n are either G or 1, and we let t be unique break in the filatration, so that $G_n = G$ for $n \le t$ and $G_n = 1$ for $n > t$. The Herbrand function and its inverse are

$$\varphi_{L/K}(u) = \begin{cases} u & u \le t \\ t + \ell^{-1}(u-t) & u \ge t \end{cases}$$

$$\psi_{L/K}(u) = \begin{cases} u & u \le t \\ t + \ell(u-t) & u \ge t \end{cases}$$

and the different has valuation

$$v_L(\mathcal{D}_{L/K}) = (t+1)(\ell - 1)$$

by formula 2.2.3.2.

2.4.2.1 Lemma *For any integer $n \ge 0$, $\mathrm{Tr}_{L/K}(\mathfrak{m}_L^n) = \mathfrak{m}^r$ where*

$$r = r(n) = \left\lfloor \frac{n+m}{\ell} \right\rfloor \quad \textit{and} \quad m = (t+1)(\ell-1).$$

Proof. By proposition 2.1.6.1 $\mathrm{Tr}_{L/K}(\mathfrak{m}_L^n) \subset \mathfrak{m}^r$ if and only if $\mathfrak{m}_L^n \subseteq \mathfrak{m}^r \mathcal{D}_{L/K}^{-1}$, i.e.

$$n = v_L(\mathfrak{m}_L^n) \le v_L(\mathfrak{m}^r) + v_L(\mathcal{D}_{L/K}^{-1})$$

which since $e_{L/K} = \ell$ is equivalent to $n \le \ell r - m$, i.e. $(n+m)/\ell \le r$. ■

In proposition 2.4.2.3 we will need the values $r(\psi(n))$ and $r(\psi(n)+1)$. There are two cases. If $n < t$ then $\psi(n) = n$, and

$$r(n) = \left\lfloor \frac{(t+1)(\ell-1)+n}{\ell} \right\rfloor.$$

The numerator of the fraction on the right is

$$(t+1)\ell - 1 - (t-n) \ge (n+2)\ell - 2$$

and consequently

$$r(n) \ge \left\lfloor n + 2 - \frac{2}{\ell} \right\rfloor \ge n+1.$$

When $n \geq t$ we have $\psi(n) = t + \ell(n-t)$ and

$$r(\psi(n)) = \left\lfloor \frac{(t+1)(\ell-1)+t+\ell(n-t)}{\ell} \right\rfloor = \left\lfloor n+1-\frac{1}{\ell} \right\rfloor = n$$
$$r(\psi(n)+1) = \left\lfloor \frac{(t+1)(\ell-1)+t+\ell(n-t)+1}{\ell} \right\rfloor = n+1$$

In short:

$$n < t \Rightarrow r(\psi(n)) \geq n+1 \tag{2.4.2.1}$$
$$n \geq t \Rightarrow r(\psi(n)) = n \quad \text{and} \quad r(\psi(n)+1) = n+1. \tag{2.4.2.2}$$

2.4.2.2 Lemma *If $x \in \mathfrak{m}_L^n$ then*

$$N_{L/K}(1+x) \equiv 1 + \mathrm{Tr}_{L/K}(x) + N_{L/K}(x) \mod \mathrm{Tr}_{L/K}(\mathfrak{m}_L^{2n}). \tag{2.4.2.3}$$

Proof. We have

$$N_{L/K}(1+x) = \prod_{s \in G}(1+{}^s x) = 1 + \sum_u {}^u x$$

where u runs over the set of elements of $\mathbb{Z}[G]$ of the form

$$u = s_1 + \cdots + s_r$$

with $s_1, \ldots, s_r$ distinct elements of G. With this notation $r = \mathrm{aug}(u)$, and the terms with $\mathrm{aug}(u) = 1$, ℓ yield the terms $\mathrm{Tr}_{L/K}(x)$ and $N_{L/K}(x)$ in 2.4.2.3. We must show that the remaining terms lie in $\mathrm{Tr}_{L/K}(\mathfrak{m}_L^{2n})$. Observe first that if $\mathrm{aug}(u) \neq \ell$ then $su \neq u$, for otherwise $u = 1+s+\cdots+s^{\ell-1}$ and then $\mathrm{aug}(u) = \ell$. Since i and ℓ are relatively prime this implies that $s^i u \neq u$ for $0 < i < \ell$, and therefore $\sum_{\mathrm{aug}(u) \neq 1, \ell} {}^u x$ is a sum of terms of the form

$$\sum_{0 \leq i < \ell} {}^{s^i u} x = \mathrm{Tr}_{L/K}({}^u x).$$

Since $\mathrm{aug}(u) \geq 2$, ${}^u x \in \mathfrak{m}_L^{2n}$ and the same is then true for $\sum_{\mathrm{aug}(u) \neq 1,\ \ell} {}^u x$. ■

2.4.2.3 Proposition *Suppose L/K is cyclic and totally ramified of degree ℓ. Then for all $n \geq 0$, $N_{L/K}(U_L^{\psi(n)}) \subseteq U_K^n$ and $N_{L/K}(U_L^{\psi(n)+1}) \subseteq U_K^{n+1}$. There are $a_n \in k^\times$ for $0 < n \leq t$ and $b_n \in k^\times$ for $n \geq t$ such that the induced morphism*

$$N_n : U_L^{\psi(n)}/U_L^{\psi(n)+1} \to U_K^n/U_K^{n+1}$$

is

$$N_n(x) = \begin{cases} x^\ell & n = 0 \\ a_n x^p & 0 < n < t \\ a_t x^p + b_t x & n = t > 0 \\ b_n x & n > t \end{cases}. \tag{2.4.2.4}$$

Proof. Since L/K is totally ramified, $N_{L/K}(\tau) = a\pi$ where π, τ are the uniformizers chosen above and $a \in \mathcal{O}_K^\times$; thus the image a_n of a^n in k is nonzero. On the other hand if r is as in lemma 2.4.2.1 the trace induces an $\mathcal{O}_K$-linear map

$$\mathfrak{m}_L^n/\mathfrak{m}_L^{n+1} \to \mathfrak{m}^r/\mathfrak{m}^{r+1}. \tag{2.4.2.5}$$

These are one-dimensional k-vector spaces which our choice of uniformizers $\tau \in \mathcal{O}_L$, $\pi \in \mathcal{O}_K$ allows us to identify with k. With these identifications 2.4.2.5 has the form $x \mapsto bx$ for some *nonzero* $b \in k$.

The assertions are clear in the case $n = 0$, and in the remaining cases we must have $\ell = p$. We treat each in turn:

$0 < n < t$: In this case $\psi(n) = n$, and in this case $\mathrm{Tr}_{L/K}(\mathfrak{m}_L^n) \subseteq \mathfrak{m}^{n+1}$ by 2.4.2.1, so

$$N_{L/K}(1 + \tau^n u) \equiv 1 + N_{L/K}(\tau^n u) \equiv 1 + a_n \pi^n u^p \mod \mathfrak{m}^{n+1}$$

by lemma 2.4.2.2. If $u \in \mathfrak{m}_L$ this shows $N_{L/K}(U_L^{n+1}) \subseteq U_K^{n+1}$, and in any case $N_n(u) = a_n u^p$ with $a_n \neq 0$, as required.

$n = t > 0$: We still have $\psi(t) = t$, and this time $\mathrm{Tr}_{L/K}(\mathfrak{m}_L^t) = \mathfrak{m}^t$ and $\mathrm{Tr}_{L/K}(\mathfrak{m}_L^{t+1}) = \mathfrak{m}^{t+1}$ by 2.4.2.2. Lemma 2.4.2.2 now yields

$$N_{L/K}(1 + \tau^t u) \equiv 1 + \mathrm{Tr}_{L/K}(\tau^t u) + N_{L/K}(\tau^t u) \mod \mathfrak{m}^{t+1}$$

which shows that $N_{L/K}(U_L^t) \subseteq U_K^t$, and taking $u \in \mathfrak{m}_L$ and again applying 2.4.2.2 shows that $N_{L/K}(U_L^{t+1}) \subseteq U_K^{t+1}$. Finally the discussion in the first paragraph shows that $N_t(u) = b_t u + a_t u^p$ with nonzero a_t, b_t.

$n > t$: This time $\psi(n) = t + \ell(n - t) \geq n + 1$ and therefore $N_{L/K}(\mathfrak{m}_L^{\psi(n)}) \subseteq \mathfrak{m}^{n+1}$. Furthermore $\mathrm{Tr}_{L/K}(\mathfrak{m}_L^{\psi(n)}) = \mathfrak{m}^n$ and $\mathrm{Tr}_{L/K}(\mathfrak{m}_L^{2\psi(n)}) \subseteq \mathrm{Tr}_{L/K}(\mathfrak{m}_L^{\psi(n)+1}) = \mathfrak{m}^{n+1}$, so that

$$N_{L/K}(1 + \tau^{\psi(n)} u) \equiv 1 + \mathrm{Tr}_{L/K}(\tau^{\psi(n)} u) \mod \mathfrak{m}^{n+1}.$$

As before $N_{L/K}(U_L^{\psi(n)}) \subseteq U_K^n$ and $N_{L/K}(U_L^{\psi(n)+1}) \subseteq U_K^{n+1}$, and finally $N_n(u) = b_n u$ with $b_n \neq 0$. ■

2.4.2.4 Corollary *The map N_n is injective for all n except $n = t$, in which case the sequence*

$$0 \to G \xrightarrow{\theta_t} U_L^t/U_L^{t+1} \xrightarrow{N_n} U_L^t/U_L^{t+1} \tag{2.4.2.6}$$

is exact.

Proof. Injectivity for $n \neq t$ is clear from the formulas in the proposition. On the other hand the image of θ_t is clearly contained in the kernel of N_t: for $t = 0$ it suffices to observe that $s(\tau)/\tau$ is in the kernel of the norm, and for $t > 0$ this is also the case for $s(1+\tau^t)/(1+\tau^t)$. When $t = 0$ G_0 injects into U_L^0/U_L^1 and has order ℓ when $t = 0$, while the kernel of N_0 has order at most ℓ, so $\theta_0(G_0)$ must be the exact kernel. Similarly when $t > 0$, G_t injects into U_L^t/U_L^{t+1}, so the image has order p; on the other hand the kernel is the set of roots of $a_t X + b_t X^p$, and there are exactly p of these. ■

2.4.2.5 Theorem *Suppose L/K is a finite Galois extension of discretely valued nonarchimedean fields with algebraically closed residue field. Then the norm map $N_{L/K} : L^\times \to K^\times$ is surjective.*

Proof. The hypothesis implies that L/K is totally ramified. Then in the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{O}_L^\times \arrow[r] \arrow[d, "N"'] & L^\times \arrow[r, "v_L"] \arrow[d, "N"'] & \mathbb{Z} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathcal{O}_K^\times \arrow[r] & K^\times \arrow[r, "v_K"] & \mathbb{Z} \arrow[r] & 0
\end{tikzcd}$$

the right hand vertical arrow is an isomorphism. It thus suffices to show that $N : \mathcal{O}_L^\times \to \mathcal{O}_K^\times$ is surjective. Since $G = \mathrm{Gal}(L/K)$ is solvable, the transitivity of the norm shows that it suffices to show that $N : \mathcal{O}_L^\times \to \mathcal{O}_K^\times$ is surjective when L/K is cyclic of prime order. Since the residue field k of K (and L) is algebraically closed, the formulas in proposition 2.4.2.3 show that N_n is surjective for all $n \geq 0$, and finally lemma 2.4.1.1 shows that $N : \mathcal{O}_L^\times \to \mathcal{O}_K^\times$ is surjective. ■

Chapter 3

Group Cohomology

In this chapter we review some basic aspects of group cohomology and homology. We assume the reader is familiar with some basic homological algebra. Our sign conventions for the latter are those of Bourbaki.

3.1 Homology and Cohomology

3.1.1 Definitions. Let G be a group. A *left G-module* is a left module over the integral group ring $\mathbb{Z}[G]$ of G. One easily checks that a G-module A can be identified with an abelian group A endowed with a (left) G-action $(g, a) \mapsto g \cdot a$ via homomorphisms, i.e. $g \cdot (a + b) = g \cdot a + g \cdot b$. For example if A is any abelian group we may make it into a G-module by means of the *trivial* action: $g \cdot a = a$ for all $a \in A$. A *morphism* of G-modules is just a morphism of left $\mathbb{Z}[G]$-modules.

Although right G-modules (i.e. right $\mathbb{Z}[G]$-modules) are less of a concern here, the entire theory described here holds with appropriate changes for right G-modules. In fact there is an exact equivalence of the categories of left and right G-modules: any group is isomorphic to its opposite group by the map $i : s \mapsto s^{-1}$, so the ring $\mathbb{Z}[G]$ is likewise isomorphic to its opposite ring. Then a left G-module becomes a right G-module via extension of scalars by i and conversely.

If A is a G-module, the *cohomology groups of G with coefficients in A* are the Ext groups

$$H^n(G, A) = \mathrm{Ext}^n_{\mathbb{Z}[G]}(\mathbb{Z}, A) \tag{3.1.1.1}$$

where $\mathbb{Z}$ has the trivial G-action. The standard properties of Ext groups imply corresponding properties for the $H^n(G, A)$. First and foremost, these groups are functorial in A: for any morphism $A \to B$ of G-modules there is a canonical homomorphism

$$H^n(G, A) \to H^n(G, B) \tag{3.1.1.2}$$

and these are compatible with composition. Second, for any short exact sequence

$$0 \to A \to B \to C \to 0 \tag{3.1.1.3}$$

of G-modules there is a long exact sequence

$$\to H^n(G,A) \to H^n(G,B) \to H^n(G,C) \xrightarrow{\partial} H^{n+1}(G,A) \to \tag{3.1.1.4}$$

in which the maps $H^n(G,A) \to H^n(G,B)$, $H^n(G,B) \to H^n(G,C)$ are the ones induced by functoriality (we will recall later how to compute ∂). This long exact sequence 3.1.1.4 is natural in the sense that if

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r] \arrow[d] & B \arrow[r] \arrow[d] & C \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & A' \arrow[r] & B' \arrow[r] & C' \arrow[r] & 0 \end{tikzcd} \tag{3.1.1.5}$$

is commutative with exact rows,

$$\begin{tikzcd} H^n(G,A) \arrow[r] \arrow[d] & H^n(G,B) \arrow[r] \arrow[d] & H^n(G,C) \arrow[r, "\partial"] \arrow[d] & H^{n+1}(G,A) \arrow[d] \\ H^n(G,A') \arrow[r] & H^n(G,B') \arrow[r] & H^n(G,C') \arrow[r, "\partial"] & H^{n+1}(G,A') \end{tikzcd} \tag{3.1.1.6}$$

is commutative.

The *homology groups of G with coefficients in A* are defined by

$$H_n(G,A) = \mathrm{Tor}_n^{\mathbb{Z}[G]}(\mathbb{Z},A) \tag{3.1.1.7}$$

and have similar formal properties: they are functorial in A, and for any exact sequence 3.1.1.3 there is a corresponding long exact sequence

$$H_{n+1}(G,C) \to H_n(G,A) \to H_n(G,B) \to H_n(G,C) \to \tag{3.1.1.8}$$

which is natural in the sense that a commutative diagram 3.1.1.5 with exact rows gives rise to a commutative diagram analogous to 3.1.1.6.

It follows from a general property of the Tor functors that if A is a flat G-module (i.e. flat as a $\mathbb{Z}[G]$-module) then $H_n(G,A) = 0$ for all $n > 0$. This is the case in particular when A is projective.

3.1.2 The bar resolution. The groups $H^n(G,A)$ can be computed by taking any resolution of $\mathbb{Z}$ by projective $\mathbb{Z}[G]$-modules

$$\cdots \to P_2 \xrightarrow{d_1} P_1 \xrightarrow{d_0} P_0 \xrightarrow{\epsilon} \mathbb{Z} \to 0. \tag{3.1.2.1}$$

Then

$$H^n(G,A) \simeq H^n(\mathrm{Hom}(P.,A)) \tag{3.1.2.2}$$

where $\mathrm{Hom}(P., A)$ is the complex

$$\mathrm{Hom}_G(P_0, A) \xrightarrow{d_0^*} \mathrm{Hom}_G(P_1, A) \xrightarrow{d_1^*} \mathrm{Hom}_G(P_2, A) \xrightarrow{d_2^*} .$$

With this notation, 3.1.2.2 becomes

$$H^n(G, A) \simeq \mathrm{Ker}(d_n^*)/\mathrm{Im}(d_{n-1}^*). \tag{3.1.2.3}$$

One has complete freedom to choose $P.$ in making computations, as long as it is a resolution of $\mathbb{Z}$ by projective $\mathbb{Z}[G]$-modules. This can be very useful for the study of specific groups, as we shall see later. But there is one resolution that works for any group, the so-called *bar resolution*. In this we take P_n to be the free $\mathbb{Z}[G]$-module with basis G^n:

$$P_n = B_n = \mathbb{Z}[G]^{G^n} \tag{3.1.2.4}$$

The elements of G^n are usually written as n-tuples $(s_1, s_2, \ldots, s_n)$ but we will follow tradition and write this as $[s_1|s_2|\cdots|s_n]$. The maps $\epsilon : B_0 \to \mathbb{Z}$ and $d_n : B_n \to B_{n-1}$ are defined by

$$\begin{aligned} \epsilon([s]) &= 1 \\ d[s_1|s_2|\cdots|s_{n+1}] &= s_1[s_2|\cdots|s_n] + \sum_{1\le i\le n} [s_1|\cdots|s_i s_{i+1}|\cdots|s_n] \\ &\quad + (-1)^{n+1}[s_1|s_2|\cdots|s_n]. \end{aligned} \tag{3.1.2.5}$$

We can show that this is a resolution of $\mathbb{Z}$ by constructing contracting homotopy for 3.1.2.1 when $P_n = B_n$, i.e. a set of G-module maps

$$\mathbb{Z} \xrightarrow{\eta} B_0 \xrightarrow{h_0} B_1 \xrightarrow{h_1} B_2 \xrightarrow{h_2} \tag{3.1.2.6}$$

satisfying

$$\begin{aligned} \epsilon\eta &= 1, \\ \eta\epsilon + d_0 h_0 &= 1, \\ h_{n-1}d_{n-1} + d_n h_n &= 1, \qquad n \ge 1. \end{aligned} \tag{3.1.2.7}$$

In fact

$$\eta(1) = [\ ], \qquad h_n(s_1[s_2|\cdots|s_n] = [s_1|s_2|\cdots|s_n] \tag{3.1.2.8}$$

does the trick.

The elements of $C^n(G, A) = \mathrm{Hom}(B_n, A)$ are called *n-cochains* and can be identified with functions $a : G^n \to A$. The subgroups

$$Z^n(G, A) = \mathrm{Ker}(d_n^*), \qquad B^n(G, A) = \mathrm{Im}(d_{n-1}^*)$$

of $C^n(G, A)$ are called the subgroups of *n-cocycles* and *n-coboundaries* respectively (of course this terminology is used for any cochain complex, but we will restrict its use to this particular case). Then 3.1.2.3 says that

$$H^n(G, A) \simeq Z^n(G, A)/B^n(G, A). \tag{3.1.2.9}$$

Two n-cocycles a, a' are *cohomologous* if the represent the same element of $H^n(G, A)$, and we will write this as $a \sim a'$. Thus $a \sim a'$ if and only if $a' = a + d^*_{n-1}(b)$ for some $(n-1)$-cochain b.

If $a(s_1, \ldots, s_n)$ is an n-cochain the definition 3.1.2.5 shows that

$$\begin{aligned} d^*_n(a)(s_1, \ldots, s_{n+1}) = s_1 a(s_2, \ldots, s_n) \\ + \sum_{1 \le i \le n} (-1)^i a(s_1, \ldots, s_i s_{i+1}, \ldots, s_n) \\ + (-1)^{n+1} a(s_1, \ldots, s_n) \end{aligned} \tag{3.1.2.10}$$

and thus the condition that $a(s_1, \ldots, s_n) \in Z^n(G, A)$ is just that the right hand side vanishes.

The coboundary map $\partial : H^n(G, C) \to H^{n+1}(G, A)$ in the long exact sequence 3.1.1.4 is computed as follows. Suppose a short exact sequence 3.1.1.3 is given and $c \in H^n(G, C)$. Pick an n-cocycle $\hat{c} \in Z^n(C, A)$ representing c and then an n-cochain $b \in C^n(G, B)$ mapping to c under the map induced by $B \to C$. One checks easily that $d^*_n(b)$ is a B-valued $(n+1)$-cocycle, and since $\hat{c}$ was an n-cocycle, $d^*_n(b)$ maps to zero under $B \to C$. In other words the "values" of $d^*_n(b)$ lie in A, and there is a unique n-cocycle $\hat{a}$ mapping to $d^*_n(b)$ under the map induced by $A \to B$. One then checks that the class a of $\hat{a}$ in $H^{n+1}(G, A)$ is independent of the choice of b, and then $\partial(c) = a$.

To compute homology we need a resolution of $\mathbb{Z}$ by right G-modules. The most direct approach here is to convert the terms of the bar resolution to right G-modules by means of the functor i in section 3.1.1, in which case the differentials 3.1.2.5 become

$$\begin{aligned} \epsilon([s]) = 1 \\ d[s_1|s_2|\cdots|s_{n+1}] = [s_2|\cdots|s_n]s_1^{-1} + \sum_{1 \le i \le n} [s_1|\cdots|s_i s_{i+1}|\cdots|s_n] \\ + (-1)^{n+1}[s_1|s_2|\cdots|s_n]. \end{aligned}$$

The change of basis

$$[s_1|s_2|\cdots|s_n] \mapsto [s_n^{-1}|\cdots|s_2^{-1}|s_1^{-1}]$$

yields a more appealing formalism: the differentials are now

$$\begin{aligned} d[s_1|\cdots|s_{n+1}] = [s_1|\cdots|s_n]s_{n+1} + \sum_{1 \le i \le n} [s_{n+1}|\cdots|s_{i+1}s_i|\cdots|s_n] \\ + (-1)^{n+1}[s_{n+1}|s_2|\cdots|s_2]. \end{aligned} \tag{3.1.2.11}$$

In particular

$$\epsilon([\ ]) = 1, \quad d[s] = [\ ]s - [\ ], \quad d[s|t] = [s]t - [st] + [t]. \tag{3.1.2.12}$$

The *right bar resolution* $\check{B}_\cdot \to \mathbb{Z}$ is the following resolution of the right G-module $\mathbb{Z}$: the nth term is the free right $\mathbb{Z}[G]$-module G^n, with the same notation for the basis elements as in the (left) bar resolution. The differentials are defined by 3.1.2.11, and the augmentation is $\epsilon([\ ]) = 1$.

3.1.3 Cohomological degree zero and one. Anyone new to this may well wonder what all this formalism is accomplishing. We now give concrete descriptions of $H^n(G, A)$ for small values of n, namely $n = 0$, 1 and 2.

The case $n = 0$ is simple: a 0-cochain in A is just an element $a \in A$, and 3.1.2.10 says $d_0^*(a)(g) = ga - a$; thus $a \in Z^0(G, A)$ if and only if a is fixed by the action of G. If we denote the set of G-fixed elements of A by A^G, we have shown that

$$H^0(G, A) \simeq A^G. \tag{3.1.3.1}$$

In fact this follows from the definition:

$$H^0(G, A) = \mathrm{Ext}^0_{\mathbb{Z}[G]}(\mathbb{Z}, A) \simeq \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A) \simeq A^G$$

where the last isomorphism identifies $f : \mathbb{Z} \to A$ with $f(1) \in A^G$. We thus see that the functor $A \mapsto A^G$ is left exact, and its right derived functors are the $H^n(G, A)$.

The case $n = 1$ is a little more interesting. A 1-cochain $a(g)$ in A must satisfy

$$s_1 a(s_2) - a(s_1 s_2) + a(s_1) = 0$$

or

$$a(s_1 s_2) = a(s_1) + s_1 a(s_2). \tag{3.1.3.2}$$

Such a map $G \to A$ is called a *crossed homomorphism*. A 1-cochain $a(s)$ is a coboundary, say $a = d_0^* b$ when $a(s) = sb - b$. When A is a trivial G-module the coboundaries vanish and a crossed homomorphism is just an ordinary group homomorphism, so

$$H^1(G, A) \simeq \mathrm{Hom}(G, A) \quad \text{when } A \text{ is a trivial } G\text{-module}. \tag{3.1.3.3}$$

3.1.4 Cohomological degree two. The case $n = 2$ is more interesting still. We will use multiplicative notation for both G and A in this section, and write a 2-cochain $a(s, t)$ as $a_{s,t}$; then the condition that $a_{s,t}$ is a 2-cocycle is that

$${}^s a_{t,u} a_{st,u}^{-1} a_{s,tu} a_{t,u}^{-1} = 1 \tag{3.1.4.1}$$

and $a_{s,t}$. It is a coboundary, say $a = d_1^*(b)$ if

$$a_{s,t} = {}^s b_t b_{st}^{-1} b_s$$

for some 1-cochain (b_s). A map $a : G \times G \to A$ satisfying 5.2.2.6 is traditionally called a *factor system*. One should note the particular cases

$${}^s a_{1,1} = a_{s,1}, \qquad a_{1,s} = a_{1,1} \tag{3.1.4.2}$$

of 5.2.2.6.

In a sense to be described shortly the group $H^2(G, A)$ classifies extensions of G by A. To see how, observe first that any extension

$$0 \to A \xrightarrow{i} E \xrightarrow{p} G \to 1 \tag{3.1.4.3}$$

gives rise to an action of G-module structure on A, by

$$^{g}a = gag^{-1} \tag{3.1.4.4}$$

for $g \in G$ and $a \in A$ (in what follows we will use multiplicative notation for G and A, even though A is an abelian group). Next, choose a section of p, say $s \mapsto e_s$ for all $s \in G$. Since $p(e_s e_t) = st$,

$$e_s e_t = i(a_{s,t}) e_{st} \tag{3.1.4.5}$$

for some set of $a_{s,t} \in A$. The associative law implies that $(a_{s,t})$ is an A-valued 2-cocyle, and if (e'_s) is a different choice of section, $e'_s = b_s e_s$ for some 1-cochaine, and the corresponding 2-cocycle is $a\partial(b)$. In this way the extension 3.1.4.5 gives rise to a well-defined element of $H^2(G, A)$.

To explain the sense in which $H^2(G, A)$ classifies extensions 3.1.4.5 (for a fixed G-module structure on A) we introduce the category $\mathrm{EXT}(G, A)$ whose objects are short exact sequences 3.1.4.3 and whose morphisms are commutative diagrams

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r] \arrow[d, equal] & E \arrow[r] \arrow[d, "f"] & G \arrow[r] \arrow[d, equal] & 1 \\ 0 \arrow[r] & A \arrow[r] & E' \arrow[r] & G \arrow[r] & 1 \end{tikzcd} . \tag{3.1.4.6}$$

We will usually denote the extension 3.1.4.3 and the extension group itself by the same letter, if this does not cause confustion. Note however that isomorphism of extensions stronger than simple isomorphism of the extension groups: in an isomorphism of extensions, the identifications of A as a subgroup of the extension groups correspond via the isomorphism of the extension groups, and similarly for G.

The snake lemma shows that f is an isomorphism, so $\mathrm{EXT}(G, A)$ is a groupoid. If $(a_{s,t})$ and $(a'_{s,t})$ are 2-cocycles for E and E' respectively, $(f(a_{s,t}))$ is another cocycle for E', so the two extensions E and E' yields the same element of $H^2(G, A)$.

Conversely, given a factor system a we can construct an object of $\mathrm{EXT}(G, A)$ as follows. Let $E_a = A \times G$ and define a composition law on E_a by

$$(x, s)(y, t) = (x^s y a_{s,t}, st) \tag{3.1.4.7}$$

One then checks the following points:

- This composition law is a group law on E_a; the condition 5.2.2.6 is what is needed for the associativity law, and the identity is $(a(1, 1)^{-1}, 1)$.
- The map $p : E_a \to G$ defined by $p(x, s) = s$ is surjective homomorphism with kernel isomorphic to A. Similarly the map $i : A \to E_a$ defined by $i(x) = (xa_{1,1}, 1)$ is injective and identifies A with the kernel of p.
- The cocycle assoiated to E_a by the section $s \mapsto (1, s)$ is a.

- The G-module structure of A defined by the extension (E_a, i, p) by 3.1.4.4 coincides with the given G-module structure.
- If $a \sim a'$ the $E_a \simeq E_{a'}$, the isomorphism $E_a \to E_{a'}$ being given by $(a, s) \mapsto (ab_s, s)$ where $a' = adb$.

The verification of the first three points is easier if one uses the fourth to replace a by a *normalized* cocycle, i.e. one satisyfing $a(1,1) = 0$. Details will be left as an exercise.

It should be clear that the set of isomorphism classes of $\mathrm{EXT}(G, A)$ is a set, which we denote by $\mathrm{Ext}(G, A)$. We have shown that $a \mapsto E_a$ induces a bijection $H^2(G, A) \xrightarrow{\sim} \mathrm{Ext}(G, A)$. This shows that $\mathrm{Ext}(G, A)$ has a natural group structure; in fact it is induced by a "categorical group structure" on $\mathrm{EXT}(G, A)$ which we now describe.

Let (E, i, p) and (F, j, q) be any two objects of $\mathrm{EXT}(G, A)$. The fibered product $E \underset{G}{\times} F$ is the set of $(e, f) \in E \times F$ such that $p(e) = q(f)$; the composition law $(e, f)(e', f') = (ee', ff')$ makes it into a group. The identity 3.1.4.4 shows that the set of $(i(a), j(a)^{-1})$ is a normal subgroup of $E \underset{G}{\times} F$, and we denote by $E * F$ the quotient of $E \underset{G}{\times} F$ by this subgroup. Denote by $[e, f]$ the image of (e, f) in $E * F$, so that $[i(a), f] = [e, j(a)f]$ for any $a \in A$. It is evident that

- there is a surjective homomorphism $r : E * F \to G$ such that $r([e, f]) = p(e) = q(f)$,
- the map $k : A \to E * F$ defined by $k(a) = [i(a), 1] = [1, j(a)]$ is injective and its image is the kernel of p.

Thus $(E * F, k, r)$ is an object of $\mathrm{EXT}(G, A)$ which we denote by $E * F$; it is called the *Baer sum* of E and F. It is clear from the construction that if $E \simeq E'$ and $F \simeq F'$ in $\mathrm{EXT}(G, A)$ then $E * F \simeq E'F'$, so the Baer sum induces a composition law on $\mathrm{Ext}(G, A)$.

It is easily checked that the class in $\mathrm{Ext}(G, A)$ of the semidirect product $A \rtimes G$ is an identity, and the class of (E, i, p) has as an inverse the class of (E, i^{-1}, p). We have therefore defined a group law in $\mathrm{Ext}(G, A)$ and an isomorphism

$$\mathrm{Ext}(G, A) \xrightarrow{\sim} H^2(G, A) \tag{3.1.4.8}$$

of abelian groups.

It remains to check that this group law corresponds with the one on $H^2(G, A)$. Suppose that (E, i, p) and (F, j, q) be any objects of $\mathrm{EXT}(G, A)$ and let $(E * F, k, r)$ denote the Baer sum. If we choose sections (e_s), (f_s) of p and q, the associated cocycles $(a_{s,t})$, $(b_{s,t})$ are defined by

$$e_s e_t = i(a_{s,t}) e_{st}, \qquad f_s f_t = i(b_{s,t}) f_{st}.$$

Then the set of $[e_s, f_s]$ is a section of $E * F$, and

$$[e_s, f_s][e_t, f_t] = [e_s e_t, f_s f_t] = [i(a_{s,t}) e_{st}, j(b_{s,t}) f_{st}] = k(a_{s,t} b_{s,t})[e_{st}, f_{st}]$$

showing that $(a_{s,t}b_{s,t})$ is indeed the cocycle associated to $E * F$ and the section $([e_s, f_s])$.

The group $H^1(G, A)$ also has an interpretation relating to group extensions. If $\mathcal{E}$ is the extension 3.1.4.3 and $\alpha \in \mathrm{Aut}(\mathcal{E})$, $\alpha(x)x^{-1} \in A$ since α induces the identity on G. Furthermore

$$\alpha(xa)(xa)^{-1} = \alpha(x)x^{-1}$$

since α induces the identity on A. It follows that there is a map $c_\alpha : G \to A$ defined by

$$c_\alpha(s) = \alpha(x)x^{-1} \quad \text{for any } x \in E \text{ such that } p(x) = s.$$

If x, $y \in E$ map to s and t respectively,

$$\begin{aligned} c_\alpha(st) &= \alpha(xy)(xy)^{-1} \\ &= \alpha(x)\alpha(y)y^{-1}x^{-1} = (\alpha(x)(\alpha(y)y^{-1})\alpha(x)^{-1})\alpha(x)x^{-1} \\ &= c_\alpha(s) \cdot {}^s c_\alpha(t) \end{aligned}$$

by the definition of the G-action on A, so c_α is an A-valued 1-cocycle. Finally if x maps to s then so does $\beta(x)$ for any $\beta \in \mathrm{Aut}(\mathcal{E})$, and then

$$c_{\alpha\beta}(s) = (\alpha\beta)(x)x^{-1} = \alpha(\beta(x))\beta(x)^{-1}\beta(x)x^{-1} = c_\alpha(s)c_\beta(s).$$

It follows that $\alpha \mapsto c_\alpha$ is a homomorphism $\mathrm{Aut}(\mathcal{E}) \to Z^1(G, A)$. We will leave it to the reader to check that this map is surjective, and the kernel is the group Inn_A of inner automorphisms by elements of A. In particular $H^1(G, A)$ is isomorphic to $\mathrm{Aut}(\mathcal{E})/\mathrm{Inn}_A$.

3.1.4.1 Pushouts. If $f : A \to B$ is a morphism of G-modules, the natural map $H^2(G, A) \to H^2(G, B)$ corresponds to the *pushout* extension. If $E = (E, i, p)$ is an object of $\mathrm{EXT}(G, A)$, the pushout f_*E is the bottom row in the diagram

$$\begin{tikzcd} 1 \arrow[r] & A \arrow[r, "i"] \arrow[d, "f"] & E \arrow[r, "p"] \arrow[d, "i_2"] & G \arrow[r] \arrow[d, equal] & 1 \\ 1 \arrow[r] & B \arrow[r, "i_1"'] & B \amalg_A E \arrow[r, "p_2"'] & G \arrow[r] & 1 \end{tikzcd} \tag{3.1.4.9}$$

where $B \amalg_A E$ is the amalgamted sum of the groups B and E over A, defined as follows: since f is a G-module homomorphism,

$$N = \{(f(a), i(a)) \in B \times E \mid a \in A\} \subseteq B \times E$$

is a normal subgroup of the product, and then

$$B \amalg_A E = (B \times E)/N. \tag{3.1.4.10}$$

If we denote the class of $(b, e) \in B \times E$ in $B \amalg_A E$ by $[b, e]$, the group law of $B \amalg_A E$ is

$$[b, e][c, f] = [bc, ef]$$

and

$$[f(a)b, e] = [a, i(b)e]$$

for all $a \in A$. The maps i_1, i_2 and p_2 in 3.1.4.9 are

$$i_1(b) = [b, 1], \quad i_2(e) = [1, e] \quad p_2([b, e]) = p(e)$$

respectively.

If $(e_s)_{s \in G}$ is a section of p, $([1, e_s])_{s \in G}$ is a section of p_2. If $(a_{s,t})$ is the A-valued cocycle of E for the (e_s), the B-valued cocycle of $f_* E$ for the $([1, e_s])$ is $(f(a_{s,t}))$.

Efforts to similarly interpret $H^n(G, A)$ for $n > 2$ quickly lead into the morass of higher category theory. So far as I know, only the case $n = 3$ has been worked out in the literature; it turns that $H^3(G, A)$ classifies equivalence classes of certain grouplike monoidal categories.

3.1.5 Homology in degree zero and one. As we saw in sect 3.1.2 we can use the bar resolution to compute homology, but there seems to be no simple interpretation of these groups except in special cases. We mention two.

For $n = 0$ we have

$$H_0(G, A) \simeq \mathbb{Z} \otimes_{\mathbb{Z}[G]} A \tag{3.1.5.1}$$

by definition. To interpret this, recall that the *augmentation ideal* $I \subset \mathbb{Z}[G]$ is the kernel of the *augmentation map*

$$\mathrm{aug} : \mathbb{Z}[G] \to \mathbb{Z} \qquad \sum_{s \in G} a_s s \mapsto \sum_{s \in G} a_s. \tag{3.1.5.2}$$

Then

$$0 \to I \to \mathbb{Z}[G] \xrightarrow{\mathrm{aug}} \mathbb{Z} \to 0 \tag{3.1.5.3}$$

is exact by definition. It is easily checked that I is generated as a left or right ideal by the $(s-1)$ for all $s \in G$. Tensoring the above short exact sequence with the G-module A yields

$$\mathbb{Z} \otimes_{\mathbb{Z}[G]} A \simeq A/IA \simeq A/(\sum_{s \in G}(s-1)A) = A_G \tag{3.1.5.4}$$

This is a quotient of A as a G-module and a trivial G-module. But if B is any quotient of A on which G acts trivially, the quotient $A \to B$ must necessarily map $(s-1)a$ to 0 for any $a \in A$. It follows that $A \to B$ factors $A \to A_G \to B$, or in other words A_G is the largest quotient of A on which G acts trivially (just as A^G is the largest submodule of A on which G acts trivially). The G-module A_G is the module of *coinvariants* of A. To summarize, we have shown that

$$H_0(G, A) \simeq A_G \tag{3.1.5.5}$$

for any G-module A.

There seems to be no simple interpretation of $H_1(G, A)$ in general. When A is a trivial G-module, i.e. $A = A^G$ we have $H_n(G, A) \simeq H_n(G, \mathbb{Z}) \otimes_{\mathbb{Z}} A$, and we will show that

$$H_1(G, \mathbb{Z}) \simeq G^{ab} \tag{3.1.5.6}$$

which implies that

$$H_1(G, A) \simeq G^{ab} \otimes_{\mathbb{Z}} A \tag{3.1.5.7}$$

for any trivial G-module A. Observe first that $C_1(G, \mathbb{Z}) = Z_1(G, \mathbb{Z})$ since

$$d[s] \otimes 1 = ([\ ]s - [\ ]) \otimes 1 = 0.$$

Next, the identity

$$0 = d[s|t] \otimes 1 = ([s]t - [st] + [t]) \otimes 1 = ([s] - [st] + [t]) \otimes 1$$

shows that

$$[s] \otimes 1 + [t] \otimes 1 = [st] \otimes 1 \tag{3.1.5.8}$$

in $H_1(G, \mathbb{Z})$. We conclude that

$$\alpha : G \to H_1(G, \mathbb{Z}) \qquad s \mapsto \langle s \rangle \otimes 1 \quad \text{mod boundaries}$$

is a surjective homomorphism. To show that $H_1(G, \mathbb{Z}) \simeq G^{ab}$ it suffices to show that $G \to H_1(G, \mathbb{Z})$ has the universal property of the abelianization: any homomorphism $f : G \to A$ to an abelian group factors uniquely through α. Since B_1 is a free $\mathbb{Z}[G]$-module, $B_1 \otimes_G \mathbb{Z}$ is a free $\mathbb{Z}$-module and there is a unique $g : B_1 \otimes_G \mathbb{Z} \to A$ such that

$$g([s] \otimes 1) = f(s).$$

Since f is a homomorphism 3.1.5.8 shows that g factors through $\bar{f} : H_1(G, \mathbb{Z}) \to A$ and then $f = \bar{f} \circ \alpha$ by construction. The factorization is unique since α is surjective.

3.1.6 Duality. Later we will need a generalization of 3.1.5.6. The homology groups $H_n(G, \mathbb{Z})$ are computed by

$$H_n(G, \mathbb{Z}) = H_n(P_\cdot \otimes_G \mathbb{Z})$$

for any projective resolution $P_\cdot$ of $\mathbb{Z}$. Therefore

$$\begin{aligned} \mathrm{Hom}(H_n(G, \mathbb{Z}), \mathbb{Q}/\mathbb{Z}) &\simeq \mathrm{Hom}(H_n(P_\cdot \otimes_G \mathbb{Z}, \mathbb{Q}/\mathbb{Z})) \\ &\simeq H^n(\mathrm{Hom}(P_\cdot \otimes_G \mathbb{Z}, \mathbb{Q}/\mathbb{Z})) \\ &\simeq H^n(\mathrm{Hom}(P_\cdot, \mathbb{Q}/\mathbb{Z}) \simeq H^n(G, \mathbb{Q}/\mathbb{Z}) \end{aligned}$$

where the penultimate isomorphism holds because any G-module homomorphism $P_i \to \mathbb{Q}/\mathbb{Z}$ must factor through the G-coinvariants $(P_i)_G \simeq P_i \otimes_G \mathbb{Z}$, the G-action on $\mathbb{Q}/\mathbb{Z}$ being trivial. We have shown that

$$\mathrm{Hom}(H_n(G, \mathbb{Z}), \mathbb{Q}/\mathbb{Z}) \simeq H^n(G, \mathbb{Q}/\mathbb{Z}) \tag{3.1.6.1}$$

and when $n = 1$ this says

$$\mathrm{Hom}(H_1(G,\mathbb{Z}),\mathbb{Q}/\mathbb{Z}) \simeq H^1(G,\mathbb{Q}/\mathbb{Z}) \simeq \mathrm{Hom}(G,\mathbb{Q}/\mathbb{Z}).$$

When G is a finite group this implies 3.1.5.6 by Pontryagin duality.

3.1.7 Cyclic groups. When G is a cyclic group there is a particular simple resolution of $\mathbb{Z}$ by free $\mathbb{Z}[G]$-modules. Suppose G is generated by an element g of order d, let C_n be a free $\mathbb{Z}[G]$-module of rank one and define $\epsilon : C_0 \to \mathbb{Z}$, $d_n : C_{n+1} \to C_n$ by

$$\begin{aligned} \epsilon(x) &= \mathrm{aug}(x) \\ d_n(x) &= \begin{cases} (g-1)x & n \text{ odd} \\ N_G(x) & n \text{ even.} \end{cases} \end{aligned} \tag{3.1.7.1}$$

where

$$N_G(x) = (g^{d-1} + g^{d-2} + \cdot + g + 1)x. \tag{3.1.7.2}$$

It is easily checked that

$$\to C_2 \xrightarrow{d_1} C_1 \xrightarrow{d_0} C_0 \xrightarrow{\epsilon} \mathbb{Z}$$

is exact. If we identify $\mathrm{Hom}_{\mathbb{Z}[G]}(C_n, A) \simeq A$ the maps $d_n^* : A \to A$ are again given by the formula 3.1.7.1 (where now $x \in A$). Since $\mathrm{Ker}(g-1) = A^G$ and $\mathrm{Im}(g-1) = IA$, we find that the $H^n(G,A)$ are

$$\begin{aligned} H^0(G,A) &= A^G \\ H^n(G,A) &= \begin{cases} \mathrm{Ker}(N_G)/IA & n \text{ odd} \\ A^G/\mathrm{Im}(N_G) & n > 0,\ n \text{ even} \end{cases} \end{aligned} \tag{3.1.7.3}$$

The same calculation can be made in homology, with the result

$$\begin{aligned} H_0(G,A) &= A_G \\ H_n(G,A) &= \begin{cases} \mathrm{Ker}(N_G)/IA & n > 0,\ n \text{ even} \\ A^G/\mathrm{Im}(N_G) & n \text{ odd.} \end{cases} \end{aligned} \tag{3.1.7.4}$$

3.1.8 Exercises.

3.1.8.1 Complete the arguments at the end of section 3.1.5 concerning the map $\mathrm{Aut}(\mathcal{E}) \to H^1(G,A)$.

3.1.8.2 Using the exact sequence 3.1.5.3, show that $H_1(G,\mathbb{Z}) \simeq I_G/I_G^2$. Then show directly that $I_G/I_G^2 \simeq G^{ab}$, thereby giving another proof of 3.1.5.6.

3.1.8.3 Show that the isomorphisms 3.1.7.3, 3.1.7.4 are induced by the following chain map $F : C. \to B.$ where $C.$ is the complex from section 3.1.7. If a is a generator of G and e_n is a $\mathbb{Z}[G]$-basis of C_n then

$$F(e_n) = \begin{cases} [\,] & n = 0 \\ \sum_I [a^{i_1}|a|a^{i_2}|a|\cdots|a^{i_s}|a] & i = 2s > 0,\ I = (i_1, \ldots, i_s) \\ \sum_I [a|a^{i_1}|a|a^{i_2}|a|\cdots|a^{i_s}|a] & i = 2s+1,\ I = (i_1, \ldots, i_s) \end{cases} \tag{3.1.8.1}$$

3.1.8.4 Cyclic groups are not the only finite groups with periodic cohomology. Consider for example the *generalized quaternion group* Q_{4n} which has generators x, y and relations

$$x^n = y^2,\ y^4 = 1,\ xyx = y. \tag{3.1.8.2}$$

Show that the trivial Q_{4n}-module $\mathbb{Z}$ has a free resolution $X. \to Q_{4n}$ with the following description:

- X_{4j} free on one element a_j, and

  $$da_j = Ne_{j-1}$$

  where $N = \sum_{0<i\leq 2n} x^i(1+y)$;

- X_{4j+1} free on b_j, b'_j with

  $$db_j = (x-1)a_j,\ db'_j = (y-1)j;$$

- X_{4j+2} free on c_j, c'_j with

  $$dc_j = Lb_j - (y+1)b'_j,\ dc'_j = (xy+1)b_j + (x-1)b'_j$$

  where $L = \sum_{0<i<n} x^i$;

- X_{4j+3} free on e_j with

  $$de_j = (x-1)c_j - (xy-1)c'_j$$

Note that Q_{4n} can be identified with the subgroup of the quaternion unit group $\mathbb{H}^\times$ by identifying $x = e^{\pi i/n}$ and $y = j$; in particular x and y have order $2n$ and 4 respectively.

3.1.8.5 Use the previous exercise to compute $H^n(Q_{4n}, \Lambda)$ for any trivial Q_{4n}-module Λ. See [3, pages 253–4] if you need help.

3.2 Change of Group

3.2.1 Restriction and Inflation. The groups $H^n(G,A)$, $H_n(G,A)$ in addition to being functorial in A, also behave in predictable ways relative to G. The are for example functorial in G in the following sense: let $f : G' \to G$ be a homomorphism, and for any G-module A let f^*A be the G'-module defined by "restriction to G'," i.e. $g' \in G'$ acts on A by $a \mapsto f(g')a$. With this notation there is a morphism

$$f^* : H^n(G,A) \to H^n(G', f^*A) \tag{3.2.1.1}$$

natural in A. The easiest definition is by means of cocycles: if $a(g_1,\dots,g_n) \in Z^n(G,A)$ represents a class in $H^n(G,A)$, the cochain $f^*(a) \in Z^n(G', f^*A)$ defined by

$$f^*a(g'_1,\dots,g'_n) = a(f(g'_1),\dots,f(g'_n)) \tag{3.2.1.2}$$

is in $Z^n(G', f^*A)$, and simlarly if $a \in B^n(G,A)$ then $f^*(a) \in B^n(G', f^*A)$. It follows that the f^* defined on $Z^n(G,A)$ passes to quotient by $B^n(G,A)$, and this defines 3.2.1.1. In most of what follows we will write A in place of f^*A when the meaning is obvious.

Two cases of this are important. In the first $H \subseteq G$ is a subgroup and the resulting map will be written

$$\mathrm{Res}^H_G : H^n(G,A) \to H^n(H,A). \tag{3.2.1.3}$$

and is called the *restriction* map, since if $a \in Z^n(G,A)$ represents a class in $H^n(G,A)$, the restriction of a to $H^n \subseteq G^n$ represents $\mathrm{Res}(a)$.

The other is when H is a normal subgroup of G and $\pi : G \to G/H$ is the canonical projection. If A is a G-module, A^H is naturally a G/H-module and the preceding construction yields a map

$$H^n(G/H, A^H) \to H^n(G, A^H).$$

Composing this with the map $H^n(G,A^H) \to H^n(G,A)$ induced by the inclusion yields the *inflation* map

$$\mathrm{Inf}^G_{G/H} : H^n(G/H, A^H) \to H^n(G,A). \tag{3.2.1.4}$$

3.2.1.1 Proposition *The sequence*

$$0 \to H^1(G/H, A^H) \xrightarrow{\mathrm{Inf}} H^1(G,A) \xrightarrow{\mathrm{Res}} H^1(H,A) \tag{3.2.1.5}$$

is exact.

Proof. (1) Inf is injective: pick $a \in Z^1(G/H, A^H)$ representing a class in $H^1(G/H, A^H)$ and suppose $\mathrm{Inf}(a)$ is a coboundary: $a(\pi(g)) = gx - x$ for some $x \in A$ and all $g \in G$. Since $\pi(gh) = \pi(g)$ for any $h \in H$ we must have $ghx - x = gx - x$, which implies $hx = x$ for any $h \in H$. Thus $x \in A^H$and it follows that $a \in B^1(G/H, A^H)$.

(2) $\mathrm{Res} \circ \mathrm{Inf} = 0$: again pick $a \in Z^1(G/H, A^H)$ representing a class in $H^1(G/H, A^H)$. Then $a|H$ is constant: $a(h) = a(1)$ for all $h \in H$. Since $a|H$ is a 1-cocycle, $a(h) = a(h1) = a(h) + ha(1)$ and it follows that $a(h) = a(1) = 0$.

(3) Pick $a \in Z^1(G, A)$ representing a class in $H^1(G, A)$ and suppose $a|H \sim 0$. This means that there is a $c \in A$ such that $a(h) = hc - c$ for all $h \in H$. Replacing a by $a - d_0(c)$, we may suppose that $a(h) = 0$ for $h \in H$. Then for $g \in G$ and $h \in H$ we have $a(gh) = a(g) + ga(h) = a(g)$, i.e. $a : G \to A$ factors through a map $G/H \to A$. Furthermore $a(hg) = a(h) + ha(g)$ implies $a(g) = ha(g)$, i.e $a(g) \in A^H$ for all $g \in G$. In other words a comes from an element of $Z^1(G/H, A^H)$. ■

3.2.1.2 Extensions again. Let's interpret the restriction and inflation maps when $n = 2$ in terms of group extensions. For any homomorphism $f : G \to G'$ the morphism 3.2.1.1 corresponds to the pullback of extensions. If $E = (E, i, p)$ is any object of $\mathrm{EXT}(A, G)$, the *pullback* of E is the top row of the diagram

$$\begin{tikzcd} 1 \arrow[r] & A \arrow[r, "i_f"] \arrow[d, equal] & E \times_G G' \arrow[r, "p_2"] \arrow[d, "p_1"] & G' \arrow[r] \arrow[d, "f"] & 1 \\ 1 \arrow[r] & A \arrow[r] & E \arrow[r] & G \arrow[r] & 1 \end{tikzcd} \tag{3.2.1.6}$$

where $E \times_G G'$ is the fibered product, p_1 and p_2 are the usual projections and $i_f(a) = (i(a), 1)$. It is clear that f^* defines a functor

$$f^*\mathrm{EXT}(G, A) \to \mathrm{EXT}(G', A) \tag{3.2.1.7}$$

and we also use f^* to denote the corresponding map

$$f^*\mathrm{Ext}(G, A) \to \mathrm{Ext}(G', A). \tag{3.2.1.8}$$

We denote the pullback by f^*E. Elements of $E \times_G G'$ are pairs $(e, s) \in E \times G'$ such that $p(e) = f(s)$, and the composition law is componentwise:

$$(e, s)(f, t) = (ef, st).$$

If (e_s) is a section of p, $(e_{f(s)}, s)$ is a section of $E \times_G G'$, and if the cocycle for E and the section (e_s) is $(a_{s,t})$, the correspondiing cocycle for f^*E is

$$f^*(a_{s,t}) = (a_{f(s),f(t)}) \tag{3.2.1.9}$$

so that 3.2.1.8 corresponds to 3.2.1.1 under the identification of $\mathrm{Ext}(G, A)$ with $H^2(G, A)$.

In particular, the restriction map 3.2.1.3 corresponds to the functor

$$\mathrm{Res}_G^H : \mathrm{EXT}(G, A) \to \mathrm{EXT}(H, A) \tag{3.2.1.10}$$

arising from the pullback by the inclusion $H \hookrightarrow G$. In this case the functor is simply

$$\mathrm{Res}_G^H(E, i, p) = (p^{-1}(H), i, p|H). \tag{3.2.1.11}$$

Suppose now H is a normal subgroup of G. The construction of the inflation 3.2.1.4 shows that it arises from the functor

$$\mathrm{Inf}^G_{G/H} : \mathrm{EXT}(G/H, A^H) \to \mathrm{EXT}(G, A) \tag{3.2.1.12}$$

which given an extension (E, i, p) of G/H by A^H first pulls it back by $G \to G/H$ and then pushes it out by $A^H \to A$ (it is easy to check that performing these operations in the reverse order produces an isomorphic result). If we follow the recipe for the pushout and pullback we arrive at the description of the elements of the extension group: they can be identified with symbols

$$[a, e, s] \quad \text{with } a \in A,\ e \in E,\ s \in G \text{ such that} \quad p(e) = \pi(s) \tag{3.2.1.13}$$

where $\pi : G \to G/H$ is the canonical homomorphism, and

$$[ab, e, s] = [a, i(b)e, s] \qquad \text{for } b \in A^H. \tag{3.2.1.14}$$

The group law is componentwise multiplication. Finally if $(e_s)_{s\in G/H}$ is a splitting of E and $(a_{s,t})$ is the corresponding cocycle, $([1, e_{\pi(s)}, s])_{s\in G}$ is a splitting of $\mathrm{Inf}^G_{G/H}(E)$, and the cocycle for this splitting is $(a_{\pi(s),\pi(t)})$.

3.2.2 Coinflation and Corestriction. There is a similar result in homology. When $H \subseteq G$ is a subgroup and M is a G-module we will call the change-of-group map $H_n(H, M) \to H_N(G, M)$ the *corestriction*, and denote it by Cor^G_H. The *coinflation*

$$\mathrm{Coinf}^{G/H}_G : H_n(G, M) \to H_n(G/H, M_H) \tag{3.2.2.1}$$

is defined as the composition of the functoriality map $H_n(G, M) \to H_n(G, M_H)$ with the change-of-group map $H_n(G, M_H) \to H_n(G/H, M_H)$.

3.2.2.1 Proposition *The sequence*

$$H_1(H, M) \xrightarrow{\mathrm{Cor}} H_1(G, M) \xrightarrow{\mathrm{Coinf}} H_1(G/H, M_H) \to 0 \tag{3.2.2.2}$$

is exact.

The proof will be left as an exercise.

3.2.3 Shapiro's Lemma. Suppose again that $H \subseteq G$ is a subgroup and let A be an H-module. If M is an H-module we define G-modules

$$\mathrm{Ind}^G_H(M) = \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} M, \qquad \mathrm{Coind}^G_H(M) = \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], M) \tag{3.2.3.1}$$

by means of the natural G-action on these G-modules. In the case of $\mathrm{Ind}^G_H(M)$ it is induced by the action of G on the left of $\mathbb{Z}[G]$, the right structure being used to take the tensor product. In the case of $\mathrm{Coind}^G_H(M)$ the left G-modules structure is used to form the Hom group, and the right action of G on $\mathbb{Z}[G]$ on itself induces a left action on the Hom group.

3.2.3.1 Lemma *The restriction of a projective left or right G-module to H is a projective H-module.*

Proof. This is clear for the free G-module $\mathbb{Z}[G]$, a $\mathbb{Z}[H]$-basis being given by a set of coset representatives of G/H. The result for free G-modules in general follows by taking direct sums, and for projective G-modules in general by passing to direct summands. ■

We now recall the following bit of general algebra. Suppose $R \to A$ is a homomorphism of rings, M is a left A-module and N is a left R-module. We may use the left R-module structure of A to form the group $\mathrm{Hom}_R(A, N)$ and the right A-module structure of A to make $\mathrm{Hom}_R(A, N)$ a left A-module. The *adjunction isomorphism* is a canonical and functorial isomorphism

$$\mathrm{Hom}_R(M, N) \xrightarrow{\sim} \mathrm{Hom}_A(M, \mathrm{Hom}_R(A, N)). \tag{3.2.3.2}$$

defined as follows. If $f : M \to N$ is R-linear and $m \in M$, the map $f_m : A \to N$ defined by $f_m(a) = f(am)$ is R-linear and the map $m \mapsto f_m$ is A-linear. This defines 3.2.3.2, and conversely if $f : M \to \mathrm{Hom}_R(A, N)$ is given we set $f_m = f(m)$ for $m \in M$, and then $m \mapsto f_m(1)$ is an R-linear map $M \to N$. It is easily checked that this map is inverse to the previous one.

Returning to the situation in which H is a subgroup of G, we take a projective G-resolution $P. \to \mathbb{Z}$, and note that $P.$ is also a resolution of $\mathbb{Z}$ by projective H-modules, by the lemma. We now apply 3.2.3.2 with R, A, M and N replaced by $\mathbb{Z}[H]$, $\mathbb{Z}[G]$, $P.$ and M respectively:

$$\mathrm{Hom}_H(P., M) \simeq \mathrm{Hom}_G(P., \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], M)) \simeq \mathrm{Hom}_G(P., \mathrm{Coind}_H^G(M)).$$

From this we deduce the isomorphism called Shapiro's lemma:

3.2.3.2 Theorem *For any H-module M,*

$$H^n(H, M) \simeq H^n(G, \mathrm{Coind}_H^G(M)). \tag{3.2.3.3}$$

A G-module is M *coinduced* if

$$M \simeq \mathrm{Coind}_1^G(A) \simeq \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], A) \tag{3.2.3.4}$$

for some abelian group A. Since the trivial group has no cohomology in positive degree, we find

3.2.3.3 Corollary *If M is a coinduced G-module, $H^n(G, M) = 0$ for all $n > 0$.*

Because of the corollary, coinduced modules play the same role for cohomology as free (or even flat) modules do for homology. The following construct is used in the procedure called *dimension-shifting*, of which we have already seen an example. If M is a G-module and

$$M^* = \mathrm{Coind}_1^G M = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], M)$$

there is a natural map $M \to M^*$ which to $m \in M$ assigns the map $f_m(g) = gm$. This is a morphism of G-modules and we define M' by the exactness of

$$0 \to M \to M^* \to M' \to 0. \tag{3.2.3.5}$$

By the corollary and the long exact sequence of cohomology we have

$$H^n(G, M') \xrightarrow{\sim} H^{n+1}(G, M) \tag{3.2.3.6}$$

for all $n > 0$. This allows us to do inductive proofs on the degree.

3.2.3.4 Lemma *Suppose H is a normal subgroup of G, M is a G-module and $M^* = \mathrm{Coind}_1^G(M)$. Then M^* is coinduced as an H-module and $(M^*)^H$ is coinduced as a G/H-module.*

Proof. Since $\mathbb{Z}[G]$ is a free $\mathbb{Z}[H]$-module there is an abelian group A and an isomorphism $\mathbb{Z}[G] \simeq \mathbb{Z}[H] \otimes_{\mathbb{Z}} A$ of $\mathbb{Z}[H]$-modules. Then

$$M^* = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], M) \simeq \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[H] \otimes_{\mathbb{Z}} A, M) \simeq \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[H], \mathrm{Hom}_{\mathbb{Z}}(A, M))$$

and M^* is coinduced as an H-module. That $(M^*)^H$ is a coinduced G/H-module follows from the isomorphism

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], M)^H \simeq \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G/H], M).$$

■

The version of Shapiro's lemma in homology is slighly simpler. With $P.$ a projective G-resolution of $\mathbb{Z}$ as before, the extension of scalars isomorphism

$$P. \otimes_{\mathbb{Z}[H]} M \simeq P. \otimes_{\mathbb{Z}[G]} (\mathbb{Z}[G] \otimes_{\mathbb{Z}[G]})$$

shows that there is an isomorphism

$$H_n(H, M) \simeq H^n(G, \mathrm{Ind}_H^G(M)) \tag{3.2.3.7}$$

for any H-module M. We could define an induced module to be one of the form $\mathrm{Ind}_1^G(A)$, but these are the same as the free G-modules.

We can now extend propositions 3.2.1.1 and 3.2.2.1.

3.2.3.5 Proposition *Suppose $H \subseteq G$, $n > 0$ and M is a G-module such that $H^i(H, M) = 0$ for $0 < i < n$. Then the inflation maps*

$$H^i(G/H, M^H) \xrightarrow{\sim} H^i(G, M) \tag{3.2.3.8}$$

are isomorphisms for $1 < i < n$ and the sequence

$$0 \to H^n(G/H, M^H) \to H^n(G, M) \to H^n(H, M) \tag{3.2.3.9}$$

is exact.

Proof. We argue by induction on $n \geq 0$, where the case $n = 1$ is proposition 3.2.1.1. Suppose the assertion is true for $n-1$, let $M^* = \mathrm{Coind}_1^G(M)$ as before and define M' by 3.2.3.5. Since $H^1(H, M) = 0$ the sequence

$$0 \to M^H \to (M^*)^H \to (M')^H \to H^1(H, M)$$

is exact. By lemma 3.2.3.4 M^* is coinduced both as a G-module and an H-module and M^H is coinduced as a G/H-module. Then the isomorphisms 3.2.3.6 show that there is a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & H^i(G/H, (M')^H) \arrow[r] \arrow[d, "\partial"] & H^i(G, M') \arrow[r] \arrow[d, "\partial"] & H^i(H, M') \arrow[d, "\partial"] \\
0 \arrow[r] & H^{i+1}(G/H, M^H) \arrow[r] & H^{i+1}(G, M) \arrow[r] & H^{i+1}(H, M)
\end{tikzcd}$$

in which the vertical maps are isomorphisms for $i > 0$. Since $H^{i+1}(H, M) = 0$ for $i + 1 < n$, $H^i(H, M') = 0$ for $i < n - 1$ and by induction the top row is exact. Then the bottom row is exact, which yields 3.2.3.11 and 3.2.3.12. ■

The exact sequence 3.2.3.12 is the *inflation-restriction sequence.* The reader familiar with spectral sequences will realize that the proposition is an immediate consequence of a spectral sequence

$$E_2^{p,q} = H^p(G/H, H^q(H, M)) \Rightarrow H^{p+q}(G, M) \tag{3.2.3.10}$$

which is a special case of the spectral sequence of a composite functor, in this case the composition $M^G \simeq (M^H)^{G/H}$.

The corresponding result in homology is proven in the same way, we leave this as an exercise.

3.2.3.6 Proposition *Suppose $H \subseteq G$, $n > 0$ and M is a G-module such that $H_i(H, M) = 0$ for $0 < i < n$. Then the coinflation maps*

$$H_i(G, M) \xrightarrow{\sim} H_i(G/H, M_H) \tag{3.2.3.11}$$

are isomorphisms for $1 < i < n$ and the sequence

$$H_n(H, M) \to H_n(G, M) \to H_n(G/H, M_H) \to 0 \tag{3.2.3.12}$$

is exact.

3.2.4 The Corestriction. Suppose $H \subseteq G$ is a subgroup and

$$\cdots \to Q_2 \to Q_1 \to Q_0 \to \mathbb{Z} \to 0$$

is a resolution of $\mathbb{Z}$ by projective left $\mathbb{Z}[H]$-modules. Since $\mathbb{Z}[G]$ is a right flat (in fact free) $\mathbb{Z}[H]$-module, the sequence

$$\cdots \to \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} Q_2 \to \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} Q_1 \to \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} Q_0 \to \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} \mathbb{Z} \to 0$$

is exact, and is thus a resolution of $\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} \mathbb{Z}$ by projective left G-modules. If M is a G-module, the adjunction isomorphism induces isomorphisms

$$\mathrm{Hom}_H(Q., M) \xrightarrow{\sim} \mathrm{Hom}_G(\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} Q., M)$$

from which we get a functorial isomorphism

$$H^n(H, M) \xrightarrow{\sim} \mathrm{Ext}^n_G(\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} \mathbb{Z}, M) \tag{3.2.4.1}$$

for all $n \geq 0$.

The same argument applies if $Q. \to \mathbb{Z}$ is a resolution by projective right $\mathbb{Z}[H]$-modules, and then the isomorphisms

$$(Q. \otimes_{\mathbb{Z}[H]} \mathbb{Z}[G]) \otimes_{\mathbb{Z}[G]} M \simeq Q. \otimes_{\mathbb{Z}[H]} M$$

induce functorial isomorphisms

$$H_n(H, M) \simeq \mathrm{Tor}^G_n(\mathbb{Z} \otimes_{\mathbb{Z}[H]} \mathbb{Z}[G], M). \tag{3.2.4.2}$$

When $H \subseteq G$ is a subgroup of finite index there is a morphism of left G-modules $\tau : \mathbb{Z} \to \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} \mathbb{Z}$ defined by choosing a set S of coset representatives of G/H and setting

$$\tau(n) = \sum_{x \in S} x \otimes n. \tag{3.2.4.3}$$

In fact for any $g \in G$,

$$g\tau(n) = g \sum_{x \in S} x \otimes n = \sum_{x \in S} \sigma(x) g \otimes n = \sum_{x \in S} \sigma(x) \otimes n = \tau(gn)$$

where σ is some permutation of S. Combining this morphism with the isomorphism 3.2.4.1 yields a functorial morphism

$$\mathrm{Cor}^G_H : H^n(H, M) \to H^n(G, M) \tag{3.2.4.4}$$

called the *corestriction*. Similarly the map $\rho : \mathbb{Z} \to \mathbb{Z} \otimes_{\mathbb{Z}[H]} \mathbb{Z}[G]$ defined by

$$\rho(n) = \sum_{x \in S} n \otimes x \tag{3.2.4.5}$$

is a morphism of right G-modules, which when combinened with 3.2.4.2 yields the corestriction

$$\mathrm{Cor}^H_G : H_n(G, M) \to H_n(H, M) \tag{3.2.4.6}$$

in homology.

We see from the construction that that the corestriction is compatible with the connecting homomorphism:

$$0 \to A \to B \to C \to 0$$

is a short exact sequence of G-modules, the diagrams

$$\begin{tikzcd} H^n(H,C) \arrow[r, "\partial"] \arrow[d, "\mathrm{Cor}"] & H^{n+1}(H,A) \arrow[d, "\mathrm{Cor}"] \\ H^n(G,C) \arrow[r, "\partial"] & H^{n+1}(G,A) \end{tikzcd} \qquad \begin{tikzcd} H_{n+1}(H,C) \arrow[r, "\partial"] \arrow[d, "\mathrm{Cor}"] & H_n(H,A) \arrow[d, "\mathrm{Cor}"] \\ H_{n+1}(G,C) \arrow[r, "\partial"] & H_n(G,A) \end{tikzcd} \tag{3.2.4.7}$$

are commutative.

3.2.4.1 Proposition *The for any subgroup $H \subseteq G$ of finite index the composition*

$$H^n(G,M) \xrightarrow{\mathrm{Res}} H^n(H,M) \xrightarrow{\mathrm{Cor}} H^n(G,M)$$

is multiplication by $[G:H]$.

Proof. For $n=0$, $\mathrm{Cor} \circ \mathrm{Res}$ is the composition

$$\mathrm{Hom}_G(\mathbb{Z},M) \to \mathrm{Hom}_H(\mathbb{Z},M) \xrightarrow{\sim} \mathrm{Hom}_G(\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} \mathbb{Z}, M) \to \mathrm{Hom}_G(\mathbb{Z},M).$$

An element of $\mathrm{Hom}_G(\mathbb{Z},M)$ is a function sending $1 \mapsto m$ for some $m \in M^G$. Its composition with τ sends $1 \mapsto \sum_{x \in S} x \otimes m$, and the image of this under the adjunction sends 1 to

$$\sum_{x \in S} xm = |S|m = [G:H]m.$$

The assertion is therefore true in cohomology for $n=0$. The proof in homology is similar.

If the assertion has been proven for n, apply 3.2.4.7 to the short exact sequence 3.2.3.5. Combining this with another obvious commutative square yields

$$\begin{tikzcd} H^n(G,M') \arrow[r, "\partial"] \arrow[d, "\mathrm{Cor}\circ\mathrm{Res}"] & H^{n+1}(G,M) \arrow[d, "\mathrm{Cor}\circ\mathrm{Res}"] \\ H^n(G,M') \arrow[r, "\partial"] & H^{n+1}(G,M) \end{tikzcd} .$$

The horizontal arrows are isomorphisms, and by induction the left vertical arrow is multiplication by $[G:H]$; the same is then true of the right one. Similarly for homology. ■

3.2.4.2 Corollary *If G is a finite group then*

$$|G|H^n(G,M) = 0$$

for all $n > 0$ and all G-modules M.

Proof. Apply the proposition with $H = 1$. ■

3.2.4.3 Corollary *If G is a finite group and M is a $\mathbb{Q}$-vector space, $H^n(G, M) = 0$ for all $n > 0$.*

Proof. By the last corollary it suffices to show that the $H^n(G, M)$ are also $\mathbb{Q}$-vector spaces. In fact this is true for the individual terms of $\mathrm{Hom}_G(B., M)$, and so true for $H^n(G, M)$ as well. ■

3.2.4.4 Example. If G is finite, the last corollary shows that the long exact sequence arising from

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$$

breaks up into isomorphisms

$$\partial : H^{n-1}(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\sim} H^n(G, \mathbb{Z})$$

for all $n > 1$. When $n = 2$ the isomorphism $H^1(G, \mathbb{Q}/\mathbb{Z}) \simeq \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$ yields

$$\partial : \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\sim} H^2(G, \mathbb{Z}) \tag{3.2.4.8}$$

The formula for the coboundary shows that 3.2.4.8 is computed as follows: given a homomorphism $f : G \to \mathbb{Q}/\mathbb{Z}$, choose for each $s \in G$ a $b_s \in \mathbb{Z}$ reducing to $f(s)$ in $\mathbb{Z}/\mathbb{Z}$; then

$$\partial f = (a_{s,t}) \qquad a_{s,t} = b_s + b_t - b_{st}. \tag{3.2.4.9}$$

The case $G = \mathbb{Z}/n\mathbb{Z}$ will be particularly important later. The group $\mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$ has a canonical generator, which sends the class of i mod n to $i/n \in \mathbb{Q}/\mathbb{Z}$. For a splitting of $\mathbb{Q} \to \mathbb{Q}/\mathbb{Z}$ we take for each $a \in \mathbb{Q}/\mathbb{Z}$ the unique element of $\mathbb{Q} \cap [0, 1)$ reducing to a. If on the other hand we identify elements of $\mathbb{Z}/n\mathbb{Z}$ with their unique representatives in the interval $[0, n)$, we find

$$a_{i,j} = \left[\frac{i+j}{n}\right] = \begin{cases} 0 & i + j < n \\ 1 & i + j \geq n. \end{cases} \tag{3.2.4.10}$$

We now have a means of constructing elements of $H^2(G, A)$ when A is any G-module: for any $a \in A^G$ there is a homomorphism $f : \mathbb{Z} \to A$ of G-modules sending 1 to a. The induced homomorphism $H^2(G, \mathbb{Z}) \to H^2(G, A)$ maps the class of the cocycle just constructed to

$$f(a_{i,j}) = \begin{cases} 0 & i + j < n \\ a & i + j \geq n. \end{cases} \tag{3.2.4.11}$$

The extensions of $\mathbb{Z}/n\mathbb{Z}$ by A that arise from these cocycles have the following description; we will use multiplicative notation for A since this will look more natural for later applications. If in the notation of section 3.1.4 we set $x = (1, 1)$, and identify A with a subgroup of the the extension E, then any element of E

has a unique expression ux^i with $u \in A$ and $0 \le i < n$. The group law is then a consequence of the relations

$$x^n = a, \qquad xb = {}^s bx \qquad b \in A \tag{3.2.4.12}$$

where $s : A \to A$ is action of $1 \in \mathbb{Z}/n\mathbb{Z}$ on A.

3.2.4.5 Corollary *If G is a finite group and M is a finitely generated G-module, $H^n(G, M)$ is a finite group for all $n > 0$.*

Proof. If M is finitely generated, the $\mathrm{Hom}(B_i, M)$ are finitely generated abelian groups for all n. The same is follows for the $H^n(G, M)$, and the assertion follows from corollary 3.2.4.2. ■

We now explicate the corestriction in homology for $n = 1$ and $M = \mathbb{Z}$, using the isomorphism $H_1(G, \mathbb{Z}) \simeq G^{ab}$. Recall that this arises as the composition of the connecting homomorphism $H_1(G, \mathbb{Z}) \xrightarrow{\partial} H_0(G, I_G)$ and the isomorphisms $H_0(G, I_G) \simeq I_G/I_G^2 \simeq G^{ab}$, where the latter identifies the s in G^{ab} with the class of $(s-1)$ in I_G/I_G^2, or equivalently the class of $1 \otimes (s-1) \in \mathbb{Z} \otimes I_G$. Since $\mathbb{Z}[G]$ is free both as a right G-module and as a right H-module we may use the exact sequence

$$0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$$

to compute both $H_1(G, \mathbb{Z})$ and $H_1(H, \mathbb{Z})$. This gives rise to a commutative diagram

$$\begin{tikzcd}
H_1(G,\mathbb{Z}) \arrow[r] \arrow[d, "\mathrm{Cor}"] & \mathbb{Z} \otimes_{\mathbb{Z}[G]} I_G \arrow[d, "\mathrm{Cor}"] \\
H_1(H,\mathbb{Z}) \arrow[r] \arrow[d, equal] & \mathbb{Z} \otimes_{\mathbb{Z}[H]} I_G \\
H_1(H,\mathbb{Z}) \arrow[r] & \mathbb{Z} \otimes_{\mathbb{Z}[H]} I_H \arrow[u]
\end{tikzcd}$$

in which the top and bottom horizontal arrows are isomorphisms and the middle one is injective; this implies that $\mathbb{Z} \otimes_H I_H \to \mathbb{Z} \otimes_H I_G$ is injective. The right hand corestriction takes $1 \otimes (s-1) \in \mathbb{Z} \underset{G}{\otimes} I_G$ to

$$\sum_{x \in H \backslash G} (1 \underset{H}{\otimes} x) \underset{G}{\otimes} (s-1) = \sum_{x \in H \backslash G} 1 \underset{H}{\otimes} (xs - x)$$

where the sum is over a set of right coset representatives. For every such x there is an $h_x(s) \in H$ such that $xs = h_x(s)\sigma(x)$ for some permutation of $H \backslash G$. Then

$$\begin{aligned} xs - x &= h_x(s)\sigma(x) - x \\ &= h_x(s)(\sigma(x) - 1) + (h_x(s) - 1) - (x - 1) \end{aligned}$$

in I_G, and

$$\begin{aligned} 1 \underset{H}{\otimes} (xs - x) &= 1 \underset{H}{\otimes} h_x(s)(\sigma(x) - 1) + 1 \underset{H}{\otimes} (h_x(s) - 1) - 1 \underset{H}{\otimes} (x - 1) \\ &= 1 \underset{H}{\otimes} (\sigma(x) - 1) + 1 \underset{H}{\otimes} (h_x(s) - 1) - 1 \underset{H}{\otimes} (x - 1) \end{aligned}$$

in $\mathbb{Z} \underset{H}{\otimes} I_G$. Summing over x yields

$$\sum_{x \in H \backslash G} 1 \underset{H}{\otimes} (xs - x) = \sum_{x \in H \backslash G} 1 \underset{H}{\otimes} (h_x(s) - 1)$$

Since $\mathbb{Z} \otimes_H I_H \to \mathbb{Z} \otimes_H I_G$ is injective we have proven the following formula for $\mathrm{Cor} : H_1(G, \mathbb{Z}) \to H_1(H, \mathbb{Q})$ viewed as a map $G^{ab} \to H^{ab}$: choose a set of coset representatives x of $H \setminus G$ and for $s \in G$ find a permutation σ of $H \setminus G$ such that $xs = h_x(s)\sigma(x)$; then

$$\mathrm{Cor}(s) = \prod_x h_x(s) \quad \text{in } H^{ab} \tag{3.2.4.13}$$

where we have reverted to multiplicative notation. This is traditionally called the *transfer* in group theory, and sometimes written $\mathrm{Ver} : G^{ab} \to H^{ab}$ (German *Verlagerung*); this usage is sometimes used in group cohomology.

3.3 Tate Cohomology

3.3.1 The Tate groups. When G is a finite group, Tate discovered that the cohomology and homology of a G-module M could be "spliced together" to obtain a set of functors $\hat{H}^n(G, M)$ defined for all $n \in \mathbb{Z}$, and with analogous formal properties (long exact sequence, restriction and corestriction...). The key is that the map

$$N_G : M \to M \qquad N_G(m) = \sum_{g \in G} gm \tag{3.3.1.1}$$

evidently takes its values in the submodule M^G. Its kernel contains $I_G M$ since the latter is generated by elements of the form $(g - 1)m$ for all $m \in M$, which are obviously annihilated by N_G. Therefore N_G defines a map $M_G \to M^G$ and we define the groups $\hat{H}^{-1}(G, M)$, $\hat{H}^0(G, M)$ by the exactness of

$$0 \to \hat{H}^{-1}(G, M) \to M_G \xrightarrow{N_G} M^G \to \hat{H}^0(G, M) \to 0. \tag{3.3.1.2}$$

In particular $\hat{H}^{-1}(G, M)$ is a subgroup of $H_0(G, M)$ and $\hat{H}^0(G, M)$ is a quotient of $H^0(G, M)$. The groups for $n \neq -1$, 0 are defined by

$$\hat{H}^n(G, M) = \begin{cases} H^n(G, M) & n > 0 \\ H_{-n-1}(G, M) & n < -1. \end{cases} \tag{3.3.1.3}$$

Observe that:

(i). $\hat{H}^0(G, M) = 0$ if and only if any $m \in M^G$ can be written $m = N_G(m')$ for some $m' \in M$;

(ii). $\hat{H}^{-1}(G, M) = 0$ if and only if any $m \in M$ such that $N_G(m) = 0$ is in $I_G M$.

If

$$0 \to A \to B \to C \to 0$$

is a short exact sequence the diagram

$$\begin{tikzcd}
H_1(G,C) \arrow[r] \arrow[d] & A_G \arrow[r] \arrow[d, "N_A"] & B_G \arrow[r] \arrow[d, "N_B"] & C_G \arrow[r] \arrow[d, "N_C"] & 0 \arrow[d] \\
0 \arrow[r] & A^G \arrow[r] & B^G \arrow[r] & C^G \arrow[r] & H^1(G,A)
\end{tikzcd}$$

is commutative, and the serpent lemma yields an exact sequence

$$\hat{H}^{-1}(G, A) \to \hat{H}^{-1}(G, B) \to \hat{H}^{-1}(G, C) \xrightarrow{\partial} \hat{H}^0(G, A) \to \hat{H}^0(G, B) \to \hat{H}^0(G, C). \tag{3.3.1.4}$$

The map ∂ is computed in the usual way: given $c \in \hat{H}^{-1}(G, C)$, lift it to a $\bar{c} \in B_G$. Then $N_B(\bar{c})$ is an element of A^G and its image in $\hat{H}^0(G, A)$ is independent of the choice of $\bar{c}$; this image is $\partial(c)$. Combining this with the long exact sequences of homology and cohomology, we find:

3.3.1.1 Theorem *For any short exact sequence*

$$0 \to A \to B \to C \to 0$$

there is a long exact sequence

$$\to \hat{H}^n(G, A) \to \hat{H}^n(G, B) \to \hat{H}^n(G, C) \xrightarrow{\partial} \hat{H}^{n+1}(G, A) \to \tag{3.3.1.5}$$

where for $n \neq -1$, ∂ is the coboundary for homology or cohomology.

If G is a finite group there is an isomorphism

$$C \otimes_{\mathbb{Z}} A \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{Z}}(C^*, A) \tag{3.3.1.6}$$

for any finite free $\mathbb{Z}[G]$-module C and abelian group A. The map 3.3.1.6 is defined by taking $c \otimes a$ to the function which to a homomorphism $f : C \to \mathbb{Z}$ assigns the value $f(c)a$. For $C = \mathbb{Z}[G]$ this shows that induced and coinduced G-modules are one and the same.

Furthermore if M is induced, $\hat{H}^{-1}(G, M) = \hat{H}^0(G, M) = 0$; it suffices to check the case $M = \mathbb{Z}[G]$, which is easy. From this we see that the dimension-shifting technique used in regular homology and cohomology can be used in Tate cohomology as well. In fact any module is a quotient of an induced module and a submodule of a coinduced module, so the groups can be shifted either way.

There is a version of the inflation-restriction exact sequence for the groups in degree 0 and -1:

3.3.1.2 Lemma *Suppose G is a finite group, $H \subseteq G$ is a normal subgroup, and M is a G-module. If*

$$\hat{H}^{-1}(H, M) = \hat{H}^0(H, M) = \hat{H}^{-1}(G/H, M^H) = 0$$

then $\hat{H}^{-1}(G, M) = 0$.

Proof. We must show that if $m \in M$ and $N_G(m) = 0$ then $m \in I_G M$. Now $N_H(m) \in M^H$ and $N_G(m) = N_{G/H} N_H(m)$, so the vanishing of $\hat{H}^{-1}(G/H, M^H)$ implies that

$$N_H(m) = \sum_{s \in G/H} (s-1) m_s$$

where $m_s \in M^H$, and the s are any set of representatives of G/H. Since $\hat{H}^0(H, M) = 0$ we may then write

$$m_s = N_H(n_s)$$

with $n_s \in M$. Then

$$\begin{aligned} N_H(m) &= \sum_{s \in G/H} (s-1) N_H(n_s) \\ &= \sum_{s \in G/H} N_H((s-1) n_s) \end{aligned}$$

where the second equality holds because H is normal in G. Therefore

$$N_H(m - \sum_{s \in G/H} (s-1) n_s) = 0$$

and the vanishing of $\hat{H}^{-1}(H, M)$ impliess that there are $r_t \in M$ for $t \in H$ such that

$$m - \sum_{s \in G/H} (s-1) n_s = \sum_t (t-1) r_t.$$

Then

$$m = \sum_{s \in G/H} (s-1) n_s + \sum_t (t-1) r_t \in I_G M$$

as required. ■

3.3.2 The double-bar complex Another definition of the $\hat{H}^n(G, M)$ will be useful in establishing other properties of these groups. As we showed in section 3.1.2, $\mathbb{Z}$ has a resolution $\check{B}. \to \mathbb{Z}$ by right G-modules whose terms are those of the bar resolution and with differentials given by 3.1.2.11. Now for any right G-module M, the $\mathbb{Z}$-dual $M^* = \mathrm{Hom}(M, \mathbb{Z})$ has a left G-module structure arising from the right action of G on M, and if $M \to N$ is a homomorphism of

right G-modules, $N^* \to M^*$ is a homomorphism of left G-modules. Since G is finite and each $\check{B}_n$ is free, the $\mathbb{Z}$-linear dual

$$0 \to \mathbb{Z} \xrightarrow{\epsilon^*} \check{B}_0^* \xrightarrow{d_0^*} \check{B}_1^* \xrightarrow{d_1^*} \check{B}_2^* \to \tag{3.3.2.1}$$

of the bar resolution is an acyclic complex of left G-modules.

For $n < 0$ we define $B_n = \check{B}^*_{-n-1}$ and

$$d_n = \begin{cases} \epsilon^* \circ \epsilon & n = -1 \\ d_n = d^*_{-n-1} & n < -1. \end{cases}$$

Then the bar resolution and 3.3.2.1 can be spliced together at the $\mathbb{Z}$ term, yielding an infinite acyclic complex

$$\to B_2 \xrightarrow{d_1} B_1 \xrightarrow{d_0} B_0 \xrightarrow{d_{-1}} B_{-1} \xrightarrow{d_{-2}} B_{-2} \to \tag{3.3.2.2}$$

which we will call the *double-bar complex*. We will produce isomorphisms

$$\hat{H}^n(G, M) \simeq \mathrm{Ker}(d_n^M)/\mathrm{Im}(d_{n-1}^M) \tag{3.3.2.3}$$

for all n, where as before $d_n^M : \mathrm{Hom}_G(B_n, M) \to \mathrm{Hom}_G(B_{n+1}, M)$. In fact for $n > 0$ the B_n and d_n are the same as before, and 3.3.2.3. For $n < -1$ we first observe that since the $\hat{H}^0$ and $\hat{H}^{-1}$ of an induced module vanish, the homomorphism

$$(C \otimes M)_G \xrightarrow{N} (C \otimes M)^G$$

is an isomorphism for any finite free G-module C. From this we get an isomorphism

$$C \otimes_{\mathbb{Z}[G]} M \simeq (C \otimes M)_G \xrightarrow{N} (C \otimes M)^G \simeq \mathrm{Hom}_{\mathbb{Z}}(C^*, M)^G \simeq \mathrm{Hom}_{\mathbb{Z}[G]}(C^*, M) \tag{3.3.2.4}$$

and taking for C the terms of the bar resolution, further isomorphisms

$$B_{-n-1} \otimes_{\mathbb{Z}[G]} M \simeq \mathrm{Hom}_G(\check{B}^*_{-n-1}, M) \simeq \mathrm{Hom}_G(\check{B}_n, M)$$

for all $n < 0$. For $n < -1$ these identify $d_n^* \otimes id_M = d_{-n-1} \otimes id_M$, so again the isomorphism is obvious.

The cases $n = 0, -1$ require a construction that we will need in greater generality later on. Recall that if M and N are free $\mathbb{Z}$-modules, an isomorphism $N \to M^*$ corresponds to a nondegenerate pairing $\langle\ ,\ \rangle : M \times N \to \mathbb{Z}$. If M (resp. N) is a right (resp. left) G-module the isomorphism $N \to M^*$ is G-linear if and only if

$$\langle ms, n\rangle = \langle m, sn\rangle \tag{3.3.2.5}$$

for all $s \in G$. Suppose finally that M is free G-module with basis $m_1, \ldots, m_r$, so that the $m_i s$ for all i and $s \in G$ are a $\mathbb{Z}$-basis of M. There are $n_1, \ldots, n_r \in N$ such that $\langle m_i, n_j\rangle = \delta_{ij}$, and the isomorphism $N \to M^*$ identifies $\{s^{-1}n_i\}$ with the dual basis to $\{m_i s\}$; in particular N is a free G-module.

We will apply this construction to the modules B_n, $\check{B}_n$ which are the free left and right G-modules on the set G^n. The pairing

$$\check{B}_n \times B_n \to \mathbb{Z} \tag{3.3.2.6}$$

defined, for β, $\gamma \in G^n$ by

$$\langle \beta t, s\gamma \rangle = \begin{cases} 1 & \beta = \gamma,\ s = t^{-1} \\ 0 & \text{otherwise.} \end{cases} \tag{3.3.2.7}$$

satisfies the linearity condition 3.3.2.5, and the resulting isomorphism $\check{B}_n^* \xrightarrow{\sim} B_n$ will also be written

$$B_n^* \xrightarrow{\sim} B_{-n-1}. \tag{3.3.2.8}$$

Note that in 3.3.2.7 we could replace the condition $\beta = \gamma$ by $\beta = \pi(\gamma)$ for any permutation π of G^n. The condition $s = t^{-1}$ is of course essential.

The dual of the augmentation $\epsilon : B_0 \to \mathbb{Z}$ is

$$\epsilon(1) = \sum_{s \in G} s[\ ]$$

since $\epsilon(1)$ must have inner product 1 with every $[\ ]s$. With the above identifications the differential $d_{-1} : B_0 \to B_{-1}$ is

$$d[\ ] = \sum_{s \in G} s[\ ]. \tag{3.3.2.9}$$

For any left G-module M the identification $\mathrm{Hom}_G(\check{B}_0, M) \simeq M$ associates to $f : B_0 \to M$ the element $f(1) \in M$. If we set

$$\nu = \sum_{s \in G} s \in \mathbb{Z}[G]$$

and use the previous identification of B_{-1} with B_0, the map $\mathrm{Hom}_G(B_{-1}, M) \to \mathrm{Hom}_G(B_0, M)$ induced by d_{-1} is the map induced by multiplication by ν, or in other words the norm map $N_G : M \to M$. Therefore the relevant part of the complex $\mathrm{Hom}_{\mathbb{Z}[G]}(B., M)$, which is

$$\mathrm{Hom}_{\mathbb{Z}[G]}(B_{-2}, M) \to \mathrm{Hom}_{\mathbb{Z}[G]}(B_{-1}, M) \to \mathrm{Hom}_{\mathbb{Z}[G]}(B_0, M) \to \mathrm{Hom}_{\mathbb{Z}[G]}(B_1, M)$$

can be identified with

$$B_1 \otimes_G M \to M_G \xrightarrow{N_G} M^G \to \mathrm{Hom}_G(B_1, M)$$

where the terms are in degrees -2 to 1. It follows that

$$H^{-1}(\mathrm{Hom}_G(B., M) \simeq \hat{H}^{-1}(G, M), \quad H^0(\mathrm{Hom}_G(B., M) \simeq \hat{H}^0(G, M)$$

as required.

Later we will need the explicit formula for $d_{-2} : B_{-1} \to B_{-2}$, viewed as a map $d : B_1 \to B_0$. If we write

$$d[\ ] = \sum_{s,t \in G} a_{s,t} s[t]$$

then

$$\begin{aligned} a_{s,t} &= \langle [t]s^{-1}, d[\ ] \rangle = \langle d([t]s^{-1}), [\ ] \rangle \\ &= \langle [\ ]ts^{-1}, [\ ] \rangle - \langle [\ ]s^{-1}, [\ ] \rangle \\ &= \begin{cases} 1 & s = t,\ s \neq 1 \\ -1 & s = 1,\ t \neq s \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

Therefore $d : B_1 \to B_0$ is

$$d[\ ] = \sum_{s \neq 1} (s-1)[s] = \sum_{s} (s-1)[s]. \tag{3.3.2.10}$$

3.3.3 Cyclic groups. We have seen that the homology and cohomology of a finite cyclic group is "nearly periodic" (equations 3.1.7.3, 3.1.7.4). The Tate groups in this case are completely periodic:

3.3.3.1 Proposition *Suppose G is a finite cyclic group and A is a G-module. For all $n \in \mathbb{Z}$,*

$$\hat{H}^n(G, A) = \begin{cases} A^G / N_G A & n \text{ even} \\ \operatorname{Ker}(N_G)/I_G A & n \text{ odd.} \end{cases} \tag{3.3.3.1}$$

Proof. We have already proven this if $n < -1$ or $n > 0$, and for $n = -1$, 0 we use the exact sequence 3.3.1.2. ■

Later it will be useful to have an explicit identification

$$\hat{H}^0(G, \mathbb{Z}) \simeq \hat{H}^2(G, \mathbb{Z}) \simeq H^2(G, \mathbb{Z}).$$

Recall from example 3.2.4.4 that if $G \simeq \mathbb{Z}/n\mathbb{Z}$, $H^2(G, \mathbb{Z})$ is cyclic of order n, generated by the class of the 2-cocycle

$$a = (a_{i,j}), \quad a_{i,j} = \begin{cases} 0 & i + j < n \\ 1 & i + j \geq n \end{cases}$$

where as before we identify i modulo n with an integer in the range $[0, n)$. As in section 3.1.7, the isomorphisms 3.3.3.1 in positive degree are induced by the chain map $F : C_\cdot \to B_\cdot$ which in degree two is

$$F(e_2) = \sum_{0 \leq i < n} [i|1]$$

and the map $H^0(G,\mathbb{Z}) \to H^2(G,\mathbb{Z})$ factors through the map $\hat{H}^0(G,\mathbb{Z}) \to H^2(G,\mathbb{Z})$ that we wish to compute. Since

$$a(F(e_2)) = \sum_{0\le i<n} a([i|1]) = \sum_{0\le i<n} a_{i.1} = 1$$

we see that the image of $1 \in \mathbb{Z}$ in $\hat{H}^0(G,\mathbb{Z}) \simeq \mathbb{Z}/n\mathbb{Z})$ maps to the class of the 2-cocycle a.

3.3.4 Products. Let's recall some general results from homological algebra. For the moment let R be any ring and let A and B be (left) R-modules. An exact sequence

$$0 \to B \to E_{n-1} \to \cdots \to E_0 \to A \to 0 \tag{3.3.4.1}$$

of length $n+2$ is called a *Yoneda n-extension* of A by B. These form a category in a manner similar to the category $\mathrm{EXT}(G,A)$ that was considered in section 3.1.4: morphisms are morphisms of complexes inducing the identity on A and B.

Suppose now

$$0 \to C \to F_{m-1} \to \cdots \to F_0 \to B \to 0 \tag{3.3.4.2}$$

is an m-extension of B by C. We can join this exact sequence to 3.3.4.1 at their common term B, leading to an $(m+n)$-extension

$$0 \to C \to F_{m-1} \to \cdots \to F_0 \to E_{n-1} \to \cdots \to E_0 \to A \to 0 \tag{3.3.4.3}$$

which we will call the result of *splicing* together 3.3.4.2 and 3.3.4.1. If we denote the exact sequences 3.3.4.1 and 3.3.4.2 by $E.$ and $F.$ respectively we will denote by $F.\circ E.$ the result of splicing the two extensions. This construction has obvious functorial properties: a morphism $u : E. \to E'_.$ of n-extensions of A by B induces a morphism $F.\circ E. \to F.\circ E'_.$, and similarly a morphism $u : F. \to F'_.$ of m-extensions of B by C induces a morphism $F.\circ E. \to F'_.\circ E.$. Furthermore this operation is associative in an obvious sense: for any p-extension $G.$ of C by D there is an isomorphism

$$(G.\circ F.)\circ E. \simeq G.\circ (F.\circ E.)$$

in the category of $(m+n+p)$-extensions of A by D.

An n-extension 3.3.4.1 gives rise an element of $\mathrm{Ext}^n_R(A,B)$ by the following well-known procedure: for any projective resolution $P. \to A$ of A there is a morphism of complexes

$$\begin{tikzcd}
P_{n+1} \arrow[r] \arrow[d] & P_n \arrow[r] \arrow[d, "f"] & P_{n-1} \arrow[r] \arrow[d] & \cdots \arrow[r] & P_0 \arrow[r] \arrow[d] & A \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & B \arrow[r] & E_{n-1} \arrow[r] & \cdots \arrow[r] & E_0 \arrow[r] & A \arrow[r] & 0
\end{tikzcd} \tag{3.3.4.4}$$

that is unique up to homotopy. The map $f : P_n \to B$ defines an element of $\mathrm{Ext}^n_R(A, B)$ which is independent of the choice of resolution, and which we will call the *class* of the extension.[1]

For any extensions $E.$, $F.$ as above the class of $F. \circ E.$ in $\mathrm{Ext}^{m+n}_R(A, C)$ depends only on the classes of $F.$ and $E.$ in $\mathrm{Ext}^m_R(B, C)$ and $\mathrm{Ext}^n_R(A, B)$. It follows that for any triple A, B, C of R-modules there is product operation

$$\mathrm{Ext}^m_R(B, C) \times \mathrm{Ext}^n_R(A, B) \to \mathrm{Ext}^{m+n}_R(A, C) \tag{3.3.4.5}$$

which on the level of extensions is obtained by the splicing operation. Since splicing is associative up to isomorphism, the product 3.3.4.5 is associative as well.

To show that 3.3.4.5 is well-defined and explain how it is computed we choose projective resolutions $P. \to A$, $Q. \to B$,

$$\cdots \to P_1 \to P_0 \to A \to 0$$
$$\cdots \to Q_1 \to Q_0 \to B \to 0$$

of A and B, and denote them by $P.$ and $Q.$ (writing $P_{-1} = A$, $Q_{-1} = B$). The identity maps of A and B extend to morphisms of complexes $P. \to E.$, $Q. \to F.$, unique up to homotopy, and the classes of 3.3.4.1 and 3.3.4.2 are represented the homomorphisms $f : P_n \to A$, $g : Q_m \to B$. Note that f factors through a map $\bar{f} : P_n/dP_{n+1} \to B$ and that $P. = P'_. \circ P''_.$ where $P''_.$ is an n-extension of A by P_n/dP_{n+1} and $P'_.$ is a projective resolution of P_n/dP_{n+1}. The situation is summarized by a commutative diagram which at the point of splicing is

$$\begin{tikzcd}
P_{n+1} \arrow[r] \arrow[d, dotted] & P_n \arrow[r] \arrow[d, dotted] \arrow[dr, "f"] \arrow[rr, bend left] & P_n/dP_{n+1} \arrow[r] \arrow[d, "\bar{f}"] & P_{n-1} \arrow[r] \arrow[d] & P_{n-2} \arrow[d] \\
Q_1 \arrow[r] & Q_0 \arrow[r] \arrow[rr, bend right] & B \arrow[r] & E_n \arrow[r] & E_{n-1}
\end{tikzcd}$$

Since P_n is projective and $Q_0 \to B$ is surjective we may fill in the arrow $P_n \to Q_0$, and by a general result of homological arrow we may fill in the remaining arrows to obtain a morphism of complexes $P. \to Q. \circ E.$ which we will also denote by $f.$.

Since $P. \to E.$ is only unique up to homotopy, $f. : P''_. \to E.$ is likewise unique up to homotopy; if $f'_.$ is a another choice, corresponding to $f' : P_n \to B$ we have $f' = f + gd$ with $d : P_n \to P_{n-1}$ and $g : P_{n-1} \to B$. Since P_{n-1} is projective

[1] This is only one possible converntion; for example in Bourbaki [2] the class of the extension 3.3.4.1 would be $(-1)^{n(n+1)/2} f$. This is done to improve the appearance of certain formulas.

we may lift g to a map $h : P_{n-1} \to Q_0$, and again by standard arguments this extends to a homotopy between the maps $f.,\ f' : P. \to Q. \circ E.$.

Thus $f. : E. \circ Q.$, and composing this with $Q. \to F.$ yields a morphism of complexes $P. \to F. \circ E.$. The term in degree $m+n$ is a map $P_{n+m} \to C$ factoring through the quotient P_{n+m}/dP_{n+m+1}, and this is the class of $F. \circ E.$. As it is completely determined by the maps $f : P_n \to B$, $g : Q_m \to C$, we have shown that 3.3.4.5 is well-defined. In fact the argument shows that the product can be computed from any morphism of complexes

$$\begin{tikzcd}
P_{m+n+1} \arrow[r] \arrow[d] & P_{m+n} \arrow[r] \arrow[d, "g"] & \cdots \arrow[r] & P_n \arrow[r] \arrow[d] & P_n/dP_{n+1} \arrow[r] \arrow[d, "\bar{f}"] & 0 \\
0 \arrow[r] & C \arrow[r] & \cdots \arrow[r] & F_0 \arrow[r] & B \arrow[r] & 0
\end{tikzcd} \tag{3.3.4.6}$$

where as above $\bar{f}$ is the factorization of the map $f : P_n \to B$ giving the class of $E.$. In fact the argument produced one such morphism, and any other is homotopic to it.

3.3.4.1 Proposition *Suppose that the class of the short exact sequence*

$$0 \to C \to E \to B \to 0 \tag{3.3.4.7}$$

is $\eta \in \mathrm{Ext}^1_R(B, C)$. *For any R-module C the map*

$$\eta\cup : \mathrm{Ext}^n_R(A, B) \to \mathrm{Ext}^{n+1}_R(A, C)$$

is the connecting homomorphism induced by 3.3.4.7.

Proof. This follows from the above construction and the explicit description of the coboundary map. ■

If we take $R = \mathbb{Z}[G]$ for any group G and recall $H^n(G, A) = \mathrm{Ext}^n_{\mathbb{Z}[G]}(\mathbb{Z}, A)$ we get a product operation

$$\mathrm{Ext}^m_{\mathbb{Z}[G]}(A, B) \times H^n(G, A) \to H^{m+n}(G, B) \tag{3.3.4.8}$$

which is associative in an obvious sense. To compute it we can use for $P.$ in the above construction any projective resolution of $\mathbb{Z}$, e.g. the bar complex. We will call this product the *cup product* (this is *not* standard terminology). We will write the operation 3.3.4.8 as $(e, a) \mapsto e \cup a$. Then proposition 3.3.4.1 yields:

3.3.4.2 Proposition *Let G be a group and suppose*

$$0 \to B \to E \to A \to 0$$

is a short exact sequence of G-modules. If $e \in \mathrm{Ext}^1_{\mathbb{Z}[G]}(A, B)$ is the class of this extension, then for any element $a \in H^n(G, A)$, the cup product $e \cup a$ is the image of a under the coboundary $\partial : H^n(G, A) \to H^{n+1}(G, B)$.

For $m \leq n$ there is a similar product

$$\mathrm{Ext}_R^m(B,C) \times \mathrm{Tor}_n^R(A,B) \to \mathrm{Tor}_{n-m}^R(A,C)$$

leading to a "cap product" in group homology

$$\mathrm{Ext}_R^m(B,C) \times H_n(G,B) \to H_{n-m}(G,C)$$

but we will lead the details to the reader. This can be combined with the product 3.3.4.8 to get a cup product in Tate cohomology

$$\mathrm{Ext}_{\mathbb{Z}[G]}^m(A,C) \times \hat{H}^n(G,A) \to \hat{H}^{m+n}(G,C) \tag{3.3.4.9}$$

for all $m \geq 0$ and $n \in \mathbb{Z}$. It is simpler however to proceed directly using the "double-bar" complex 3.3.2.2 and imitating the construction of 3.3.4.5 by means of 3.3.4.6. Suppose $n \in \mathbb{Z}$ and

$$0 \to C \to F_{m-1} \to \cdots \to F_0 \to A \to 0$$

is an m-extension of A by C with class $e \in \mathrm{Ext}_{\mathbb{Z}[G]}^m(A,C)$. An element α of $\hat{H}^n(G,A)$ is represented by a G-module map $f : B_n \to A$ vanishing on dB_{n+1}. Since B_n is projective this lifts to a map $B_n \to F_0$ which extends to a morphism

$$\begin{tikzcd}
B_{m+n+1} \arrow[r] \arrow[d] & B_{m+n} \arrow[r] \arrow[d, "g"] & \cdots \arrow[r] & B_n \arrow[r] \arrow[d] & B_n/dB_{n+1} \arrow[r] \arrow[d, "f"] & 0 \\
0 \arrow[r] & C \arrow[r] & \cdots \arrow[r] & F_0 \arrow[r] & A \arrow[r] & 0
\end{tikzcd}$$

of complexes. We define the cup product $e \cup \alpha$ to be the class of the map $g : B_{m+n} \to C$ in $\hat{H}^{m+n}(G,C)$. When $n > 0$, $\hat{H}^n(G,A) = H^n(G,A)$ and this construction is the same one as before. When $m = 1$ this is the coboundary in Tate cohomology; the proof is the same as that of proposition 3.3.4.1:

3.3.4.3 Proposition *Let G be a group and suppose*

$$0 \to C \to E \to A \to 0$$

is a short exact sequence of G-modules. If $e \in \mathrm{Ext}_{\mathbb{Z}[G]}^1(A,C)$ is the class of this extension, then for any element $\alpha \in \hat{H}^n(G,A)$, the cup product $e \cup \alpha$ is the image of α under the coboundary $\partial : \hat{H}^n(G,A) \to \hat{H}^{n+1}(G,C)$.

3.3.5 Duality in Tate cohomology. The duality formula 3.1.6.1 for homology and cohomology extends to a duality

$$\mathrm{Hom}(\hat{H}^{-n-1}(G,\mathbb{Z}),\mathbb{Q}/\mathbb{Z}) \simeq \hat{H}^n(G,\mathbb{Q}/\mathbb{Z}) \tag{3.3.5.1}$$

for the Tate groups. In fact for $n > 0$ this is exactly the formula 3.1.6.1; the general case is proven in the same way, only replacing the resolution $P.$ in section 3.1.6 by the double-bar complex $B.$ and using 3.3.2.3.

For positive n this duality can be expressed in terms of the cup product 3.3.4.9. In fact with $A = \mathbb{Z}$ and $C = \mathbb{Q}/\mathbb{Z}$, one case of 3.3.4.9 is

$$\mathrm{Ext}^n(\mathbb{Z}, \mathbb{Q}/\mathbb{Z}) \times \hat{H}^{-n-1}(G, \mathbb{Z}) \to \hat{H}^{-1}(G, \mathbb{Q}/\mathbb{Z}).$$

Since $n > 0$, $\mathrm{Ext}^n(\mathbb{Z}, \mathbb{Q}/\mathbb{Z}) = \hat{H}^n(G, \mathbb{Q}/\mathbb{Z})$ by definition, while on the other hand

$$\hat{H}^{-1}(G, \mathbb{Q}/\mathbb{Z}) = \mathrm{Ker}(N_G)|(\mathbb{Q}/\mathbb{Z})_G = \mathrm{Ker}(N_G)|\mathbb{Q}/\mathbb{Z} = \frac{1}{|G|}\mathbb{Z}/\mathbb{Z}$$

so the cup product is

$$\hat{H}^n(G, \mathbb{Q}/\mathbb{Z}) \times \hat{H}^{-n-1}(G, \mathbb{Z}) \to \frac{1}{|G|}\mathbb{Z}/\mathbb{Z} \tag{3.3.5.2}$$

and we can replace the right hand side by $\mathbb{Q}/\mathbb{Z}$ if we like since the Tate groups are killed by $|G|$.

[finish this]

3.4 Galois Cohomology

In this section L/K is a finite Galois extension and G is the Galois group $\mathrm{Gal}(L/K)$. Any abelian group M depending functorially on L is then a G-module, the most important cases being L and $L^\times$. In this section we focus on the cases when $n = 0$ or 1. The interpretation of $H^2(G, L^\times)$ will be discussed later.

3.4.1 General results. The computation of H^0 is simple:

$$H^0(G, L) = K, \qquad H^0(G, L^\times) = K^\times$$

and most importantly

$$\hat{H}^0(G, L^\times) = K^\times / N_{L/K} L^\times. \tag{3.4.1.1}$$

For the additive group we have more generally, if perhaps disappointingly,

3.4.1.1 Proposition *For $n > 0$,*

$$H^n(G, L) = 0.$$

Proof. This follows from the normal basis theorem, which says says that L is an induced G-module, and thus a coinduced G-module since G is finite. ■

The multiplicative case with $n = 1$ is known as *Hilbert's theorem 90*:

3.4.1.2 Theorem *With G and L as above,*

$$H^1(G, L^\times) = 0.$$

Proof. By Artin's theorem on the linear independence of characters, the maps $s : L^\times \to L$ induced by the $s \in G$ are linearly independent. Suppose now $a(s)$ is a 1-cocycle with values in $L^\times$. By Artin's theorem there is an $x \in L^\times$ such that

$$b = \sum_{s \in G} a(s)s(x) \neq 0.$$

Then for any $s \in G$,

$$s(b) = \sum_{t \in G} (sa(t))st(x) = \sum_{t \in G} (a(st)a(s)^{-1})st(x) = a(s)^{-1}b$$

and thus $a(s) = b \cdot s(b)^{-1}$ is a coboundary. ■

The version actually proven by Hilbert, however, was this:

3.4.1.3 Corollary *Suppose L/K is a cyclic Galois extension and $x \in L^\times$ is an element of norm 1. If s is a generator of* $\mathrm{Gal}(L/K)$, *$x = s(y)y^{-1}$ for some $y \in L^\times$.*

Proof. This follows from the theorem and the description of $H^1(G, M)$ in the cyclic case. ■

Theorem 3.4.1.2 is the tip of a fairly large algebraic iceberg: Galois descent, Grothendieck's theory of faithfully flat descent and the Barr-Beck theorem in category theory are all descendents of this simple-looking result.

3.4.2 The case of algebraically closed residue field. The main result of this section is that if the residue field of K is algebraically closed, the G-module $L^\times$ is cohomologically trivial. This is one of the key points in our treatment of local class field theory. Note that in this case the extension L/K is totally ramified.

3.4.2.1 Lemma *Let K be a discretely valued nonarchimedean field with algebraically closed residue field. If L/K is a finite Galois extension with group G, $L^\times$, $\hat{H}^0(G, L^\times) = 0$.*

Proof. This follows immediately from theorem 2.4.2.5, since $\hat{H}^0(G, L^\times) = K^\times / N_{L/K} L^\times$. ■

3.4.2.2 Lemma *Let K be a discretely valued nonarchimedean field with algebraically closed residue field. If L/K is a finite Galois extension with group G, $L^\times$, $\hat{H}^{-1}(G, L^\times) = 0$.*

Proof. The proof is by induction on the order of G, and the case of $|G| = 1$ is immediate. Since L/K is totally ramified G is solvable, and if it is nontrivial there is a normal subgroup $H \subset G$ with G/H cyclic and nontrivial. If M is the fixed field of H, $G/H \simeq \mathrm{Gal}(M/K)$; then Hilbert's theorem 90 and the periodicity of the cohomology of a cyclic group show that

$$\hat{H}^{-1}(G/H, (L^\times)^H) \simeq \hat{H}^{-1}(G/H, M^\times) \simeq \hat{H}^1(G/H, M^\times) = 0.$$

On the other hand the induction hypothesis yields $\hat{H}^{-1}(H, L^\times) = 0$, and we know that $\hat{H}^0(H, L^\times) = 0$ as well, so the lemma follows from lemma 3.3.1.2. ■

3.4.2.3 Corollary *With the above hypotheses, the natural homomorphism*

$$(L^\times)_G \to (L^\times)^G$$

is an isomorphism.

Proof. This follows from lemmas 3.4.2.1, 3.4.2.2 and the exact sequence

$$0 \to \hat{H}^{-1}(G, L^\times) \to (L^\times)_G \to (L^\times)^G \to \hat{H}^0(G, L^\times) \to 0.$$

■

3.4.2.4 Theorem *Let K be a discretely valued nonarchimedean field with algebraically closed residue field. If L/K is a finite Galois extension with group G, $L^\times$ is cohomologically trivial, i.e. $\hat{H}^n(G, L^\times) = 0$ for all n.*

Proof. The last two lemmas have shown this for $n = 0$ and -1, and the case $n = 1$ is theorem 90. If G is cyclic, the assertion follows from the periodicity of Tate cohomology of cyclic groups and the vanishing of $\hat{H}^0(G, L^\times)$ and $\hat{H}^1(G, L^\times)$.

We first treat the case $n \geq 2$ by induction on $|G|$, the assertion being trivial if $|G| = 1$. When $|G| \neq 1$ we can find a normal subgroup $H \subset G$ with G/H cyclic and nontrivial. If $H^i(G, L^\times) = 0$ for all $1 < i < n$ the exact sequence of proposition 3.2.3.5 yields

$$0 \to H^n(G/H, M^\times) \to H^n(G, L^\times) \to H^n(H, L^\times)$$

where $M = L^H$ is the fixed field of H. Then $H^n(G/H, M^\times) = 0$ by the cyclic case and $H^n(H, L^\times) = 0$ by the induction hypothesis, and it follows that $\hat{H}^n(G, L^\times) = H^n(G, L^\times) = 0$ for all $n \geq 1$.

It remains to show that $\hat{H}^n(G, L^\times) = 0$ for $n \leq -2$, or equivalently that $H_n(G, L^\times) = 0$ for all $n \geq 1$. Again we use induction on $|G|$. When $n = 1$ the exact sequence 3.2.2.2 is

$$H_1(H, L^\times) \to H_1(G, L^\times) \to H_1(G/H, (L^\times)_H) \to 0.$$

By corollary 3.4.2.3 and the cyclic case,

$$H_1(G/H, (L^\times)_H) \simeq H_1(G/H, (L^\times)^H) \simeq H_1(G/H, M^\times) = 0$$

where as before $M = L^H$. By induction $H_1(H, L^\times) = 0$, so $H_1(G/H, (L^\times)^G) = 0$ as well. Finally if $H_i(G, L^\times) = 0$ for $1 \leq i < n$, proposition 3.2.3.6 yields an exact sequence

$$H_n(H, L^\times) \to H_n(G, L^\times) \to H_n(G/H, (L^\times)_H) \to 0.$$

Again $(L^\times)_H \simeq (L^\times)^H \simeq M^\times$ and thus $H_n(G/H, (L^\times)_H) = 0$ by the cyclic case, while $H_n(H, L^\times) = 0$ by induction. We conclude that $H_n(G, L^\times) = 0$. ■

3.4.2.5 Remark. The theorem also from a fairly general criterion for cohomological triviality due to Tate and Nakayama: a G-module M is cohomologically trivial if for every p-Sylow subgroup $G_p \subseteq G$ there is an integer q such that $\hat{H}^q(G_p, M) = H^{q+1}(G_p, M) = 0$ (see [12, Ch. 9 §6 Th. 8] or [4, Ch. 4 §9 Th. 9]). This can be used in two ways. First, one can use lemma 3.4.2.1 and Hilbert's theorem 90, which shows that $\hat{H}^0(G_p, L^\times) = \hat{H}^1(G_p, L^\times) = 0$. Alternatively one could use the fact that $\mathrm{Br}(L/K) = 0$ for any finite Galois extension of nonarchimedean fields whose residue fields are separably closed; then $\hat{H}^1(G_p, L^\times) = \hat{H}^2(G_p, L^\times) = 0$.

Chapter 4

Central Simple Algebras and The Brauer Group

The determination of the Brauer group of local field is central to the cohomoligical approach to local class field theory (and correspondingly, the Brauer group of a global field in global class field theory). We will be more interested in the relative Brauer group attached to a finite Galois extension of local fields.

4.1 Central Simple Algebras

In this section we are concerned with some purely algebraic properties of central simple algebras. In this section k is a (commutative) field, unless otherwise specified.

4.1.1 Basic Results. We first recall two basic results on division algebras, whose proofs can be found in the standard references.

Recall that a K-algebra is a ring A and a ring homomorphism $k \to A$ such that the image of k is contained in the center of A. We say A is a *central k-algebra* if the image of $k \to A$ is the entire center of A. Finally a *central simple k-algebra* is a central k-algebra that is simple as a ring, i.e. its only 2-sided ideals are itself and the zero ideal. A central division algebra is automatically central simple.

When k is a field, the structure map $k \to A$ of a k-algebra is injective. In this case A is naturally k-vector space and the ring operations are k-linear. The *degree* of the k-algebra A is the (possibly infinite) dimension of A as a k-vector space, and is denoted by $[A : k]$ (just as for fields).

The structure of a central simple k-algebra of finite degree is given by the following theorem. In the statement we use the convention that if A is a ring and M is a left A-module, then endomorphism ring $\mathrm{End}_A(M)$ acts on M on the right.

4.1.1.1 Theorem *(Wedderbun-Artin) A simple left artinian ring A is isomorphic to a matrix ring $M_n(D)$, where D is the endomorphism ring of any simple left A-module.*

4.1.1.2 Corollary *Let k be a field. A central simple k-algebra of finite degree over k is isomorphic to a matrix ring $M_n(D)$ for some central division k-algebra D.*

Proof. Any such central simple algebra is artinian. ■

4.1.1.3 Corollary *If k is an algebraically closed field, a central simple k-algebra of finite k-dimension is isomorphic to $M_n(k)$.*

Proof. In fact k is the only division algebra of finite degree over k. ■

4.1.1.4 Theorem *(Noether-Skolem) Suppose k is a field, A is a central simple k-algebra of finite degree over k, B is a simple k-algebra and f, $g : B \to A$ are k-algebra homomorphisms. There is an a $b \in A$ such that $g = ad(b) \circ f$, i.e. such that $g(x) = bf(x)b^{-1}$ for all $x \in B$.*

Since f and g are necessarily injective, this can be rephrased (in fact usually is) as follows: If B and B' are any simple subalgebras of A, any isomorphism $B \to B'$ extends to an inner automorphism of A.

4.1.1.5 Corollary *If A is a central simple k-algebra of finite degree over k, any k-automorphism of A is inner.*

Proof. If α is an automorphism of A, apply the theorem with $f = \alpha$ and $g = id_A$. ■

4.1.2 Products. From now on k is a field, unless otherwise specified. If A and B are k-algebras, the product algebra $A \otimes_k B$ is the ordinary tensor product with its usual addition, and with multiplication defined by

$$(a \otimes b)(a' \otimes b') = aa \otimes bb'. \tag{4.1.2.1}$$

The map $A \to A \otimes_k B$ defined by $a \mapsto a$ is a k algebra homomorphism whose image we denote by $A \otimes 1$. When k is a field, $A \to A \otimes_k B$ is an isomorphism of A onto $A \otimes 1$. Likewise there is a k-algebra homomorphism $B \to A \otimes_k B$ with image $1 \otimes B$.

If A is a k-algebra and and $S \subseteq A$ is any subset, we denote by $C_A(S)$ the centralizer of S. It is a sub-k-algebra of A.

4.1.2.1 Proposition *Let A, A' be k-algebras and $B \subseteq A$, $B' \subseteq A'$ two k-subalgebras. Then*

$$C_{A \otimes_k A'}(B \otimes_k B') = C_A(B) \otimes_k C_{A'}(B'). \tag{4.1.2.2}$$

Proof. It is clear that $C_A(B) \otimes_k C_{A'}(B') \subseteq C_{A\otimes_k A'}(B \otimes_k B')$, so it suffices to show $C_{A\otimes_k A'}(B \otimes_k B') \subseteq C_A(B) \otimes_k C_{A'}(B')$.

We first observe that $C_{A\otimes_k A'}(B\otimes 1) \subseteq C(B)\otimes_k A'$. In fact if $(e_i)_{i\in I}$ is a basis of A' as a k-vector space then any $x \in A \otimes_k A'$ can be written uniquely as $x = \sum_i b_i \otimes e_i$ with $b_i \in B$. Then for $b \in B$, $x(b\otimes 1) = (b\otimes 1)x$ if and only if $bb_i = b_i b$, and if this holds for all $b \in B$ then $b_i \in C_A(B)$ and consequently $x \in C(B)\otimes_k A'$. This proves the stated inclusion, and by symmetry $C_{A\otimes_k A'}(1\otimes B') \subseteq A\otimes_k C(B')$. Since $C_{A\otimes_k A'}(B \otimes B')$ is a subring of $C_{A\otimes_k A'}(B \otimes 1)$ and $C_{A\otimes_k A'}(1 \otimes B')$,

$$C_{A\otimes_k A'}(B \otimes B') \subseteq (C(B) \otimes_k A') \cap (A \otimes C_{A'}B') = C_A(B) \otimes_k C_{A'}(B').$$

■

The following corollaries are immediate:

4.1.2.2 Corollary *The tensor product of two central k-algebras is central.*

4.1.2.3 Corollary *If D is a finite-dimensional division k-algebra, the diagonal embedding $Z(D) \to Z(M_n(D))$ is an isomorphism.*

Proof. Since $M_n(D) \simeq M_n(k) \otimes_k D$, we have

$$Z(M_n(D)) = Z(M_n(k)) \otimes_k Z(D) \simeq k \otimes_k Z(D) \simeq Z(D)$$

and the isomorphism $k \xrightarrow{\sim} Z(M_n(k))$ is the diagonal embedding of k. ■

Since the center of a division algebra is a field, we get:

4.1.2.4 Corollary *The center of a finite-dimensional simple k-algebra is a field.*

The product of two simple algebras is not necessarily simple, or even semisimple. We will see that this is the case, however if one is central simple. We will need the following bit of linear algebra. Let k be any division ring, V a left k-vector space and $\mathcal{B} = (e_i)_{i\in I}$ a basis of V (we do not assume V has finite k-dimension). For any $v \in V$ with $v = \sum_{i\in I} a_i v_i$ we denote by $J(v)$ the set of $i \in I$ such that $a_i \neq 0$. Thus $v = 0$ if and only if $J(v) = \emptyset$.

If $W \subseteq V$ is a subspace, an element $w \in W$ is *primordial* with respect to the basis $\mathcal{B}$ if at least one coefficient of w relative to $\mathcal{B}$ is 1, and $J(w)$ is minimal among the nonempty sets $J(v)$ for all $v \in W$. For example if $W = V$, the primordial elements are the elements of $\mathcal{B}$.

4.1.2.5 Lemma *Let V, $\mathcal{B}$ and $W \subseteq V$ be as above. (i) If $w \in W$ is primordial and $v \in W$ then $J(v) = J(w)$ if and only if v is a multiple of w. (ii) W is spanned by its set of primordial elements.*

Proof. (i) The condition is evidently sufficient, so suppose $J(v) = J(w)$ and $w = \sum_i a_i e_i$ with $a_j = 1$. If b_j is the coefficient of e_j in the expansion of v then

$J(v - b_j w)$ is a proper subset $J(w)$. Then $v - b_j w = 0$ by the minimality of $J(w)$.

(ii) We will show that any $v \in W$ is in the span of the primordial elements by induction on $|J(v)|$, and there is nothing to show if $|J(v)| = 0$. If $|J(v)| \neq 0$ pick $w \in W$ with $J(w) \subseteq J(v)$ with $J(w)$ is minimal. We can assume that w is primordial; then for some $c \in k$, $J(v - cw)$ is a proper subset of $J(v)$. If $v - cw = 0$ we are done; otherwise we conclude by induction. ■

We now revert to the situation in which k is a field.

4.1.2.6 Lemma *Suppose A is a k-algebra and D is a central division algebra over k. Any two-sided ideal $\mathfrak{a} \subset A \otimes_k D$ is generated as a left D-vector space by $\mathfrak{a} \cap A \otimes 1$. In particular, if A is simple then so is $A \otimes_k D$.*

Proof. The D-module structure of $A \otimes_k D$ is given by $x(a \otimes y) = a \otimes xy$, and we observe that $\mathfrak{a}$ is a D-subspace of $A \otimes_k D$. Choose a basis $(e_i)_{i \in I}$ of A as a k-vector space; then $\mathcal{B} = (e_i \otimes 1)_{i \in I}$ is a basis of $A \otimes_k D$ as a left D-vector space. Suppose $x \in \mathfrak{a}$ is primordial for $\mathfrak{a}$ and $\mathcal{B}$ and write $x = \sum_i e_i \otimes d_i$ with $d_j = 1$. For any $d \in D$,

$$x(1 \otimes d) = \sum_i e_i \otimes d_i d = \sum_i (1 \otimes d_i d)(e_i \otimes 1)$$

and therefore $J(x(1 \otimes d)) = J(x)$. By (i) of lemma 4.1.2.5, $x(1 \otimes d) = (1 \otimes d')x$ for some $d' \in D$, and since $d_j = 1$ we must have $d' = d$. Then $dd_i = d_i d$, i.e. $d_i \in Z(D) = k$ for all i, and $x = \sum_i e_i \otimes d_i = \sum_i d_i e_i \otimes 1 \in A \otimes 1$.

For the last assertion it suffices to observe that the homomorphism $A \to A \otimes_k D$ sending $a \mapsto a \otimes 1$ is nontrivial, and therefore injective, so we may identify $\mathfrak{a} \cap A \otimes 1$ with a two-sided ideal of A. This is either 0 or all of A, so $\mathfrak{a}$ is either 0 or $A \otimes_k D$. ■

4.1.2.7 Proposition *If A and B are simple finite-dimensional k-algebras and at least one is central simple, $A \otimes_k B$ is simple.*

Proof. We may suppose that B is central simple and write $B = M_n(D)$ for some finite-dimensional k-division algebra D. Then

$$A \otimes_k B = A \otimes_k M_n(D) \simeq M_n(A \otimes_k D)$$

and by lemma 4.1.2.6, $A \otimes_k D$ is simple. Since it has finite dimension over k, $A \otimes_k D \simeq M_m(D')$ for some division k-algebra D' and then $A \otimes_k B \simeq M_{mn}(D')$. ■

4.1.2.8 Theorem *If A and B are central simple k-algebras of finite dimension then $A \otimes_k B$ is central simple.*

Proof. This follows from propositions 4.1.2.1 and 4.1.2.7. ■

If A is a central simple algebra there is a natural k-algebra homomorphism

$$A \otimes_k A^{\mathrm{op}} \to \mathrm{End}_k(A) \tag{4.1.2.3}$$

which maps $a \otimes b \in A \otimes_k A^{\mathrm{op}}$ to the k-linear map $x \mapsto axb$.

4.1.2.9 Corollary *The map 4.1.2.3 is an isomorphism of k-algebras.*

Proof. The theorem says that $A \otimes_k A^{\mathrm{op}}$ is a simple k-algebra, and as 4.1.2.3 is not trivial it must be injective. Then

$$[A \otimes_k A^{\mathrm{op}} : k] = [A : k]^2 = (\dim_k A)^2 = \dim_k \mathrm{End}_k(A)$$

from which it follows that 4.1.2.3 must be surjective as well. ■

4.1.3 Base change. We now consider products where one factor is a field.

4.1.3.1 Proposition *Suppose A is a central simple k-algebra of finite dimension and K/k is any extension of fields. Then $A \otimes_k K$ is a central simple K-algebra.*

Proof. We can write $A = M_n(D)$ with D a central k-division algebra of finite dimension. Then $A \otimes_k K \simeq M_n(D \otimes_k K)$, so it suffices to show that $D \otimes_k K$ is central simple over K. By lemma 4.1.2.6 $D \otimes_k K$ is a simple; by proposition 4.1.2.1,

$$Z(D \otimes_k K) \simeq Z(D) \otimes_k Z(K) \simeq k \otimes_k K \simeq K$$

and thus $D \otimes_k K$ is central simple. ■

If A is a central simple k-algebra and K/k is an extension, we say that A *splits* over K if $A \otimes_k K \simeq M_n(K)$ for some n. For example, corollary 4.1.1.3 says that any central simple k-algebra of finite degree over k is split over the algebraic closure of k. We will eventually show that a central simple k-algebra of finite degree over k splits over a finite separable extension of k. If k is a local field, it splits over a finite unramified extension of k.

4.1.3.2 Corollary *If A is a central simple k-algebra of finite degree, $[A : k]$ is a square.*

Proof. In fact $[A : k] = [A \otimes_k k^{alg} : k^{alg}]$ and $A \otimes_k k^{alg}$ is a matrix algebra over k^{alg} by corollary 4.1.1.3. ■

4.1.3.3 Corollary *A central simple k-algebra of finite degree splits over a finite extension of k.*

Proof. For any such algebra A, $A \otimes_k k^{alg}$ is split, and the isomorphism $A \otimes_k k^{alg} \simeq M_n(k^{alg})$ only involves finitely many elements of k^{alg}. If K is the finite extension they generate, $A \otimes_k K \simeq M_n(K)$. ■

4.1.3.4 Lemma *Suppose B is a k algebra and let $\ell : B \to \mathrm{End}_k(B)$, $r : B^{\mathrm{op}} \to \mathrm{End}_k(B)$ be the embeddings given by left and right multiplication. Then $\ell(B)$ and $r(B)$ are each others' centralizers in $\mathrm{End}_k(B)$.*

Proof. The centralizer of $\ell(B)$ is the set of B-linear maps $f : B \to B$ where B is a left B-module in the usual way. If $f(1) = b$ and $x \in B$ then

$$f(x) = f(x \cdot 1) = xf(1) = xb$$

and consequently $f \in r(B^{\mathrm{op}})$. Thus the centralizer of $\ell(B)$ is contained in $r(B^{\mathrm{op}})$, and the converse inclusion is clear. The centralizer of $r(B^{\mathrm{op}})$ is treated similarly. ■

Note that the centralizer of $\ell(B)$ in $\mathrm{End}_k(B)$ is $\mathrm{End}_B(B)$. In fact it is standard that $\mathrm{End}_k(B^n) \simeq M_n(B^{\mathrm{op}})$.

The following is a version of what is sometimes called the double-centralizer theorem:

4.1.3.5 Theorem *Let A be a central simple k-algebra of finite degree and $B \subseteq A$ a simple sub-k-algebra. Then $C = C_A(B)$ is a simple k-algebra, $B = C_A(C)$ and*

$$[A : k] = [B : k][C : k]. \tag{4.1.3.1}$$

Proof. The k-algebra $D = A \otimes_k \mathrm{End}_k(B)$ is central simple over k by theorem 4.1.2.8. Consider the following two k-embeddings $B \to A \otimes_k \mathrm{End}_k(B)$: one is $b \mapsto b \otimes 1$ by means of the given embedding of B in A, while the other is $b \mapsto 1 \otimes b$ where $B \to \mathrm{End}_k(B)$ comes from the left action of B on itself. We denote the images of these embeddings by B_1 and B_2 respectively; then by Noether-Skolem the canonical isomorphism $B_1 \simeq B_2$ extends to an inner automorphism of D. From this it follows that $C_D(B_1) \simeq C_D(B_2)$. Now by proposition 4.1.2.1, $C(B_1) \simeq C \otimes_k \mathrm{End}_k(B)$, while $C(B_2) \simeq A \otimes_k B^{\mathrm{op}}$ by proposition 4.1.2.1 and lemma 4.1.3.4, so we conclude that

$$C \otimes_k \mathrm{End}_k(B) \simeq A \otimes_k B^{\mathrm{op}} \tag{4.1.3.2}$$

and in particular

$$[C \otimes_k \mathrm{End}_k(B) : k] = [A \otimes_k B^{\mathrm{op}} : k].$$

This says

$$[C : k][B : k]^2 = [A : k][B : k]$$

which yields 4.1.3.1.

Since A is central simple and B^{op} is simple $A \otimes_k B^{\mathrm{op}}$ is simple by proposition 4.1.2.7, so by 4.1.3.2 $C \otimes_k \mathrm{End}_k(B)$ is simple. A 2-sided ideal $\mathfrak{a} \subset C$ produces a

two-sided ideal $\mathfrak{a} \otimes_k \mathrm{End}_k(B)$ in $C \otimes_k \mathrm{End}_k(B)$, which is either 0 or the whole of $C \otimes_k \mathrm{End}_k(B)$. Comparing dimensions shows that $\mathfrak{a} = 0$ or $\mathfrak{a} = C$, and we conclude that C is simple.

We can now apply the above results with C in place of B, and if we set $C' = C_A(C)$ then $[A : k] = [C : k][C' : k]$. It follows that $[C' : k] = [B : k]$, and since evidently $B \subseteq C'$, $B = C' = C_A(C)$. ■

4.1.3.6 Corollary *With the notation and assumptions of the proposition, if B is central simple over k then so is C, and the natural homorphism $B \otimes_k C \to A$ is an isomorphism.*

Proof. Observe that B and C have the same center, which is $B \cap C$, so C is central if B is. Then $B \otimes_k C$ is a simple algebra, and $B \otimes_k C \to A$ must be injective. Since both sides have the same dimension, this map is an isomorphism. ■

We can now characterize maximal commutative subalgebras of a central simple algebra:

4.1.3.7 Corollary *Suppose A is a central simple k-algebra of finite degree and $L \subseteq A$ is a subfield containing k. The following are equivalent:*

(i). $L = C_A(L)$,

(ii). $[A : k] = [L : k]^2$;

(iii). L is a maximal commutative k-subalgebra of A.

Proof. That (i) implies (ii) follows from theorem 4.1.3.5.

(ii) implies (iii): let $L' \supseteq L$ be a commutative subalgebra containing L; then $L' \subseteq C_A(L)$ and consequently

$$[L : k]^2 = [A : k] = [L : k][C_A(L) : k] \geq [L : k][L' : k] \geq [L : k]^2.$$

Therefore $[L : k] = [L' : k]$ and $L' = L$.

(iii) implies (i): if $x \in C_A(L)$ is not in L then $L[x]$ is a commutative k properly containing L, a contradiction. ■

4.1.3.8 Corollary *If A is a central simple k-algebra of finite degree, any subfield of A that is a maximal commutative k-algebra splits A. In particular a subfield of A of degree $\sqrt{[A : k]}$ splits A.*

Proof. Suppose L is a subfield of A that is a maximal commutative k-subalgebra. We can make A into an L-vector space via the natural action of L on the right of A, and for this vector space structure corollary 4.1.3.7 shows that $[A : L] = [L : k]$. On the other hand the action of A on itself by the left yields a k-algebra homomorphism $A \to \mathrm{End}_L(A)$, whence an L-algebra homomorphism $A \otimes_k L \to \mathrm{End}_L(A)$ by adjunction. Since the latter homomorphism is nontrivial and $A \otimes_k L$ is simple, $A \otimes_k L \to \mathrm{End}_L(A)$ is injective, and therefore an isomorphism since

both sides have the same L-dimension, namely $[A : k] = [A : L]^2$. The last assertion follows from corollary 4.1.3.7. ■

Example. Suppose L/k is a finite extension of fields of degree n and let $i : L \to \mathrm{End}_k(L)$ be the injective homomorphism given by left multiplication. Since $[\mathrm{End}_k(L) : k] = n^2 = [L : k]^2$, i embeds L as a maximal commutative subalgebra of $\mathrm{End}_k(L)$.

We next show that any central simple k-algbra of finite degree over k splits over a finite separable extension.

4.1.3.9 Lemma *Suppose k is a field of characterstic $p > 0$ and D is a central k-division algebra. If every element of D is purely inseparable over K then $D = K$.*

Proof. Suppose $a \in D \setminus K$ and choose a power q of p such that $a^q \in k$. If $\sigma = \mathrm{ad}(a)$ then $\sigma \neq 1$ and $\sigma^q = 1$. Since K has characteristic p, $(\sigma - 1)^q = 0$ and there is a positive integer $f < q$ such that $(\sigma - 1)^f \neq 0$. Choose f as large as possible and $b \in D$ such that $(\sigma - 1)^f(b) \neq 0$. We can now forget about q and set

$$x = (\sigma - 1)^{f-1}(b), \quad y = (\sigma - 1)(x) = (\sigma - 1)^f(b)$$

then $y \neq 0$ and we put $z = xy^{-1}$. Since $(\sigma - 1)^{f+1}(b) = 0$, $\sigma(y) = y$ and then

$$\sigma(z) = \sigma(x)\sigma(y)^{-1} = (x + y)y^{-1} = z + 1.$$

Once again there is a power q of p such that $z^q \in K$, and then

$$z^q = \sigma(z^q) = \sigma(z)^q = z^q + 1$$

which is absurd. ■

4.1.3.10 Proposition *Let D be a central division algebra over k of finite degree. There is a maximal commutative subalgebra of D that is a finite separable field extension of k.*

Proof. If k has characteristic zero, any finite extension of k is separable and the assertion follows from corollary 4.1.3.3. Suppose k has characteristic $p > 0$ and let F/k be a maximal separable extension of k in D. By the double centralizer theorem 4.1.3.5 the centralizer $B = C_D(F)$ is simple, $F = C_D(B)$ and $[D : k] = [B : k][F : k]$. Then $F \subseteq B$ and B is a central divison algebra over F. Since F is a maximal separable subfield of D every element of B is purely inseparable over F. Then $B = F$ by lemma 4.3.1.2 and F is a maximal commutative subalgebra of D, i.e D splits over F. ■

From this and the Artin-Wedderburn theorem we find:

4.1.3.11 Corollary *Any central simple k-algebra splits over a finite separable extension of k.*

4.2 The Brauer Group

We continue to assume k is a field, and from now on all central simple k-algebras are assumed to have finite degree.

4.2.1 Brauer equivalence. If A and B are central simple k-algebras, we say that A and B are *Brauer-equivalent* or *similar* if $A \otimes_k \mathrm{End}_k(V) \simeq B \otimes_k \mathrm{End}_k(W)$ for some finite-dimensional k-vector spaces V, W. We will write $A \sim B$ to mean that A and B are similar. This is a categorical equivalence relation: it is obviously reflexive and symmetric, while if $A \otimes_k \mathrm{End}_k(V) \simeq B \otimes_k \mathrm{End}_k(W)$ and $B \otimes_k \mathrm{End}_k(X) \simeq C \otimes_k \mathrm{End}_k(Y)$,

$$A \otimes_k \mathrm{End}_k(V) \otimes_k \mathrm{End}_k(X) \simeq C \otimes_k \mathrm{End}_k(W) \otimes_k \mathrm{End}_k(Y).$$

Since this implies that

$$A \otimes_k \mathrm{End}(V \otimes_k X) \simeq C \otimes_k \mathrm{End}_k(W \otimes_k Y)$$

we see that $A \sim B$ and $B \sim C$ imply $A \sim C$.

It is easily checked that there is a *set* of equivalence classes of central simple k-algebras: for any n the number of maps $k^n \times k^n \to k^n$ is bounded by $|k|$ if k is infinite, and is finite otherwise, so the number of isomorphism classes of k-algebras of degree n is bounded, and the same is true for the union of these sets for all $n \geq 1$. We denote by $[A]$ the class of A, and by $\mathrm{Br}(k)$ the set of equivalence classes of central simple k-algebras.

A choice of basis of a k-vector space V of dimension n identifies $\mathrm{End}_k(V) \simeq M_n(k)$, and then $A \otimes_k \mathrm{End}(V) \simeq M_n(A)$ for any k-algebra A. In fact the older definition of Brauer equivalence is that $A \sim B$ if and only if $M_m(A) \simeq M_n(B)$ for some integers m, n.

4.2.1.1 Proposition *(i) Two central division algebras over k are isomorphic if and only if they are similar. (ii) Two central simple k-algebras A, B are isomorphic if and only if $A \sim B$ and $[A : k] = [B : k]$.*

Proof. (i) Suppose D and E are central division algebras and $M_n(D) \simeq M_m(E)$ for some m, n. Then any simple left $M_n(D)$-module is isomorphic to any simple left $M_m(E)$-module, and thus the endomorphism rings of these modules are isomorphic, i.e. $D \simeq E$.

(ii) Suppose $A \sim B$ and write $A \simeq M_n(D)$ and $B \simeq M_m(E)$ with central divison algebras D, E. Then $D \sim A \sim B \sim E$ and consequently $D \simeq E$ by (i). In particular $[D : k] = [E : k]$, and since $[A : k] = n^2[D : k]$, $[B : k] = m^2[E : k]$ it follows that $m = n$. The converse is clear. ■

From this point of view, theorem 4.1.1.1 and corollary 4.1.1.2 show that any central simple algebra is equivalent to a central division algebra which is unique up to isomorphism. Thus there is a bijection of $\mathrm{Br}(k)$ with the set of isomorphism classes of central division algebras over k.

The real power of this construction comes from the fact that $\mathrm{Br}(k)$ has a natural group law. Suppose $A \sim A'$ and $B \sim B'$, say

$$A \otimes_k \mathrm{End}(V) \simeq A' \otimes_k \mathrm{End}_k(V'), \quad B \otimes_k \mathrm{End}(W) \simeq B' \otimes_k \mathrm{End}_k(W').$$

Then

$$(A \otimes_k B) \otimes_k \mathrm{End}_k(V \otimes_k W) \simeq (A' \otimes_k B') \otimes_k \mathrm{End}_k(V' \otimes_k W')$$

and consequently $A \otimes_k B \sim A' \otimes_k B'$. Therefore $([A],[B]) \mapsto [A \otimes_k B]$ is a well-defined binary operation on $\mathrm{Br}(k)$. It is associative by the associativity of tensor products, and $[k]$ is an identity element. Finally, corollary 4.1.2.9 shows that $[A][A^{\mathrm{op}}] = [k]$, and we conclude that $\mathrm{Br}(k)$ is a group under this operation. It is called the *Brauer group* of k.

Suppose K/k is a field extension. We have seen that if A is a central simple k-algebra, $A \otimes_k K$ is a central simple K-algebra. Furthermore if $A \sim B$ then $A \otimes_k \mathrm{End}_k(V) \simeq B \otimes_k (W)$ and tensoring with K yields

$$(A \otimes_k K) \otimes_K \mathrm{End}_K(V \otimes K) \simeq (B \otimes_k K) \otimes_K \mathrm{End}_K(B \otimes K)$$

so that $A \otimes_k K \sim B \otimes_k K$. Finally, since

$$(A \otimes_k K) \otimes_K (B \otimes_k K) \simeq (A \otimes_k B) \otimes_k K$$

we see that $A \mapsto A \otimes_k K$ defines a homomorphism $\mathrm{Br}(k) \to \mathrm{Br}(K)$. We define the *relative Brauer group* $\mathrm{Br}(K/k)$ to be the kernel of $\mathrm{Br}(k) \to \mathrm{Br}(K)$, so

$$0 \to \mathrm{Br}(k) \to \mathrm{Br}(K) \to \mathrm{Br}(K/k) \tag{4.2.1.1}$$

is exact by definition. Thus $\mathrm{Br}(K/k)$ is the group of equivalence classes of central simple algebras over k that are split by K.

For the constructions of the next section we will need that fact that if K/k splits a central simple k-algebra A then A is similar to one in which K embeds as a maximal commutative subalgebra. Since a matrix algebra is isomorphic to its opposite algebra, a central simple k-algebra of finite dimension splits if and only if its opposite algebra does so. Thus the next proposition applies to any central simple algebra split by the finite extension K.

4.2.1.2 Proposition *Suppose A is a central simple k-algebra, K/k is a finite extension, V is a K-vector space and $K \otimes_k A^{\mathrm{op}} \simeq \mathrm{End}_K(V)$ is an isomorphism. Identify A^{op} and K with their images in $\mathrm{End}_k(V)$ under the map $\mathrm{End}_K(V) \to \mathrm{End}_k(V)$, and let B be the centralizer of A^{op} in $\mathrm{End}_k(V)$. Then B is a central simple k-algebra similar to A, and K is a maximal commutative subalgebra of B.*

Proof. By corollary 4.1.3.6 B is central simple over k and the natural homomorphism $B \otimes_k A^{\mathrm{op}} \to \mathrm{End}_k(V)$ is an isomorphism. This shows that $B \sim A$, and since K centralizes A in $\mathrm{End}_K(V) \subseteq \mathrm{End}_k(V)$, $K \subseteq B$.

The isomorphism $A^{\mathrm{op}} \otimes_k K \simeq \mathrm{End}_K(V)$ shows that

$$[A : k] = [A \otimes_k K : K] = \dim_K(V)^2$$

while $B \otimes_k A \to \mathrm{End}_k(V)$ similarly shows that

$$[A : k][B : k] = \dim_k(V)^2 = \dim_K(V)^2[K : k]^2.$$

Comparing these equalities shows that $[B : k] = [K : k]^2$, and since $K \subseteq B$, K is maximal commutative in B. ■

4.2.2 Extensions and algebras. In the situations we will be concerned with K/k is a finite Galois extension with Galois group G, in which case the relative Brauer group can be computed by means of an isomorphism $\mathrm{Br}(K/k) \simeq H^2(G, K^\times)$. However we recall from section 3.1.4 that the group of isomorphism classes of extensions of G by $K^\times$ is also isomorphic to $H^2(G, K^\times)$. In this section we give a direct construction of an isomorphism $\mathrm{Br}(K/k) \to \mathrm{Ext}(\mathrm{Gal}(K/k), K^\times)$. The natural way to construct an isomorphism $\mathrm{Br}(K/k) \simeq \mathrm{Ext}(\mathrm{Gal}(K/k), K^\times)$ would be to construct some kind of equivalence of categories and show that it is compatible with products. For this purpose we will rework the definition of $\mathrm{Br}(K/k)$ so as to make it the group of isomorphism classes of a catgory with a grouplike monoidal structure.

Fix a finite extension K/k and consider the following category $\mathrm{CS}(K/k)$: objects are pairs (A, i) where A is a central simple k-algebra and $i : K \to A$ is a k-algebra homomorphism embedding K as a maximal commutative k-subalgebra of A. In particular $[A : k] = [K : k]^2 < \infty$. A morphism $f : (A, i) \to (B, j)$ is a commutative diagram

$$\begin{tikzcd} K \arrow[r, "i"] \arrow[dr, "j"'] & A \arrow[d] \\ & B \end{tikzcd} . \tag{4.2.2.1}$$

Since A and B have the same dimension the k-algebra homomorphism $A \to B$ is an isomorphism. In other words $\mathrm{CS}(K/k)$, like $\mathrm{EXT}(G, K^\times)$ is a groupoid. The exact relation of $\mathrm{CS}(K/k)$ with $\mathrm{Br}(K/k)$ will be explained later.

The functor

$$E : \mathrm{CS}(K/k) \to \mathrm{EXT}(G, K^\times) \tag{4.2.2.2}$$

is defined as follows. For any object (A, i) in $\mathrm{CS}(K/k)$ let $E(A, i)$ be the set of pairs $(a, s) \in A^\times \times G$ such that

$$i \circ s = \mathrm{ad}(a) \circ i \tag{4.2.2.3}$$

or, more explicitly

$$i({}^s x) = axa^{-1} \tag{4.2.2.4}$$

for all $x \in K$ and $a \in A^\times$. If (a,s) and (b,t) are elements of $E(A,i)$ the computation

$$\begin{aligned} i \circ st &= i \circ s \circ t = \mathrm{ad}(a) \circ i \circ t \\ &= \mathrm{ad}(a) \circ \mathrm{ad}(b) \circ i = \mathrm{ad}(ab) \circ i \end{aligned}$$

shows that

$$(a,s)(b,t) = (ab, st)$$

is a group law on $E(A,i)$. The Noether-Skolem theorem shows that for any $s \in G$ there is a $a \in A^\times$ such that 4.2.2.3 holds, so $(a,s) \mapsto s$ defines a surjective homomorphism $p : E(A) \to G$. The kernel of p is the subgroup of $a \in A^\times$ centralizing the image of i, which is $i(K^\times)$ since K is a maximal commutative subalgebra of A. Since $(a,s) = (a,t)$ implies $s = p(a) = t$, the map $(a,s) \mapsto a$ is an injective homomorphism $E(A) \to A^\times$. We will identify the map $K^\times \to A^\times$ induced by i with the map $K^\times \to E(A)$ sending x to $(i(x), 1)$. Then

$$1 \to K^\times \xrightarrow{i} E(A,i) \xrightarrow{p} G \to 1$$

is an object of $\mathrm{EXT}(G, K^\times)$ which we also denote by $E(A,i)$ as before. There is no real ambiguity in using i for the k-algebra homomorphism $K \to A$ and the group homomorphism $K^\times \to E(A,i)$. In fact from 4.2.2.3 we see that

$$u : E(A,i) \to A^\times \qquad (u,s) \mapsto u \tag{4.2.2.5}$$

is an injective homomorphism, and the map $i : K^\times \to E(A,i)$ is the restriction to $K^\times$ of the above u. We will call 4.2.2.5 the canonical embedding of $E(A,i)$ in $A^\times$.

Finally if $f : (A,i) \to (B,j)$ is a morphism in $\mathrm{CS}(K/k)$ we define $E(f)$ to be the evident morphism of extensions

$$\begin{tikzcd} 1 \arrow[r] & K^\times \arrow[r, "i"] \arrow[d, equal] & E(A,i) \arrow[r] \arrow[d, "f"'] & G \arrow[r] \arrow[d, equal] & 1 \\ 1 \arrow[r] & K^\times \arrow[r, "j"'] & E(B,j) \arrow[r] & G \arrow[r] & 1 \end{tikzcd}$$

induced by $f : A \to B$. This completes the construction of 4.2.2.2.

4.2.3 Crossed products. A construction called the *crossed product algebra* will yield an inverse functor to 4.2.2.2. We consider the following data: G is a group, R is a commutative ring with a G-module structure and E is an object

$$1 \to R^\times \xrightarrow{i} E \xrightarrow{p} G \to 1 \tag{4.2.3.1}$$

of $\mathrm{EXT}(G, R^\times)$. Given this,

$$R^\times \times (R \times E) \to R \times E \qquad (a,(x,u)) \mapsto (xa^{-1}, i(a)u)$$

defines an action of $R^\times$ on $R \times E$, and we denote by $[R, E]$ the quotient of $R \times E$ by this action. If $(x, u) \in R \times E$ we denote by $[x, a]$ its image in $[R, E]$. Since $ai(x) = i({}^{p(a)}x)a$ in E, the set $[R, E]$ has a monoid structure for which

$$[x, a][y, b] = [x \cdot {}^{p(a)}y, ab]. \tag{4.2.3.2}$$

For $s \in G$ let $[R, E]_s$ be the set of $[x, a] \in [R, E]$ such that $p(a) = s$. The monoid structure clearly induces maps

$$[R, E]_s \times [R, E]_t \to [R, E]_{st}. \tag{4.2.3.3}$$

If $e_0 \in E$ is such that $p(e_0) = s$, any element of $[R, E]_s$ has a unique expression as $[x, e_0]$. In particular if $s = 1$, $x \mapsto [x, 1]$ is a canonical isomorphism $R \xrightarrow{\sim} [R, E]_1$ of monoids for the operation of multiplication on R. If we use this identification to make $[R, E]_1$ into a commutative ring, the addition operation is

$$[x, 1] + [y, 1] = [x + y, 1].$$

More generally if $s \in G$ and $p(e) = s$, any element of $[R, E]_s$ has a unique expression as $[x, e]$ and we can then identify $[R, E]_s$ with a free R-module of rank one, the operations being

$$[x, e] + [y, e] = [x + y, e] \qquad a[x, e] = [a, 1][x, e] = [ax, e].$$

It is easily checked that the R-module structure on $[R, E]_s$ is independent of the choice of e.

Finally, the free R-module

$$R \Vdash E = \bigoplus_{s \in G} [R, E]_s \tag{4.2.3.4}$$

has a natural ring structure arising from 4.2.3.3; the additive and multiplicative identities are $[0, 1]$ and $[1, 1]$ respectively, and any element of the form $[x, e]$ with $x \in R^\times$ is a unit. We call $R \Vdash E$ the *crossed product algebra* associated to the extension E (note that we are using the symbol E to denote both a group and an extension; the construction $R \Vdash E$ depends on the extension and not just on the group).

Note how $R \Vdash E$ differs from the set $[R, E]$: in $R \Vdash E$ any element of the form $[0, e]$ is the additive identity of $R \Vdash E$, but two elements $[0, e]$, $[0, t] \in [R, E]$ with $p(e) \neq p(f)$ are distinct in $[R, E]$. In geometric terms, if the individual summands in 5.2.2.5 are thought of as "coordinate axes" then $[R, E]$ is the disjoint sum of the coordinate axes.

The equality 4.2.3.2 shows that

$$\iota_E : R \to R \Vdash E \qquad \iota_E(a) = [a, 1]_1 \tag{4.2.3.5}$$

is a homomorphism of R onto a subring of $R \Vdash E$, the *canonical embedding* of R. If $k = R^G \subseteq R$ is the subring of G-invariants of R, we see from 4.2.3.2 that

i maps k into the center of $R \Vdash E$, so that $R \Vdash E$ is an k-algebra. Likewise the group homomorphism

$$\upsilon_E : E \to (R \Vdash E)^\times \qquad \upsilon_E(a) = [1, a]_{p(a)} \tag{4.2.3.6}$$

will be called the *canonical embedding* of E. By construction the diagram

$$\begin{tikzcd} K^\times \arrow[r, "\iota_E|K^\times"] \arrow[d, "i"'] & K \Vdash E \\ E \arrow[ur, "\upsilon_E"'] & \end{tikzcd} \tag{4.2.3.7}$$

is commutative.

To do computations in a crossed product algebra it helps to observe that by construction any $a \in R \Vdash E$ has a unique expression

$$a = \sum_s a_s \quad \text{with} \quad a_s \in [R, E]_s. \tag{4.2.3.8}$$

If we identify $x \in R$ with its image in $R \Vdash E$ by the canonical embedding the formula 4.2.3.2 shows that

$$a_s x = {}^s x a_s \tag{4.2.3.9}$$

for all $x \in R$.

An isomorphism $(E, i, p) \xrightarrow{\sim} (E', i', p')$ in $\mathrm{EXT}(G, R^\times)$ induces an isomorphism $R \Vdash E \xrightarrow{\sim} R \Vdash E'$ of crossed product algebras. Thus $E \mapsto R \Vdash E$ defines a functor

$$\mathrm{EXT}(G, R^\times) \to \mathrm{Alg}_k. \tag{4.2.3.10}$$

The crossed product has the following universal property:

4.2.3.1 Proposition *Suppose (E, i, p) is an extension of G by $R^\times$, $k = R^G$, B is a k-algebra, $j : R \to B$ is a k-algebra homomrphism and $u : E \to B^\times$ is a group homomorphism such that*

$$j(x) = u(i(x)) \quad \textit{and} \qquad u(a)j(x)u(a)^{-1} = j({}^{p(a)}x) \tag{4.2.3.11}$$

for all $x \in R^\times$ and $a \in E$. There is a unique homorphism $f : R \Vdash E \to B$ such that

$$\begin{tikzcd} R^\times \arrow[r, "\iota_E|K^\times"] \arrow[d, "i"'] \arrow[rr, bend left, "j|K^\times"] & R \Vdash E \arrow[r, "f"] & B \\ E \arrow[ur, "\upsilon_E"'] \arrow[urr, bend right, "u"'] & & \end{tikzcd} \tag{4.2.3.12}$$

is commutative.

Proof. Uniqueness holds because $R \Vdash E$ is generated as a k-algebra by elements of the form $\iota(x)$ and $\upsilon(a)$. For existence, observe that the conditions of 4.2.3.1 imply that there is an R-linear map $[R,E]_s \to B$ such that

$$f_s([x,a]_s) = j(x)u(a)$$

and the diagram

$$\begin{tikzcd}
{[R,E]_s \times [R,E]_t} \arrow[r] \arrow[d, "f_s \times f_t"'] & {[R,E]_{st}} \arrow[d, "f_{st}"] \\
B \times B \arrow[r] & B
\end{tikzcd}$$

is commutative. The map

$$f = \bigoplus_s f_s : \bigoplus_s [R,E]_s \to B$$

is then a k-algebra homomorphism $R \Vdash E \to B$ satisfying the given conditions. ■

Suppose that (E,i,p) is an object of $\mathrm{EXT}(G,R^\times)$ and $f : G' \to G$ is a homomorphism. As before denote by $f^*E = (E',i',p')$ the pullback extension

$$\begin{tikzcd}
1 \arrow[r] & R^\times \arrow[r, "i'"] \arrow[d, equal] & E' \arrow[r, "p"] \arrow[d, "g"] & G \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & R^\times \arrow[r, "i"'] & E \arrow[r, "p"'] & G \arrow[r] & 1
\end{tikzcd}$$

and recall that the G'-module structure of A is the one induced by f. If $u : E \to (R \Vdash E)^\times$ is the canonical embedding then $u \circ g$ is a homomorphism $E' \to (R \Vdash E)^\times$ satisfying the conditions of proposition 4.2.3.1, so there is a unique R-algebra homomorphism

$$f^* : R \Vdash E' \to R \Vdash E \tag{4.2.3.13}$$

such that $u \circ (g|E') = f^* \circ u'$ where $u' : E' \to R \Vdash E'$ is the canonical embedding of the pullback.

Suppose on the other hand that R' is a ring with a G-action and $f : R \to R'$ is a ring homomorphism compatible with the G-actions. If (E,i,p) is an object of $\mathrm{EXT}(G,R^\times)$ pushout extension by f is

$$\begin{tikzcd}
1 \arrow[r] & R^\times \arrow[r, "i"] \arrow[d, "f"] & E \arrow[r, "p"] \arrow[d, "g"] & G \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & (R')^\times \arrow[r] & E' \arrow[r, "p'"'] & G \arrow[r] & 1
\end{tikzcd}$$

and we may form $R' \Vdash E'$. There is a canonical R'-algebra isomorphism

$$f_* : R' \otimes_R (R \Vdash E) \xrightarrow{\sim} R' \Vdash E' \tag{4.2.3.14}$$

identifying the canonical embeddings $u : E \to (R \Vdash E)^\times$ and $u' : E \to (R' \Vdash E)^\times$. As before this follows from the universal property of crossed products.

4.2.4 Application to the Brauer group. We now return to our original situation.

4.2.4.1 Theorem *Suppose K/k is a finite Galois extension and E is an extension of $G = \mathrm{Gal}(K/k)$ by $K^\times$. The k-algebra $K \Vdash E$ is central simple, and $\iota : K \to K \Vdash E$ embeds K as a maximal commutative subalgebra.*

Proof. $K \Vdash E$ is central: suppose $x = \sum_s a_s$ is in the center, where as before $a_s \in [K, E]_s$, and let $\ell \in K$ be a primitive element. Then

$$\sum_s \ell a_s = \ell x = x\ell = \sum_s {}^s\ell a_s$$

and since ${}^s\ell \neq \ell$ for $s \neq 1$ we must have $a_s = 0$ for $s \neq 1$. Therefore $x = a_1 u_1 \in K$. Then $xu_s = u_s x = {}^s x u_s$ for all $s \in G$ implies $x \in K^G = k$.

$K \Vdash E$ is simple: pick a basis $\{u_s\}_{s \in G}$ of $K \Vdash E$ with $u_s \in [K, E]_s$ and let $I \subseteq K \Vdash E$ be a nonzero ideal. It suffices to show that in the K-vector space $K \Vdash E$ with basis $\{u_s\}_{s \in G}$, a primordial element of I is one of the u_s, for if $u_s \in I$ then so is $u_{s^{-1}} u_s$, which is a nonzero multiple of the identity. Suppose that $x = \sum_s x_s u_s$ is primordial and s_s, $s_t \neq 0$. If $b \in K$ is a primitive element then $x' = s(b)x - xb$ is a nonzero element of I since $s(b) \neq t(b)$. Then $|J(x')| < |J(x)|$ contradicts the minimality of $J(x)$. Therefore $x = u_s$ for some $s \in G$.

Since $|G| = [K : k]$, $[K \Vdash E : k] = [K : k]^2$ and $i(K)$ is a maximal commutative subalgebra of $K \Vdash E$. ■

The theorem shows that $E \mapsto (K \Vdash E, \iota)$ defines a functor

$$CS : \mathrm{EXT}(G, K^\times) \to \mathrm{CS}(K/k). \tag{4.2.4.1}$$

4.2.4.2 Theorem *The functors*

$$CS : \mathrm{EXT}(G, K^\times) \to \mathrm{CS}(K/k) \qquad E : \mathrm{CS}(K/k) \to \mathrm{EXT}(G, K^\times)$$

are inverse equivalences of categories.

Proof. (1) We show $CS \circ E$ is isomorphic to the identity functor of $\mathrm{CS}(K/k)$, or in other words there is a functorial isomorphism $(K \Vdash E(A, i), \iota) \simeq (A, i)$ for every (A, i) in $\mathrm{CS}(K/k)$. If $u : E(A, i) \to A^\times$ is the canonical embedding, $i = j$ and u satisfy the conditions of proposition 4.2.3.1, so there is a k-algebra homomorphism $f : K \Vdash E(A) \to A$ which is necessarily injective since $K \Vdash E(A)$ is simple. Since the dimensions of the source and target are the

same, f is an isomorphism. It is immediate that f extends to an isomorphism $(K \Vdash E(A,i),\iota) \simeq (A,i)$ which is functorial in A.

(2) We show $E \circ CS$ is isomorphic to the identity functor of $\mathrm{EXT}(G,K^\times)$. Let (E,i,p) be an object of $\mathrm{EXT}(G,K^\times)$. For $s \in G$ the set $[K,E]_s^\times = [K,E]_s \setminus \{[0,1]\}$ is exactly the set of $a \in K \Vdash E$ satisfying 4.2.2.3 for $i = \iota$. If we denote by $[K,E]^\times$ the disjoint union of the $[K,E]_s^\times$ endowed with the multiplication induced by that of $K \Vdash E$, $EXT(\mathrm{CS}(E))$ is group $[K,E]^\times$ endowed with the injection $i : K^\times \to [K,E]^\times$ induced by $\iota : K \to K \Vdash E$ and the projection $[K,E]^\times \to G$ given by $[x,e] \mapsto p(e)$. On the other hand the group homomorphism $E \to [K,E]^\times$ given by $e \mapsto [1,e]$ is clearly an isomorphism, and extends to a isomorphism of extensions $E \to EXT(\mathrm{CS}(E))$. It is clear from the construction that this is functorial in E. ■

4.2.4.3 Corollary *For any finite Galois extension L/K with Galois group G there are canonical isomorphisms*

$$\mathrm{Br}(L/K) \xrightarrow{\sim} \mathrm{EXT}(G,L^\times) \xrightarrow{\sim} H^2(G,L^\times) \tag{4.2.4.2}$$

of groups, where the first is induced by the functor E and the second is 3.1.4.8 for $A = L^\times$.

Since $\mathrm{EXT}(G,K^\times)$ has a "product structure" (more formally, a monoidal structure) arising from the Baer sum of extensions we expect that $\mathrm{CS}(K/k)$ should have a similar structure that is in some way compatible with the product in $\mathrm{Br}(K/k)$. The difficulty is that if (A,i) and (B,j) are in $\mathrm{CS}(K/k)$, the tensor product $A \otimes_k B$ does not have an embedding of K as a maximal commutative subalgebra, since the dimensions are wrong except in the trivial case where A or B is k. We must therefore use the procedure of proposition 4.2.1.2.

Suppose (A,i) and (B,j) are objects of $\mathrm{CS}(K/k)$ and denote by V_A and V_B be the K-vector spaces A and B with the K-vector space structure coming from left multiplication by elements of K via i and j respectively. By comparing dimensions we see that there is an isomorphism

$$K \otimes_k A^{\mathrm{op}} \otimes_k B^{\mathrm{op}} \xrightarrow{\sim} \mathrm{End}_K(V_A \otimes_K V_B) \tag{4.2.4.3}$$

sending $c \otimes a \otimes b$ to the K-linear endomorophism

$$x \otimes y \mapsto i(c)xa \otimes yb = xa \otimes j(c)yb.$$

Denote by $A *_k B$ the centralizer of the image of $A^{\mathrm{op}} \otimes_k B^{\mathrm{op}}$ in $\mathrm{End}_k(V_A \otimes_k V_B)$ and by $i * j$ the embedding $K \to A *_k B$ induced by 4.2.4.3 and the inclusion of $\mathrm{End}_K(V_A \otimes_K V_B)$ into $\mathrm{End}_k(V_A \otimes_K V_B)$. By proposition 4.2.1.2, $A *_k B$ is a central simple k-algebra similar to $A \otimes_k B$ and $i * j$ embeds $K \to A *_k B$ as a maximal commutative subalgebra; thus $(A *_k B, i * j)$ is an object of $\mathrm{CS}(K/k)$.

If

$$(A,i) \simeq (A',i'), \quad (B,j) \simeq (B',j')$$

are isomorphisms in $\mathrm{CS}(K/k)$ it is clear from the construction that there is

$$(A *_k B, i * j) \simeq (A' *_k B', i' * j')$$

as well.

4.2.4.4 Proposition *For any two objects E, F of* $\mathrm{EXT}(G, K^\times)$,

$$CS(E) *_k CS(F) \xrightarrow{\sim} CS(E * F). \tag{4.2.4.4}$$

in $\mathrm{CS}(K/k)$.

Proof. Recall the construction of $E * F$: as a group it is the cokernel of the fibered product $E \underset{G}{\times} F$ by the image of the subgroup of elements of the form $(i(x), j(x)^{-1})$. We denote by $[e, f]$ the image of $(e, f) \in E \underset{G}{\times} F$ in $E * F$. The projection $E * F \to G$ is $(e, f) \mapsto p(e) = q(f)$ and the kernel $w : K^\times \to E * F$ is

$$w(x) = [i(x), 1] = [1, j(x)].$$

Set $A = K \Vdash E$, $B = K \Vdash F$ and let $u : E \to A^\times$, $v : F \to B^\times$ be the canonical injections, and denote by $i : K \to A$, $j :\to B$ the canonical injections. Finally let V_A, V_B be as in the discussion preceding the proposition.

For any $(e, f) \in E \underset{G}{\times} F$,

$$x \otimes y \mapsto u(e)x \otimes v(f)y$$

defines a k-linear endomorphism of $V_A \otimes_K V_B$ (that this definition is consistent with the identities $i(a)x \otimes y = x \otimes j(a)y$ follows from $p(e) = q(f)$). Since it is defined by left multiplication, this endomorphism centralizes $A^{\mathrm{op}} \otimes_k B^{\mathrm{op}}$ and thus belongs to $A *_k B$, whence a homomorphism $E \underset{G}{\times} F \to (A *_k B)^\times$. It is clear that elements of the form $(i(a), j(a^{-1})$ act trivially on $V_A \otimes_k V_B$, so this homomorphism passes to the quotient, yielding $w : E * F \to (A *_k B)^\times$. Now the embedding $\ell : K^\times \to E * F$ is $a \mapsto (i(a), 1) = (1, j(a))$, and it is clear from the construction that $(e, f)\ell(a) = \ell({}^s a)(e, f)$ if $p(e) = q(f) = s$. It follows from the universal property of crossed product algebras that w and ℓ define a (necessarily injective) k-algebra homomorphism $K \Vdash (E * F) \to A *_k B$, and since source and target have the same degree $|G|$ over k, it is an isomorphism $K \Vdash (E * F) \xrightarrow{\sim} A *_k B$ as required. ∎

We can now explain the precise relation between $\mathrm{CS}(K/k)$ and the Brauer group. Denote by $\pi_0(\mathrm{CS}(K/k))$ the set of isomorphism classes of objects of $CS(K/k)$. If (A, i) is an object of $\mathrm{CS}(K/k)$ we denote by $[A, i]$ the corresponding element of $\pi_0(\mathrm{CS}(K/k))$. The above results show that the product $*_k$ induces a binary composition law on $\pi_0(\mathrm{CS}(K/k))$.

4.2.4.5 Proposition *The set $\pi_0(\mathrm{CS}(K/k))$ with the binary composition law induced by $*_k$ is a group, and there is a unique homomorphism of groups $\alpha : \pi_0(\mathrm{CS}(K/k)) \to \mathrm{Br}(k)$ such that*

$$\alpha([A,i]) = [A] \tag{4.2.4.5}$$

for all (A,i) in $\mathrm{CS}(K/k)$. The homomorphism α is injective and its image is $\mathrm{Br}(K/k)$.

Proof. Uniqueness of the homomorphism is clear, and that α is compatible with products follows from the fact that $A *_k B \sim A \otimes_k B$. It is well-defined since $(A,i) \simeq (B,j)$ implies that $A \simeq B$ and thus $A \sim B$; furthermore if A is any central simple k-algebra A split by K, $[A]$ is in the image of α since it is similar to one with an embedding of K as a maximal commutative subalgebra, and the converse is clear. Thus the image of α is $\mathrm{Br}(K/k)$.

If $\alpha(A,i) = \alpha(B,j)$ then $A \sim B$ and hence $A \simeq B$ since A and B have the same dimension (given that K is embedded as a maximal commutative subalgebra of both). By the Noether-Skolem theorem there is an inner automorphism u of B such that $j = u \circ i$, and this u is an isomorphism $(A,i) \simeq (B,j)$ in $\mathrm{CS}(K/k)$. It follows that α is injective, and since its image is a subgroup of $\mathrm{Br}(K/k)$, $\pi_0(\mathrm{CS}(K/k))$ is a group. ■

The procedure for associating a 2-cocycle to an element of $\mathrm{Ext}(G, K^\times)$ can thus be applied to $\mathrm{Br}(K/k)$. Recall that for any object (E,i,p) of $\mathrm{EXT}(G,K^\times)$ we choose $e_s \in E$ for all $s \in G$ such that $p(e_s) = s$. For all s, $t \in G$, $p(e_s e_t) = st = p(e_{st})$ and thus there is an $a_{s,t} \in K^\times$ such that

$$e_s e_t = a_{s,t} e_{st}.$$

Then $(a_{s,t})$ is a 2-cocycle and $E] \mapsto (a_{st})$ induces an isomorphism $\mathrm{Ext}(G,K^\times) \xrightarrow{\sim} H^2(G,K^\times)$.

In the crossed product algebra $K \rtimes E$ we may then set $u_s = [1, e_s]$, and then

$$u_s u_t = a_{s,t} u_{st}, \qquad u_s i(a) = i({}^s a) u_s \tag{4.2.4.6}$$

for all $a \in K$. Conversely, if A is any central simple k-algebra and $i : K \to A$ is a k-embedding of K as a maximal commutative subalgebra, there are $u_s \in A$ satisfying the second equality of 4.2.4.6, and then $a_{s,t} \in K^\times$ satisfying the first. The class of the 2-cocycle $(a_{s,t})$ in $H^2(G,K^\times)$ corresponds to the class of A in $\mathrm{Br}(K/k)$ by the previous isomorphism.

In fact the following slightly more general statement is true:

4.2.4.6 Proposition *Suppose A is a k-algebra, K/k is a finite Galois extension with group G and $i : K \to A$ is a k-algebra homomorphism. Suppose that for all $s \in G$ there are elements $u_s \in A$ satisyfing 4.2.4.6 and which generate A when it is made into a K-vector space via i. Then A is a central simple k-algebra split by K and the class $(a_{s,t})$ in $H^2(G,K^\times)$ corresponds to the class of A in $\mathrm{Br}(K/k)$.*

Proof. Let E be an extension whose class is that of the cocycle $(a_{s,t})$. The universal property of crossed products shows that there is a k-algebra homomorphism $K \Vdash E \to A$, which is necessarily injective since it is nontrivial and $K \Vdash E$ is simple. The hypotheses imply that $[A : K] \leq |G| = [K \Vdash E : k]$, so we must have $[A : K] = [K \Vdash E : k]$ and thus $A \simeq K \Vdash E$. From this it follows that the class of A in $H^2(G, K^\times)$ is that of $(a_{s,t})$. ■

4.2.4.7 Example: Hamilton quaternions Before going on let's consider a simple example. The ring $\mathbb{H}$ of *Hamilton quaternions* is a 4-dimensional $\mathbb{R}$-vector space with basis 1, i, j, k whose multiplication is determined by the relations

$$i^2 = j^2 = k^2 = -1, \qquad ij = k = -ji. \tag{4.2.4.7}$$

It is easily seen to be a division ring with center $\mathbb{R}$.

Let $i : \mathbb{C} \to \mathbb{H}$ be the $\mathbb{R}$-algebra homomorphism mapping $i \in \mathbb{C}$ to $i \in \mathbb{H}$. It is easily checked that its image is a maximal commutative subalgebra of $\mathbb{H}$, and this is also clear from corollary 4.1.3.8. As usual let $G = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$, which is cyclic of order 2 with generator c (complex conjugation). On account of the relations 4.2.4.7 the group $E = E(\mathbb{H}, i)$ is the disjoint union $\mathbb{C}^\times \cup j\mathbb{C}^\times$, and the projection $p : E \to G$ is $p(\mathbb{C}^\times) = 1$, $p(j\mathbb{C}^\times) = c$. If we choose $1 \mapsto 1$, $c \mapsto j$ as a section of p, the corresponding 2-cocycle is

$$a_{1,1} = a_{1,c} = a_{c,1} = 1, \quad a_{c,c} = -1. \tag{4.2.4.8}$$

Conversely if we use the recipe 4.2.4.6 for the crossed product algebra and write $u_1 = 1$, $u_c = j$, the crossed product algebra $E \Vdash G$ is $\mathbb{C} \oplus \mathbb{C}j$ with the multiplication determined by

$$j^2 = -1, \quad jz = \bar{z}j, \quad z \in \mathbb{C}$$

which is of course $\mathbb{H}$.

4.2.4.8 Cyclic algebras. The cocycle 4.2.4.8 is an example of the cocycle 3.2.4.11 for a cyclic group G and an element a of a G-module A such that $a \in A^G$. Recall that cocycle is

$$a_{i,j} = \begin{cases} 1 & i + j < n \\ a & i + j \geq n. \end{cases}$$

if we identify $G \simeq \mathbb{Z}/n\mathbb{Z}$ and identify $i \in \mathbb{Z}/n\mathbb{Z}$ with its representative in $[0, n)$,

Suppose now K/k is a cyclic Galois extension with group G. Fix as before an isomorphism $G \simeq \mathbb{Z}/n\mathbb{Z}$ and let $s \in G$ correspond to $1 \in \mathbb{Z}/n\mathbb{Z}$. In the notation of 4.2.4.6,

$$u_i u_j = \begin{cases} u_{i+j} & i + j < n \\ a u_{i+j} & i + j \geq n \end{cases}$$

and $u_1 b = {}^s b u_1$ for $b \in K$. Then u_0 is the identity of $K \Vdash G$ and $u_i = u_1^i$ for $0 \le i < n$, while $u_1^n = a u_1 = a$. If we write $x = u_1$, then $K \Vdash E$ is a K-vector space with basis $1, x, \ldots, x^{n-1}$ and the multiplication is determined by

$$xb = {}^s bx,\ b \in K, \quad x^n = a. \tag{4.2.4.9}$$

These algebras are (unsurprisingly) called *cyclic algebras*. Before the development of the cohomological approach they were one of the main tools in local class field theory, particular when K/k was a Kummer or Artin-Schreier extension.

4.2.5 Inflation and restriction. In section 3.2.1.2 we constructed functors on categories of groups extensions that correspond to the restriction and inflation on degree two cohomology. Here we do the same things for the categories $\mathrm{CS}(K/k)$.

Suppose first that L/k is a finite Galois extension with group G, K is an extension of k in L and $H = \mathrm{Gal}(L/K)$. Let (A, i) be an object in $\mathrm{CS}(L/k)$. By the double centralizer theorem 4.1.3.5 the centralizer $C_A(i(K))$ is a simple k-algebra and its centralizer in A is $i(K)$. In particular its own center is $i(K)$, so if we make $C_A(i(K))$ a K-algebra via the restriction i to K, $C_A(i(K))$ is a central simple K-algebra. The equality 4.1.3.1 shows that

$$[C_A(i(L)) : k] = [A : k]/[K : k]$$

and then

$$[C_A(i(L)) : K] = [A : k]/[K : k]^2 = [L : K]^2$$

since $[A : k] = [L : k]^2$. Therefore i embeds L into $C_A(i(K))$ as a maximal commutative subalgebra, and $(C_A(i(K)), i)$ is an object of $\mathrm{CS}(L/K)$. This construction is evidently functorial in (A, i), and we have defined a functor

$$\mathrm{Res}_{L/K} : \mathrm{CS}(L/k) \to \mathrm{CS}(L/K). \tag{4.2.5.1}$$

We will also use $\mathrm{Res}_{L/K}(A)$ to denote the K-algebra $C_A(i(K))$.

Denote by W_A the K-vector space A where K acts on A by right multiplication via i. The action of $\mathrm{Res}_{L/K}(A)$ is K-linear, whence an embedding $r : \mathrm{Res}_{L/K}(A)^{\mathrm{op}} \to \mathrm{End}_K(W_A)$. On the other hand the action of A on itself by left multiplication yields a k-linear map $A \to \mathrm{End}_K(W_A)$, which in turn yields a K-algebra homomorphism $\ell : K \otimes_k A \to \mathrm{End}_K(W_A)$ by adjunction. Since the image of ℓ lies in the centralizer of the image of r there is a K-algebra homomorphism

$$(K \otimes_k A) \otimes_K \mathrm{Res}_{L/K}(A)^{\mathrm{op}} \to \mathrm{End}_K(W_A)$$

and a quick computation shows that source and target have the same dimension. Therefore the map is an isomorphism, and

$$K \otimes_k A \xrightarrow{\sim} \mathrm{Res}_{L/K}(A). \tag{4.2.5.2}$$

It follows that the the restriction functor $\mathrm{CS}(L/k) \to \mathrm{CS}(L/K)$ yields, on passing to isomorphism classes the map $\mathrm{Br}(L/k) \to \mathrm{Br}(L/K)$.

4.2.5.1 Proposition *For any object E of* $\mathrm{EXT}(G, L^\times)$ *there is a functorial isomorphism*

$$CS_{L/K}(\mathrm{Res}_G^H(E)) \xrightarrow{\sim} \mathrm{Res}_{L/K}(CS_{L/k}(E)) \tag{4.2.5.3}$$

in $\mathrm{CS}(L/K)$.

Proof. The assertion is that for all E there is a functorial isomorphism

$$L \Vdash \mathrm{Res}_G^H(E) \xrightarrow{\sim} \mathrm{Res}_{L/K}(L \Vdash E)$$

compatible with the embeddings of L. Suppose $a = \sum_{s\in G} a_s$ is an element of $L \Vdash E$ with $a_s \in [L, E]_s$. For $x \in K$ the equality $xa = ax$ says that

$$x \sum_s a_s = \sum_s a_s x = \sum_s {}^s x a_s$$

and if this is to hold for all $x \in K$, $a_s \neq 0$ if and only if $s \in H$. Then $a = \sum_{s\in H} a_s$ can be identified with an element of $L \Vdash \mathrm{Res}_G^H E$, and this identification is evidently functorial and compatible with the identifications of L as a maximal commutative subalgebra. ■

Suppose now that as before L/k is a finite Galois extension with group $G_{L/k}$, but now K is a Galois extension of k contained in L with Galois group $G_{K/k}$, and denote by $\pi : G_{L/k} \to G_{K/k}$ the canonical projection. We will construct a functor $\mathrm{CS}(K/k) \to \mathrm{CS}(L/k)$ correspsonding to the inflation functor for π.

let (A, i) be an object of $\mathrm{CS}(K/k)$. As in the construction of the product $*_k$ we denote by V_A the K-vector space A, where L acts on V_A by left multiplication. As in section 4.2.4 the homomorphism $r : A^{\mathrm{op}} \to \mathrm{End}_K(V_A)$ defined by right multiplication induces an isomorphism

$$K \otimes_k A^{\mathrm{op}} \xrightarrow{\sim} \mathrm{End}_K(V_A)$$

and tensoring with L over K yields

$$L \otimes_k A^{\mathrm{op}} \xrightarrow{\sim} \mathrm{End}_L(L \otimes_K V_A) \subseteq \mathrm{End}_k(L \otimes_K V_A)$$

The centralizer of $r(A^{\mathrm{op}})$ in $\mathrm{End}_k(L \otimes_K V_A)$ of the image of is a central simple k-algebra similar to A which we will denote by $I(A, i)$, and the above isomorphism yields an embedding $i : L \to I(A, i)$ as a maximal commutative subalgebra. We denote by $\mathrm{Inf}_H^G(A,)$ the resulting object $(I(A, i), i)$ of $\mathrm{CS}(L/k)$. This is clearly functorial in (A, i), so we have constructed a functor

$$\mathrm{Inf}_{L/K} : \mathrm{CS}(K/k) \to \mathrm{CS}(L/k). \tag{4.2.5.4}$$

As usual we will use $\mathrm{Inf}_{L/K}(A)$ to denote the algebra $I(A, i)$.

Corresponding to proposition 4.2.5.1 we have:

4.2.5.2 Proposition *For any object E of* $\mathrm{Ext}(H, K^\times)$ *there is a functorial isomorphism*

$$CS_{L/k}(\mathrm{Inf}_{G_{K/k}}^{G_{L/k}}(E)) \xrightarrow{\sim} \mathrm{Inf}_{L/K}(CS_{K/k}(E)) \tag{4.2.5.5}$$

in $\mathrm{CS}(L/k)$.

Proof. Write $E = (E, i, p)$ and set $A = K \Vdash E$; in the preceding construction V_A is A with the K-vector space structure given by the canonical injection $\iota : K \to A$. Set $G = G_{L/k}$ and $G' = G_{K/k}$; we will construct a homomorphism $v : \mathrm{Inf}^G_{G'}(E) \to \mathrm{Inf}_{L/K}(A)$ as follows. Recall that elements of $\mathrm{Inf}^G_{G'}(E)$ can be represented by pairs $[x, e]$ with $x \in L^\times$, $e \in E \times_G G'$ and $[xa, e] = [x, i(a)e]$ for $a \in K^\times$. For $[x, e] \in \mathrm{Inf}^G_{G'}(E)$ we define $v(x, e)$ to be the L-linear endomorphism of $L \otimes_K V_A$ given by

$$\ell \otimes w \mapsto \ell x \otimes u(\tau(e))w$$

where $\tau : E \times_G G' \to E$ is the projection. Denote by $\bar{v}$ the induced map

$$\bar{v} : \mathrm{Inf}^G_{G'}(E) \to \mathrm{End}_k(L \otimes_K V_A).$$

The image of $\bar{v}$ clearly lies in the centralizer of the image of the map $r : L \otimes_k A^{\mathrm{op}} \to \mathrm{End}_k(L \otimes_K V_A)$ induced by right mulitplication on A, and thus factors through a map $v : \mathrm{Inf}^G_{G'}(E) \to \mathrm{Inf}_{L/K}(A)$ as required.

On the other hand the k-algebra homomorphism $L \to \mathrm{End}_k(L \otimes_K V_A)$ embeds L into the centralizer of the image of r, yielding a k-algebra homomorphism $j : L \to \mathrm{Inf}_{L/K}(A)$. It is easily checked that v and j satisfy the conditions of proposition 4.2.3.1. Therefore there is a k-algebra homomorphism

$$f : L \Vdash \mathrm{Inf}^G_{G'}(E) \to \mathrm{Inf}_{L/K}(A)$$

compatible with the embeddings of L as a maximal commutative subalgebra of source and target. Since both source and target have the same k-dimension, f is an isomorphism. ■

To summarize the results of this section: If L/k is a Galois extension with group G, $H \subseteq G$ and $K = L^H$, the restriction functor induces on isomorphism classes the homomomorphism $\mathrm{Br}(L/k) \to \mathrm{Br}(L/K)$ given by $A \mapsto K \otimes_k A$, and then the diagram

$$\begin{tikzcd}
\mathrm{Br}(L/K) \arrow[r] \arrow[d] & \mathrm{Ext}(G, L^\times) \arrow[r] \arrow[d, "\mathrm{Res}"] & H^2(G, L^\times) \arrow[d, "\mathrm{Res}"] \\
\mathrm{Br}(L/K) \arrow[r] & \mathrm{Ext}(H, L^\times) \arrow[r] & H^2(H, L^\times)
\end{tikzcd} \tag{4.2.5.6}$$

is commutative. If H is normal in G and $G' = G/H$, the inflation functor yields on passage to isomorphism classes the canonical inclusion $\mathrm{Br}(K/k) \to \mathrm{Br}(L/k)$, and

$$\begin{tikzcd}
\mathrm{Br}(K/k) \arrow[r] \arrow[d] & \mathrm{Ext}(G', K^\times) \arrow[r] \arrow[d, "\mathrm{Inf}"] & H^2(G', K^\times) \arrow[d, "\mathrm{Inf}"] \\
\mathrm{Br}(L/k) \arrow[r] & \mathrm{Ext}(G, L^\times) \arrow[r] & H^2(G, L^\times)
\end{tikzcd} \tag{4.2.5.7}$$

is commutative.

4.3 Nonarchimedean Fields

The aim of this section is to compute the Brauer group of a discretely valued nonarchimedean field with perfect residue field, given that the Brauer group of the residue field is known. Since the case of a local field is the one of interest in class field theory we treat this first.

4.3.1 Local fields. We will need the following general result:

4.3.1.1 Proposition *If K is a nonarchimedean field, any central simple K-algebra of finite degree splits over an unramified extension of K.*

The argument is completely parallel to that of proposition 4.1.3.11, with lemma 4.3.1.2 replaced by the following:

4.3.1.2 Lemma *Suppose K is a discretely valued nonarchimedean field and D is a central division algebra over K. If every subfield of D is totally ramified over K then $D = K$.*

Proof. Suppose $b \in D \setminus K$ and let $L = K(b)$. By hypothesis L/K is totally ramified. Choose a uniformizer $\pi \in \mathcal{O}_D$. Since L/K is totally ramified we may write $b = a_0 + b_1\pi$ with $a_0 \in K$. Similarly $b_1 = a_1 + b_2\pi$ with $a_1 \in K$, and by induction

$$b = a_0 + a_1\pi + a_2\pi^2 + \cdots + b_n\pi^n \quad \text{with } a_i \in K,\ b_n \in L$$

for all n. Thus b is in the closure of $K(\pi)$. Since $[K(\pi) : K]$ is finite, $K(\pi)$ is closed in D, and it follows that $b \in K(\pi)$. Since b was any element of D, $D = K(\pi)$ is commutative, so $D = K$. ■

The proof of proposition 4.3.1.1 repeats that of proposition 4.1.3.11 with "separable" replaced by "unramified."

The structure of the relative Brauer group of a finite unramified extension of local fields follows from proposition 3.3.3.1 and the calculations following it.

4.3.1.3 Theorem *Let L/K be a finite Galois extension of local fields with residual extension k_L/k and Galois group G. Let $n = [L : K]$ and let $G \simeq \mathbb{Z}/n\mathbb{Z}$ be isomorphism which to $1 \in \mathbb{Z}/n\mathbb{Z}$ associates the lifting of the qth power Frobenius of k_L to L. There is a canonical isomorphism*

$$\mathrm{inv}_{L/K} : \mathrm{Br}(L/K) \to \frac{1}{n}\mathbb{Z}/\mathbb{Z} \tag{4.3.1.1}$$

such that $1/n \mod \mathbb{Z}$ is the image of the class in $\mathrm{Br}(L/K)$ represented by the cyclic algebra defined by the cocycle

$$a_{i,j} = \begin{cases} 1 & i + j < n \\ \pi & i + j \geq n. \end{cases} \tag{4.3.1.2}$$

where π is any uniformizer of K, and as before we identify $i \in \mathbb{Z}/n\mathbb{Z}$ with its lifting in $[0, n)$.

Proof. This follows from the case $n = 2$ of proposition 3.3.3.1 and the computation of $K^\times/N_{L/K}(L^\times)$ in proposition 2.4.1.5. ■

In particular every central simple algebra of finite dimension over K is a cyclic algebra.

The isomorphism 4.3.1.1 is the *invariant map*. If A is a central simple K-algebra split by L we write $\mathrm{inv}_{L/K}(A)$ for $\mathrm{inv}_{L/K}([A])$ and call it the *invariant* of A. The discussion following proposition 3.3.3.1 shows that if $\mathrm{inv}_{L/K}(A) = r/n$ modulo 1, A is similar to the cyclic algebra defined by the relations

$$xa = {}^\sigma a x,\ a \in L, \qquad x^n = \pi^a. \tag{4.3.1.3}$$

If we recall that any central simple K-algebra has an unramified extension of L of K embedded as a maximal commutative subalgebra, we can give a more intrinsic description of the invariant (the classical definition, in fact). It suffices to treat the case of a central division algebra over K, and recall that for any such algebra D the absolute value of K extends uniquely to D. Denote by v_D the extension to D of the normalized valuation of K. The Noether-Skolem theorem implies that any automorphism of L extends to an inner automorphism of D; in particular there is an $x \in D$ such that such that $xax^{-1} = {}^\sigma a$ for all $a \in L$, and x is determined up to a factor in L. Then

$$\mathrm{inv}_{L/K}(D) = v_D(x) \mod \mathbb{Z}. \tag{4.3.1.4}$$

In fact 4.3.1.3 shows that the x defined there can serve as the x in 4.3.1.4, and the last equality in 4.3.1.3 shows that

$$v_D(x) = \frac{a}{n} = \mathrm{inv}_{L/K}(D).$$

Suppose now L'/L is an unramified extension of degree m, so that L'/K is unramified of degree mn, and let G' be the Galois group of L'/K. We are then in the situation of of the commutative diagram 4.2.5.7 with $L'/L/K$ replacing $L/K/k$ and the roles of G and G' are reversed. The description of the inflation map in cohomology shows that

$$\begin{tikzcd}
\mathrm{Br}(L/K) \arrow[r] \arrow[d] & H^2(G, L^\times) \arrow[r, "v_L"] \arrow[d, "\mathrm{Inf}"] & H^2(G, \mathbb{Z}) \arrow[d, "\mathrm{Inf}"] & \mathrm{Hom}(G', \mathbb{Q}/\mathbb{Z}) \arrow[l, "\partial"'] \arrow[d, "\mathrm{Inf}"] \\
\mathrm{Br}(L'/K) \arrow[r] & H^2(G', (L')^\times) \arrow[r, "v_{L'}"] & H^2(G', (L')^\times) & \mathrm{Hom}(G', \mathbb{Q}/\mathbb{Z}) \arrow[l, "\partial"']
\end{tikzcd}$$

is commutative. Now G and G' have canonical generators, the lifting to L and L' of the Frobenius of the residual extension. If $n = [L : K]$ and $n' = [L' : K] = nm$, this fixes isomorphisms $G \simeq \mathbb{Z}/n\mathbb{Z}$ and $G' \simeq \mathbb{Z}/n'\mathbb{Z}$, as well as canonical identifications $\mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) \simeq (1/n)\mathbb{Z}/\mathbb{Z}$, $\mathrm{Hom}(G', \mathbb{Q}/\mathbb{Z}) \simeq (1/n')\mathbb{Z}/\mathbb{Z}$ making

$$\begin{tikzcd}
\mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) \arrow[r] \arrow[d, "\mathrm{Inf}"] & \frac{1}{n}\mathbb{Z}/\mathbb{Z} \arrow[d] \\
\mathrm{Hom}(G', \mathbb{Q}/\mathbb{Z}) \arrow[r] & \frac{1}{n'}\mathbb{Z}/\mathbb{Z}
\end{tikzcd}$$

where the right hand vertical arrow is the natural inclusion. Therefore

$$\begin{array}{ccc} \mathrm{Br}(L/K) & \xrightarrow{\mathrm{inv}_{L/K}} & \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \\ \downarrow & & \downarrow \\ \mathrm{Br}(L'/K) & \xrightarrow{\mathrm{inv}_{L'/K}} & \frac{1}{[L':K]}\mathbb{Z}/\mathbb{Z} \end{array} \tag{4.3.1.5}$$

and since $\mathrm{Br}(K)$ is the direct limit of the relative Brauer groups $\mathrm{Br}(L/K)$ with L/K unramified, we have proven:

4.3.1.4 Theorem *The direct limit of the invariant maps is an isomorphism*

$$\mathrm{inv}_K : \mathrm{Br}(K) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}. \tag{4.3.1.6}$$

4.3.2 Finite fields. Along the way, the following important result got lost in the shuffle:

4.3.2.1 Theorem *The Brauer group of a finite field is trivial.*

Proof. It suffices to show that $\mathrm{Br}(k'/k)$ is trivial for any finite extension of k. If G is the Galois group of k'/k,

$$\mathrm{Br}(k'/k) \simeq H^2(G, (k')^\times) \simeq \hat{H}^0(G, (k')^\times) \simeq k^\times / N_{k'/k}(k')^\times$$

and the last group is trivial by lemma 2.4.1.4. ■

One consequence is a celebrated theorem of Wedderburn:

4.3.2.2 Corollary *A finite division ring is a field.*

Proof. Such a ring is evidently central simple over its center, which is a finite field. ■

Since you can't have too many proofs of a good theorem, we include two more:

4.3.2.3 Second proof. Let D be a finite division algebra of degree d^2 over its center k. A maximal subfield K of D has $[K : k] = d$, so all of the maximal subfields of D are isomorphic. Fix a maximal subfield K of D and let $x \in D$; then x is contained in a subfield of D isomorphic to K, and therefore conjugate to K by Noether-Skolem. Thus D is the union of conjugates of K, but a finite group can not be a union of the conjugates of a proper subgroup (exercise). Therefore $D = K = k$.

4.3.2.4 Third proof. Again let D be a finite division ring of degree d^2 over its center k. Any k-subalgebra $F \subseteq D$ is a division ring; then D is a left F-vector space and F is a k-vector space. For any $x \in D$ let $D(x)$ denote the centralizer of x in D. If $|k| = q$ then $|D(x)| = q^{d(x)}$ for some integer $d(x)$, and if $|D| = q^n$ then $d(x)|n$ for all x. The class equation of $D^\times$ is then

$$q^n - 1 = q - 1 + \sum_x \frac{q^{d(x)} - 1}{q - 1}$$

where the sum is over representatives of the non-central conjugacy classes of $D^\times$.

Suppose now $n > 1$ and let $P(X)$ be the nth cyclotomic polynomial, i.e. $P(X) = \prod_\zeta (X - \zeta)$ where ζ runs through the nth roots of 1 in $\mathbb{C}$. Then $P(X) \in \mathbb{Z}[X]$ (another exercise) and for any $m < n$ dividing n, $P(X)$ divides $(X^n - 1)/(X^m - 1)$. Then $P(q)$ divides $q^n - 1$ and all of the terms $(q^{d(x)} - 1)/(q-1)$ in the above sum. Therefore $P(q)$ divides $q-1$, but this is impossible since $P(q) = \prod_\zeta (q - \zeta)$ and $|q - \zeta| > q - 1$ for all primitive nth roots ζ of 1.

We can now complete our discussion of the structure of division algebras over a local field.

4.3.2.5 Theorem *Suppose D is a division algebra of finite degree n^2 over a local field K. Then D has order in $\mathrm{Br}(K)$ and its invariant is a/n with $\gcd(a, n) = 1$. The residue ring of D is a finite field, and*

$$e_{D/K} = f_{D/K} = n.$$

Conversely if A is a central simple K-algebra of degree n^2, invariant a/n and $\gcd(a, n) = 1$, A is a division algebra.

Proof. We know that we must have $e_{D/K} f_{D/K} = [D : K] = n^2$, and $f_{L/K} \geq n$, so we must show $e_{D/K} \geq n$. The proof of the equality 4.3.1.4 showed that there is an $x \in D$ such that $x^n = \pi^a$ where π is a uniformizer of K, where $a/n = \mathrm{inv}_K(D)$. It thus suffices to show that a and n are relatively prime, which will complete the proof. We can assume that $0 \leq a < n$.

Suppose d is a common divisor of a and n, choose $x \in D$ satisfying $x^n = \pi^a$ and set $y = x^{n/d}$ and $\tau = \pi^{a/d}$. Then

$$y^d - \tau^d = x^n - \pi^a = 0$$

while on the other hand

$$y^d - \tau^d = (y - \tau)(y^{d-1} + y^{d-2}\tau + \cdots + t^d) = 0$$

and thus $y = \tau$ or $y^{d-1} + y^{d-2}\tau + \cdots + \tau^d = 0$, but neither of these is possible if $d > 1$ since $1, x, \ldots, x^{n-1}$ are linearly independent over K.

For the last assertion it suffices to observe that we must have $A \simeq M_m(D)$ for some central K-division algebra D, and then $\mathrm{inv}_K(D) = a/n$. Since a and n are relatively prime, $[D : K] = n^2$ and $A = D$. ■

4.3.3 The General Case. Suppose now K is any discretely valued nonarchimedean field with perfect residue field and L/K is a finite unramified Galois extension with group G, normalized valuation v_L and residual extension k_l/k. The exact sequence

$$1 \to \mathcal{O}_L^\times \to L^\times \xrightarrow{v_L} \mathbb{Z} \to 0 \tag{4.3.3.1}$$

is split exact as a sequence of G-modules (since L/K is unramified, a uniformizer π of K is also a uniformizer of L, so it suffices to lift $1 \in \mathbb{Z}$ to a uniformizer of K). The long exact sequence of cohomology then decomposes into split short exact sequences

$$0 \to H^n(G, \mathcal{O}_L^\times) \to H^n(G, L^\times) \to H^n(G, \mathbb{Z}) \to 0. \tag{4.3.3.2}$$

Recall that a filtration $(A_n)_{n\geq 0}$ of an abelian group A is complete and separated if the natural homomorphism

$$A \to \varprojlim_n A/A_n$$

is an isomorphism.

4.3.3.1 Lemma *Suppose A is a G-module and $(A_n)_{n\in\mathbb{N}}$ is a filtration of A for which A is complete and separated. If $H^n(G, A_n/A_{n+1}) = 0$ for all $n \geq 0$ then $H^n(G, A) = 0$.*

Proof. Suppose u is an n-cocycle for (G, A). The exact sequences

$$H^n(G, A_{n+1}) \to H^n(G, A_n) \to H^n(G, A_n/A_{n+1}) = 0$$

show that we can define a sequences of n-cocycles (a_n) and n-cochains (b_n) for (G, A_n) such that $a = a_0$ and

$$a_n = \partial b_n + a_{n+1}$$

for all $n \geq 0$. Since A is complete and separated for the filtration, the sum $b = \sum_n b_n$ converges and the above equalities show that $a = \partial b$, so the class of a in $H^n(G, A)$ is zero. ■

Recall the filtration $U^n \subseteq \mathcal{O}_L^\times$ where $x \in U^n$ if and only if $x \equiv 1 \mod \mathfrak{m}^n$, and that $U^0/U^1 \simeq k_L^\times$ and $U^n/U^{n+1} \simeq k_L$ as G-modules. By proposition 3.4.1.1,

$$H^m(G, U^n/U^{n+1}) \simeq H^n(G, k_L) = 0$$

for $n > 0$ since G is also the Galois group of k_L/k. The previous lemma implies that

$$H^n(G, U^1) = 0 \qquad n > 0$$

and finally the long exact sequence obtained from

$$1 \to U^1 \to \mathcal{O}_L^\times \to k_L^\times \to 1$$

yields isomorphisms

$$H^n(G, \mathcal{O}_L^\times) \xrightarrow{\sim} H^n(G, k_L^\times) \tag{4.3.3.3}$$

for all $n > 0$. From 4.3.3.2 we get split short exact sequences

$$0 \to H^n(G, k_L^\times) \to H^n(G, L^\times) \to H^n(G, \mathbb{Z}) \to 0 \tag{4.3.3.4}$$

for $n > 0$. If we set $n = 2$ and recall the isomorphism

$$H^2(G, \mathbb{Z}) \simeq \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$$

the result is an exact sequence

$$0 \to \mathrm{Br}(k_L/k) \to \mathrm{Br}(L/K) \to \mathrm{Hom}(G_{L/K}, \mathbb{Q}/\mathbb{Z}) \to 0$$

where we have replace G by $G_{L/K}$. Passing to the direct limit over unramified extensions L/K then yields:

4.3.3.2 Theorem *If L/K is an unramified finite Galois extension of discretely valued nonarchimedean fields with residual extension k_L/k. If k is perfect and $G = \mathrm{Gal}(L/K)$ there is a split exact sequence*

$$0 \to \mathrm{Br}(k) \to \mathrm{Br}(K) \to \mathrm{Hom}_{cont}(G, \mathbb{Q}/\mathbb{Z}) \to 0 \tag{4.3.3.5}$$

where $\mathrm{Hom}_{cont}(G, \mathbb{Q}/\mathbb{Z})$ denotes the group of continuous homomorphisms $G \to \mathbb{Q}/\mathbb{Z}$ for the discrete topology of $\mathbb{Q}/\mathbb{Z}$.

Proof. The only point needing explanation is that $\mathrm{Hom}_{cont}(G, \mathbb{Q}/\mathbb{Z})$ is the direct limit of the groups $\mathrm{Hom}(G_{L/K}, \mathbb{Q}/\mathbb{Z})$. In fact the individual $\mathrm{Hom}(G_{L/K}, \mathbb{Q}/\mathbb{Z})$ inject into the direct limit and induce continuous homomorphisms $G \to \mathbb{Q}/\mathbb{Z}$. On the other hand since $\mathbb{Q}/\mathbb{Z}$ is discrete any continuous homomorphism $G \to \mathbb{Q}/\mathbb{Z}$ factors through a finite quotient. ■

The splitting is not canonical, but is determined by the choice of a uniformizer of K. The theorem shows a central simple K-algebra is similar to the product of algebras of one of two kinds, which we will now analyze.

The algebras arising from the term $\mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$ in 4.3.3.5 are cyclic, since any homomorphism $G \to \mathbb{Q}/\mathbb{Z}$ with finite image factors through a finite cyclic group. Formally they look like the algebras defined by 4.3.1.3, but now σ can be any generator of a cyclic quotient of G (and n is the order of the quotient).

The algebras corresponding to the term $\mathrm{Br}(k)$ are more interesting. Let us recall how they arise: they belong to the subgroup $H^2(G_{L/K}, \mathcal{O}_L^\times \subset H^2(G_{L/K}, L^\times)$ of $\mathrm{Br}(L/K)$ for some unramified L/K. In other words there is a cocycle representing the Brauer class that takes its values in $\mathcal{O}_L^\times$; following the usual terminology of algebraic geometry we could say that these classes have "good reduction." If $a_{s,t} \in Z^2(G, \mathcal{O}_L^\times)$ is any such cocycle, its reduction $\bar{a}_{s,t}$ modulo the maximal ideal represents a class in $\mathrm{Br}(k_L/k)$; conversely if a cocycle $\bar{a}_{s,t} \in Z^2(G, k_L^\times$ is given its "Teichmüller lift" $[\bar{a}_{s,t}] \in Z^2(G, \mathcal{O}_L^\times)$ yields an element of $\mathrm{Br}(L/K)$.

In fact we can say more. Let R be a local ring with maximal ideal $\mathfrak{m}$; an R-algebra A is an *Azumaya algebra* if it is free of finite type as an R-module, and the natural map $A \otimes_R A^{\mathrm{op}} \to \mathrm{End}_R(A)$ is an isomorphism (the map is the same one as in 4.1.2.9).

Chapter 5

The Reciprocity Isomorphism

Let L/K be a Galois extension of local fields with group G. In this chapter we establish an isomorphism $G^{ab} \xrightarrow{\sim} K^\times/N_{L/K}L^\times$, which for historical reasons is called the *reciprocity map*. Our method uses an explicit determination of the relative Brauer group $\mathrm{Br}(L/K)$, which so far has been carried out only if L/K is unramified.

5.1 F-isocrystals

The calculation of the Brauer group of a local field in the last section is nonconstructive, since the proof of existence of an unramified splitting field was nonconstructive. In this section we realize central simple algebras of a local field as endomorphism algebras of simple modules over a noncommutative ring, the *Dieudonné ring*.

In this section K is a discretely valuded nonarchimedean field with residue field k of characteristic $p > 0$, $q = p^f$ is a power of p and $\sigma : K \to K$ is a lifting of the qth power Frobenius. Further restrictions will be made on the way.

5.1.1 Definitions. An *F-isocrystal* is a finite-dimensional K-vector space V endowed with an σ-linear isomorphism $F : V \to V$, i.e. an additive map satisfying $F(av) = {}^\sigma a F(v)$ for all $a \in K$. The map F is called the *Frobenius structure* of the F-isocrystals. A morphism $f : (V, F) \to (V', F')$ is a K-linear map $f : V \to V'$ such that

$$\begin{tikzcd} V \arrow[r, "f"] \arrow[d, "F"'] & V \arrow[d, "F'"] \\ V \arrow[r, "f"'] & V' \end{tikzcd}$$

We denote by $\mathrm{FIsoc}(K, \sigma)$ the category of F-isocrystals on K. It is an abelian category: the kernel and cokernel of a morphism of F-isocrystals are F-isocrystals

and behave in the expected way. If σ is understood we will write $\mathrm{FIsoc}(K)$ for $\mathrm{FIsoc}(K, \sigma)$.

Certain basic constructions of linear algebra can be made for F-isocrystals, which we describe in the next few paragraphs. The *direct sum* of F-isocrystals (V, F_V), (W, F_W) is $V \oplus W$ with the Frobenius structure $F_V \oplus F_W$. The *tensor product* $V \otimes W$ of F-isocrystals (V, F_V) and (W, F_W) is $V \otimes_K W$ with the Frobenius structure $F(x \otimes y) = F_V(x) \otimes F_V(y)$ (note that this is well-defined). Similarly for exterior and symmetric products.

Suppose L/K is a finite extension and $\sigma : K \to K$ extends to a lifting $\sigma' : L \to L$ of the q-th power Frobenius of the residue field of L. The *extension of scalars to* L of an F-isocrystal (V, F) is the L-vector space $L \otimes_K M$ with the Frobenius structure

$$F(a \otimes v) = \sigma'(a) \otimes F(v).$$

This yields an exact functor

$$K\otimes : \mathrm{FIsoc}(K) \to \mathrm{FIsoc}(L).$$

Extension of scalars does not change the rank.

In the same situation as before we can define the *restriction of scalars to* K of an F-isocrystal (V, F) on L: it is simply V viewed as K-vector space endowed with the same F. This defines an exact functor

$$\mathrm{Res}_{L/K} : \mathrm{FIsoc}(L) \to \mathrm{FIsoc}(K)$$

and then

$$\dim_K \mathrm{Res}_{L/K}(V) = [L : K] \dim_L V.$$

For any finite extension L/K there is a functorial isomorphism

$$\mathrm{Hom}_K(M, \mathrm{Res}_{L/K}(N)) \xrightarrow{\sim} \mathrm{Hom}_L(L \otimes M, N) \tag{5.1.1.1}$$

induced by the usual adjunction morphism.

The nth *iterate* of a σ-F-isocrystal (M, F) is the σ^n-F-isocrystal V endowed with $F^n : M \to M$.

The *Tate twist* $V_K(n)$ for $n \in \mathbb{Z}$ is the F-isocrystal K with the Frobenius structure $F(a) = \pi^n a^\sigma$. More generally, if V is any F-isocrystal, the *nth twist* of V is the tensor product $V \otimes V(n)$.

5.1.2 The Dieudonné ring Our first task is to classify F-isocrystals on K when k is algebraically closed. The main tool is the *Dieudonné ring*, which we define as the crossed product algebra

$$\mathbb{D}_K = K \Vdash \mathbb{Z} \tag{5.1.2.1}$$

where $\mathbb{Z}$ acts on K by having $1 \in \mathbb{Z}$ act as σ. In the notation of section 4.2.3 the additive and multiplicative identites of $\mathbb{D}_K$ are $[0, 0]_0$ and $[1, 0]_0$ since additive notation is used for $\mathbb{Z}$! We use the canonical embedding $K \hookrightarrow K \Vdash \mathbb{Z}$ to identify

K with a subring of $\mathbb{D}_K$, so if in the notation of section we set $F = [1,1]_1$ then any $a \in \mathbb{D}_K$ has a unique expression

$$a = \sum_{n \in \mathbb{Z}} a_n F^n \tag{5.1.2.2}$$

and multiplication in $\mathbb{D}_K$ is done using the formula

$$Fa = a^\sigma F \tag{5.1.2.3}$$

for $a \in K$.

If $a \in \mathbb{D}_K$ is given by 5.1.2.2 and $a \neq 0$ let r (resp. s) is the largest (resp. smallest) integer n such that $a_n \neq 0$ we define the *degree* of a to be

$$\deg(a) = r - s. \tag{5.1.2.4}$$

It is immediate that

$$\deg(a) \geq 0 \tag{5.1.2.5}$$

$$\deg(ab) = \deg(a) + \deg(b) \tag{5.1.2.6}$$

for all nonzero a, $b \in \mathbb{D}_K$. If we define $\deg(0) = -\infty$ the second formula holds for all a and b in $\mathbb{D}_K$. From this we see that $\mathbb{D}_K$ has no left or right divisors of zero, and the units of $\mathbb{D}_K$ are the elements of degree zero, i.e. monomials aF^n for $a \in K$ and $n \in \mathbb{Z}$.

Any nonzero element of $\mathbb{D}_K$ is a unit times a "polynomial in F", so the usual division algorithm holds in the following form:

5.1.2.1 Lemma *For any a, $b \in \mathbb{D}_K$ with $b \neq 0$ there are q, q', r and $r' \in \mathbb{D}_K$ such that*

$$a = bq + r = q'b + r' \qquad \deg(r),\ \deg(r') < \deg b. \tag{5.1.2.7}$$

The usual argument then yields:

5.1.2.2 Proposition *Any left or right ideal in $\mathbb{D}_K$ is principal.*

A left $\mathbb{D}_K$-module M has a K-vector space structure by the restriction of scalars $K \to \mathbb{D}_K$, and the map $F : M \to M$ given by left multiplication by $F \in \mathbb{D}_K$ is semilinear by 5.1.2.3, so (M, F) is an F-isocrystal on K. Conversely an F-isocrystal (V, F) has a natural structure as a left $\mathbb{D}_K$-module, and this allows us to identify $\mathrm{FIsoc}(K)$ with the category of left $\mathbb{D}_K$-modules of finite dimension over K.

For the rest of this section we assume that the residue fields k of K is algebraically closed (we will frequently repeat this hypothesis for emphasis). By corollary 1.3.6.3 K has a uniformizer π that is fixed by σ. We fix such a uniformizer; from 5.1.2.3 it follows that π is in the center of $\mathbb{D}_K$.

It will be useful to adopt the convention that rational numbers, unless specified otherwise, are written in lowest terms. The integer 0 in lowest terms is 0/1. With this convention we define, for any $\lambda = r/d \in \mathbb{Q}$, $V_K(\lambda)$ is the F-isocrystal

$$V_K(\lambda) = \mathbb{D}_K/\mathbb{D}_K(F^d - \pi^r) \tag{5.1.2.8}$$

and note that when $\lambda = n/1$ with $n \in \mathbb{Z}$ this coincides with our earlier definition. The division algorithm 5.1.2.7 shows that $V_K(\lambda)$ has dimension d; in fact the images of 1, $F, \ldots, F^{d-1} \in \mathbb{D}_K$ are a K-basis of $V_K(\lambda)$. It will sometimes be useful to write this basis as

$$e_i^\lambda = F^i \mod (F^d - \pi^r) \qquad 0 \le i < d. \tag{5.1.2.9}$$

With $\lambda = r/d$ as before we define K_λ to be the fixed field of σ^d. When the residue field k is algebraically closed K_λ is the unramified extension of $K_0 = K^\sigma$ of degree d, and in general is some subfield of this containing K_0. In any case it is a local field by theorem 1.3.6.5. The definition 5.1.2.8 shows that right multiplication by elements of K_λ defines an embedding $K_\lambda \to D_\lambda$.

The goal of the next few sections is to show that the $V_K(\lambda)$ are simple $\mathbb{D}_K$-modules, and that any F-isocrystal on K is a direct sum of modules of this form.

5.1.3 Cyclic Modules. The first task is to compute the endomorphism rings of the $V_K(\lambda)$ and the Ext groups $\mathrm{Ext}^i_{\mathbb{D}_K}(V_K(\lambda), V_K(\mu))$. We may as well look at the problem for cyclic modules in general, so in this section R is any ring with identity, $f \in R$ is not a right zero-divisor, and M is the left R-module R/Rf. Then

$$0 \to R \xrightarrow{\cdot f} R \to M \to 0$$

is a resolution of M by free R-modules, and for any left R-module N the groups $\mathrm{Ext}^i_R(M, N)$ are computed by the complex

$$\cdots \to 0 \to N \xrightarrow{f\cdot} N \to 0 \to \cdots$$

whose nonzero terms are in degrees 0 and 1. Denoting by ${}_fN$ the kernel of left multiplicatin by f in N, we find that

$$\begin{aligned} &\mathrm{Hom}_R(M, N) \simeq {}_fN, \\ &\mathrm{Ext}^1_R(M, N) \simeq N/fN, \\ &\mathrm{Ext}^n_R(M, N) = 0 \quad n \ge 2. \end{aligned} \tag{5.1.3.1}$$

We now apply this calculation to $R = \mathbb{D}_K$ and $f = F^r - \pi^d$:

5.1.3.1 Proposition *Suppose k is algebraically closed and λ, $\mu \in \mathbb{Q}$.*

(i). If $\lambda \ne \mu$ then $\mathrm{Hom}_{\mathbb{D}_K}(V_K(\lambda), V_K(\mu)) = 0$.

(ii). $\mathrm{Ext}^n_{\mathbb{D}_K}(V_K(\lambda), V_K(\mu)) = 0$ *for all* λ, $\mu \in \mathbb{Q}$ *and* $n \geq 1$.

Proof. Write $\lambda = r/d$ as before. By the isomorphisms 5.1.3.1 it suffices to show that left multiplication by $F^d - \pi^r$ on $V_K(\mu)$ is (1) injective if $\mu \neq \lambda$, and (2) surjective in any case. Write $\mu = r'/d'$.

(1) Suppose x is in the kernel of left multiplication by $F^d - \pi^r$ on $V_K(\mu)$. Recall that $1, F, \ldots, F^{d'-1} \in \mathbb{D}_K$ reduce to a K-basis of $e_0^\mu, \ldots, e_{d'-1}^\mu$ of $V_K(\mu)$; then with $x = \sum_i a_i e_i^\mu$,

$$F^{dd'}(x) = \sum_i a_i^{\sigma^{dd'}} \pi^{dr'} e_i^\mu \quad \text{and} \quad \pi^{rd'} x = \sum_i \pi^{rd'} a_i e_i^\mu.$$

Since $r'd \neq rd'$, we cannot have $F^{dd'}(x) = \pi^{rd'} x$ unless all a_i are zero.

(2) Again with $\mu = r'/d'$, the identity

$$F^{dd'} - \pi^{rd'} = (F^d - \pi^r)(F^{d(d'-1)} + \pi^r F^{d(d'-2)} + \cdots + \pi^{r(d'-1)})$$

shows that it suffices to prove that $F^{dd'} - \pi^{rd'}$ is surjective. For $x = \sum_i a_i e_i^\mu \in V_K(\mu)$ we see that

$$(F^{dd'} - \pi^{rd'})x = \sum_i (a_i^{\sigma^{dd'}} - \pi^{rd'} a_i) e_i^\mu$$

the assertion follows from corollary 1.3.6.4 ■

5.1.4 The Endomorphism Ring of $V_K(\lambda)$. When $N = M$ the first isomorphism of 5.1.3.1 is

$$\mathrm{End}(M) \simeq {}_f M$$

and it can be described explicitly as follows: $\alpha \in \mathrm{End}(M)$ corresponds to right multiplication by any element of R lifting $\alpha(e)$, where $e \in M = R/Rf$ is the image of $1 \in R$. It is easy to check directly that this is well-defined: if $m \in M$ and $\alpha \in {}_f M$, we choose $\underline{m} \in R$ and $\underline{a}$ representing m and $\alpha(e)$ respectively; the image of $\underline{ma}$ in M is independent of the choice of $\underline{m}$ since any other choices would be $\underline{m} + xf$, $\underline{a} + yf$ with x, $y \in R$, and then

$$(\underline{m} + xf)(\underline{a} + yf) = \underline{m}\,\underline{a} + \text{element of } Rf$$

since $fa = 0$ in M.

We can now determine the structure of the endomorphism ring

$$D_\lambda = \mathrm{End}(V_K(\lambda))$$

which we identify, as in 5.1.3, with the kernel of $F^d - \pi^r$ on $V_K(\lambda)$. As before the image of $F^i \in \mathbb{D}_K$ in $V_K(\lambda)$ for $0 \leq i < d$ will be denoted by e_i^λ with $i \in \mathbb{Z}/d\mathbb{Z}$, and $e_0^\lambda, \ldots, e_{d-1}^\lambda$ is a K-basis of $V_K(\lambda)$. The kernel of $F^d - \pi^r$ is the set of $a_0 + a_1 F + \cdots + a_{d-1} F^{d-1}$ with $a_i \in K_\lambda$, and recall that if k is algebraically closed K_λ is an extension of K_0 of degree d.

As before we identify $a \in K_\lambda$ with the corresponding endomorphism (right multiplication by a) of $V_K(\lambda)$, and denote by ξ the endomorphism corresponding to right multiplication by F. From this it is clear that D_λ is a K_λ-vector space with basis $1, \xi, \ldots, \xi^{d-1}$, and that

$$\xi^d = \pi^r, \qquad a\xi = \xi a^\sigma \tag{5.1.4.1}$$

in D_λ.

5.1.4.1 Proposition *Suppose the residue field of K is algebraically closed. If $\lambda = r/d$ in lowest terms, D_λ is a central division algebra over $K_0 = K^\sigma$ of degree d^2, invariant $-\lambda$ modulo $\mathbb{Z}$ and containing K_λ as a maximal commutative subfield.*

Proof. From 5.1.4.1 we see that the center of D_λ is K_0. Since π is a unit in D_λ so is x, and if we set $x = \xi^{-1}$ the relations

$$x^d = \pi^{-r} \qquad xa = {}^\sigma a x$$

show that D is a central simple K^σ-algebra with invariant $-r/d$. Since r and d are relatively prime, D is a division algebra by theorem 4.3.2.5. The last statement is clear. ■

5.1.5 The classification: k algebraically closed. We now suppose that the residue field of K is algebraically closed. Let $\lambda = r/d$ with the fraction in lowest terms, let $L = K(\pi^{1/d})$, and extend σ to L by setting $\sigma(\pi^{1/d}) = \pi^{1/d}$. Then $\mathcal{O}_L = \mathcal{O}_K[\pi^{1/d}]$ has the $\mathcal{O}_K$-basis $\pi^{i/d}$ for $0 \le i < d$. Since $e_0^{d\lambda} \in V_L(d\lambda)$ is a basis of the rank one F-isocrystal $V_L(d\lambda)$, the $\pi^{i/d} e_i^{d\lambda}$ for $0 \le i < d$ form a basis of the F-isocrystal $\mathrm{Res}_{L/K} V_L(d\lambda)$. It is easily checked that the linear map sending $\pi^{i/d} e_0^{d\lambda}$ to e_i^λ is an isomorphism

$$\mathrm{Res}_{L/K} V_L(d\lambda) \xrightarrow{\sim} V_K(\lambda). \tag{5.1.5.1}$$

5.1.5.1 Lemma *Let $F^n + a_1 F^{n-1} + \cdots + a_{n-1} F + a_n$ be an element of $\mathbb{D}_K$ such that $a_i \neq 0$ for some i. Suppose*

$$\inf_i \frac{v_\pi(a_i)}{i} = \lambda = \frac{r}{d} \qquad \gcd(r, d) = 1 \tag{5.1.5.2}$$

and let $L = K(\pi^{-d}$. There are $b_1, \ldots, b_{n-1} \in L$ and $u \in \mathcal{O}_L^\times$ such that

$$(F^n + a_1 F^{n-1} + \cdots + a_{n-1} F + a_n) u = (b_0 F^{n-1} + b_1 F^{n-2} + \cdots + b_{n-1})(F - \pi^\lambda) \tag{5.1.5.3}$$

in $\mathbb{D}_L$.

Proof. Since π is in the center of $\mathbb{D}_K$ there is an automorphism of $\mathbb{D}_K$ such that $F \mapsto \pi^\lambda F$. Applying this automorphism to 5.1.5.3 and dividing by π^λ yields an equality similar to 5.1.5.3 with a_i, b_i and $F - \pi^\lambda$ replaced by $\pi^{-\lambda i} a_i$, $\pi^{-\lambda i} b_i$

and $F-1$ respectively. Thus it suffices to prove the lemma in the case where all a_i are in $\mathcal{O}_K$, at least one is a unit, and $\lambda = 0$. The b_i are determined by

$$(F^n + a_1F^{n-1} + \cdots + a_{n-1}F + a_n)u = (b_0F^{n-1} + b_1F^{n-2} + \cdots + b_{n-1})(F-1) \tag{5.1.5.4}$$

or equivalently

$$u^{\sigma^n}F^n + u^{\sigma^{n-1}}a_1F^{n-1} + \cdots + ua_n = b_0F^n + (b_1 - b_0)F^{n-1} + \cdots + (b_{n-1} - b_{n-2})F - b_n$$

so that u and the b_i satisfy

$$\begin{aligned} u^{\sigma^n} &= b_0 \\ a_1u^{\sigma^{n-1}} &= b_1 - b_0 \\ &\cdots\cdots \\ a_{n-1}u^{\sigma} &= b_{n-1} - b_{n-2} \\ a_n &= -b_{n-1}. \end{aligned}$$

If these equations are satisfied, then u is a solution of

$$u^{\sigma^n} + a_1u^{\sigma^{n-1}} + \cdots + a_nu = 0 \tag{5.1.5.5}$$

and conversely if u is a solution of 5.1.5.5 then $b_i \in \mathcal{O}_L$ can be found satisfying 5.1.5.4. Finally, since k is algebraically closed, 5.1.5.5 always has a solution by lemma 1.3.6.2. ■

5.1.5.2 Lemma *If k is algebraically closed and M is a nonzero F-isocrystal, there is a nonzero homomorphism $M \to V_K(\lambda)$ for some λ.*

Proof. Set $L = K[\pi^{1/d}]$ as before. By replacing M by a quotient, if necessary, we can assume M is simple, and therefore cyclic, say $M = \mathbb{D}_K/\mathbb{D}_KP$ for some $P \in \mathbb{D}_K$. Write $P = F^n + a_1F^{n-1} + \cdots + a_n$; since F is bijective on M we must have $a_n \neq 0$, and the previous lemma is applicable. Write $Pu = Q(F - \pi^\lambda)$ with $\lambda = r/d$ as in 5.1.5.2 and $Q \in \mathbb{D}_L$. Since $M \simeq \mathbb{D}_K/(Pu)$, we see that $L \otimes_K M$ has $V_L(d\lambda) \simeq \mathbb{D}_L/(F - \pi^\lambda)$ as a quotient, say via a map $L \otimes_K M \to V_L(d\lambda)$. Applying the restriction functor and using 5.1.5.1 yields a morphism $M \to V_K(\lambda)$ which is nonzero, for if it were zero the morphism $L \otimes_K M \to V_L(d\lambda)$ corresponding to it by adjunction would also be zero. ■

5.1.5.3 Proposition *The F-isocrystal $V_K(\lambda)$ is a simple object of* $\mathrm{FIsoc}(K)$.

Proof. Suppose M is a proper submodule of $V_K(\lambda)$. By lemma 5.1.5.2 there is a nontrivial morphism $f : V_K(\lambda)/M \to V_K(\mu)$ for some μ. By the first part of proposition 5.1.3.1 we must have $\lambda = \mu$. The composite map

$$V_K(\lambda) \to V_K(\lambda)/M \xrightarrow{f} V_K(\lambda)$$

is an element of the division algebra $\mathrm{End}(V_K(\lambda)) = D_\lambda$, and is therefore an isomorphism. It follows that $M = 0$. ■

5.1.5.4 Proposition *If k is algebraically closed, a simple F-isocrystal is isomorphic to some $K(\lambda)$. For $\lambda \neq \mu$ the isocrystals $V_K(\lambda)$ and $V_K(\mu)$ are nonisomorphic.*

Proof. For any M there is a surjective morphism $M \to V_K(\lambda)$ for some λ which, if M is simple, must be an isomorphism. The second statement follows from the first part of proposition 5.1.3.1. ■

We can now prove Dieudonné's classification theorem [6], c.f. also Manin [9]:

5.1.5.5 Theorem *If k is algebraically closed, any F-isocrystal on K is a direct sum of simple F-isocrystals, and a simple F-isocrystal is isomorphic to $V_K(\lambda)$ for a unique $\lambda \in \mathbb{Q}$.*

Proof. We have shown that every $V_K(\lambda)$ is simple (proposition 5.1.5.4), and proposition 5.1.3.1 shows that $V_K(\lambda)$ and $V_K(\mu)$ are nonisomorphic when $\lambda \neq \mu$. This establishes the last statement. Furthermore lemma 5.1.5.2 shows that any nonzero F-isocrystal has some $V_K(\lambda)$ as a quotient: since $V_K(\lambda)$ is simple, a nonzero homomorphism $V \to V_K(\lambda)$ must be surjective. To conclude the proof it suffices to show that $\mathrm{Ext}^1(V, V_K(\lambda)) = 0$ for any F-isocrystal V, but this follows by induction on $\dim_K V$ from the equality $\mathrm{Ext}^1_{\mathbb{D}_K}(V_K(\mu), V_K(\lambda)) = 0$ (proposition 5.1.3.1). ■

5.1.6 Slopes. Theorem 5.1.5.5 asserts that an F-isocrystal M over a field K with algebraically closed residue field k has a direct sum decomposition

$$M = \bigoplus_{\lambda \in \mathbb{Q}} V_K(\lambda)^{m_\lambda} \tag{5.1.6.1}$$

and the set of $\lambda \in \mathbb{Q}$ for which $m_\lambda \neq 0$ are the *slopes* of M. For each $\lambda \in S$ we define the *multiplicity of λ in M* to be

$$\mathrm{mult}_\lambda(M) = m_\lambda \dim_K V_K(\lambda). \tag{5.1.6.2}$$

Explicitly, if $\lambda = r/d$ then $\mathrm{mult}_\lambda(M) = dm_\lambda$.

We may rewrite 5.1.6.1 as

$$M = \bigoplus_{\lambda \in S} M^\lambda \tag{5.1.6.3}$$

where S is a finite subset of $\mathbb{Q}$ and M^λ is the sum of all sub-F-isocrystals of M isomorphic to $K(\lambda)$. This decomposition is *functorial* in M: if N is another F-isocrystal on K with slope decomposition $N = \oplus_\lambda N^\lambda$, then any morphism $F : M \to N$ induces morphisms $M^\lambda \to N^\lambda$ for all λ; this follows immediately from part (i) of proposition 5.1.3.1.

We say M is *isopentic of slope* λ if $\mathrm{mult}_\mu = 0$ for all $\mu \neq \lambda$ (some authors use the term *isoclinic*). We say that M is *unit-root* if it is isopentic of slope 0.

It will be useful to write the slopes of an F-isocrystal as an increasing sequence

$$\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_d \tag{5.1.6.4}$$

in which each slope is repeated as many times as its mulitplicity, so that d is the dimension of M.

Still supposing that the residue field of K is algebraically closed, let (V, F) is an F-isocrystal on K with slopes $\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_d$. It is clear from the definitions that

$$\text{The } n\text{-th iterate } (V, F^n) \text{ has slopes } n\lambda_1 \leq n\lambda_2 \leq \cdots \leq n\lambda_d \tag{5.1.6.5}$$

$$\text{The twist } M \otimes K(i) \text{ has slopes } \lambda_1 + i \leq \lambda_2 + i \leq \cdots \leq \lambda_d + i. \tag{5.1.6.6}$$

For more complicated operations we need the following description of the slopes. If K is any nonarchimedean field, a *lattice* in a K-vector space V of finite dimension is a finite $\mathcal{O}_K$-submodule $M \subset V$ such that the natural map $K \otimes_{\mathcal{O}_K} M \to V$ is an isomorphism.

5.1.6.1 Proposition *Suppose the residue field of K is algebraically closed. The slopes of an F-isocrystal (M, F) are contained in the interval $[\lambda, \mu]$ if and only if for some uniformizer π of K and some lattice $M_0 \subset M$ there are constants C, D such that*

$$\pi^{[n\mu]+C} M_0 \subseteq F^n(M_0) \subseteq \pi^{[n\lambda]+D} M_0 \tag{5.1.6.7}$$

independently of n.

Proof. We first observe that the validity of 5.1.6.7 is independent of π, and it is also independent of the choice of M_0. In fact if 5.1.6.7 holds for M_0 and M_1 is any another lattice there are integers a and b such that

$$\pi^a M_1 \subseteq M_0 \subseteq \pi^b M_1$$

and then 5.1.6.7 holds for M_1 with C and D replaced by $C + a - b$ and $D + b - a$ respectively.

To show that the condition 5.1.6.7 is necessary it therefore suffices to show that it holds for $M = V_K(\lambda)$ with $\mu = \lambda$, for we may take as the lattice the direct sum of lattices in each summand of M of the form $V(\lambda)$. If we take the lattice to be the $\mathcal{O}_K$-span $V_K^0(\lambda)$ of the standard basis $\{e_i^\lambda\}$ of $V_K(\lambda)$ and $\lambda = r/d$, then

$$F^m e_0 = \pi^{[m\lambda]} e_m$$

where as before we view the subscripts as elements of $\mathbb{Z}/d\mathbb{Z}$. This leads to the estimate

$$F^m e_i = \pi^{[m\lambda]+C} e_{i+m} \tag{5.1.6.8}$$

with $C = 0$ or r depending on i and m, and with the same convention on subscripts. Then 5.1.6.7 with $\mu = \lambda$ follows immediately.

Suppose conversely that ν is a slope of M and 5.1.6.7 holds. Choose a direct summand of M isomorphic to $V_K(\nu)$, let V_ν be a lattice in this summand and

let V' be an F-stable sub-$\mathcal{O}_K$-module of M such that $V_\nu \oplus V'$ is a lattice in M. By 5.1.6.7 we have

$$\pi^{[n\mu]+C} V_\nu \subseteq F^n(V_\nu) \subseteq \pi^{[n\lambda]+D} V_\nu$$

and by our previous result,

$$\pi^{[n\nu]+E} V_\nu \subseteq F^n(V_\nu) \subseteq \pi^{[n\nu]+G} V_\nu$$

for all n and some constants E, G, from which it follows that $\lambda \leq \nu \leq \mu$. ■

From this we see how slopes vary with base change:

5.1.6.2 Corollary *Suppose L is an extension of K with ramification index e.*
(1) If V is an F-isocrystal on K with slopes

$$\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_d$$

the slopes of $L \otimes_K V$ are

$$e\lambda_1 \leq e\lambda_2 \leq \cdots \leq e\lambda_d.$$

(2) If V is an F-isocrystal on L with slopes

$$\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_d$$

the slopes of $\mathrm{Res}_{L/K} V$ *are*

$$\lambda_1/e \leq \lambda_2/e \leq \cdots \leq \lambda_d/e.$$

Proof. The first assertion is clear from the definitions. For the second it suffices to check it for $V = V_K(\lambda)$, which is done in the same way as in the argument for 5.1.5.1. ■

Proposition 5.1.6.1 shows that the slopes of an F-isocrystal behave like the p-adic ordinals of the eigenvalues of a linear transformation with respect to the operations of linear algebra. For more precise statements see exercises 5.1.7.4 and 5.1.7.5.

5.1.7 Exercises

5.1.7.1 Let V be a K-vector space. Show that a σ-linear map $F : V \to V$ is the same as a linear map $V^{(\sigma)} \to V$, where $V^{(\sigma)} = K \otimes_{K,\sigma} V$.

5.1.7.2 Let V and W be F-isocrystals on K. If $f \in \mathrm{Hom}_K(V, W)$, show that

$$V \xrightarrow{F_V^{-1}} V \xrightarrow{f} W \xrightarrow{F_W} W.$$

is an element of $\mathrm{Hom}_K(V, W)$ as well, and that the above map defines a Frobenius structure on $\mathrm{Hom}(V, W)$. It is called the *internal Hom* of V and W, and usually denoted by $Hom(V, W)$.

5.1.7.3 The F-isocrystal $V^\vee = Hom(V, V(0))$ is the *dual* of V. Show that the internal Hom of two F-isocrystals V, W is

$$Hom(V, W) \simeq W \otimes V^\vee. \tag{5.1.7.1}$$

Show also that there is a canonical isomorphism

$$\mathrm{Hom}(V_K(0), Hom(V, W)) \xrightarrow{\sim} \mathrm{Hom}(V, W) \tag{5.1.7.2}$$

expressing the fact that the elements of $\mathrm{Hom}(V, W)$ are the elements of $Hom(V, W)$ fixed by the Frobenius structure of $Hom(V, W)$.

5.1.7.4 Let K_0 be a local field whose residue field has cardinality q, V_0 a K_0-vector space of finite dimension, and suppose $F_0 : V_0 \to V_0$ is a linear endomorphism of V_0. Let K be the completion of a maximal unramified extension of K_0 and set $V = K \otimes_{K_0} V_0$. Denote by σ the lifting to K of the qth power Frobenius of its residue field, so that $\sigma|K_0$ is the identity. Finally suppose $F : V \to V$ is the extension of scalars

$$F(a \otimes v) = \sigma(a) \otimes F_0(v)$$

of F_0. Show that (V, F) is an F-isocrystal on V whose slopes are the p-adic ordinals of the eigenvalues of F_0 in K_0^{alg} (use proposition 5.1.6.1) (reduce to the case where the eigenvalues of F_0 lie in K_0, and use Jordan normal form.

5.1.7.5 Here is another application of proposition 5.1.6.1. Suppose V, W are F-isocrystals with slopes $\lambda_1, \ldots, \lambda_m$ and $\mu_1, \ldots, \mu_n$ respectively. then:

- the slopes of $V \oplus W$ are $\lambda_1, \ldots, \lambda_m, \mu_1, \ldots, \mu_n$;
- the slopes of $V \otimes W$ are the $\lambda_i + \mu_j$ for all i, j;
- the slopes of $Hom(V, W)$ are the $-\lambda_i + \mu_j$ for all i,
- the slopes of the dual $V^\vee$ are the $-\lambda_i$, and
- the slopes of the exterior power $\wedge^r V$ are the $\lambda_{i_1} + \lambda_{i_2} + \cdots + \lambda_{i_r}$ for all sequences of integers $i_1 < i_2 < \cdots < i_r$. In particular the highest exterior power $\det(V)$ has the single slope $\lambda_1 + \lambda_1 + \cdots + \lambda_n$, where n is the rank of V

(the listing of slopes in the above is not necessarily in order of magnitude). Deduce from these assertions that if k is algebraically closed and λ, $\mu \in \mathbb{Q}$,

$$V_K(\lambda) \otimes V_K(\mu) \simeq V_K(\lambda + \mu)^d$$

and determine d in terms of λ and μ.

5.2 The Fundamental Class

For the rest of this chapter K is a local field with residue field k. As in the last section K^{nr} is the completion of a maximal unramified extension of K. We fix a uniformizer π of K.

5.2.1 Some K^{nr}-algebras. Rings of the form $K^{nr} \otimes_K A$ for some K-algebra A will be so frequent in what follows that we denote this construct by

$$A_K = K^{nr} \otimes_K A \tag{5.2.1.1}$$

which is functorial in A and K^{nr}. Thus when L/K is a Galois extension the Galois group $\mathrm{Gal}(L/K)$ acts on L_K with invariants $K_K \simeq K^{nr}$. The map $\sigma \otimes 1 : L_K \to L_K$ induced by σ will frequently be abbreviated by σ, and its subring of invariants is $(A_K)^\sigma = A$. When L/K is a Galois extension the actions of $\mathrm{Gal}(L/K)$ and σ on L_K commute.

Let L/K be a finite separable extension of K of degree d and residual degree f. Then L_K is a direct sum of f copies of the completion L^{nr} of a maximal unramified extension of L. In fact we can identify L_K with a direct sum of copies of L^{nr} in a canonical way by choosing an embedding $K^{nr} \hookrightarrow L^{nr}$ such that

$$\begin{tikzcd} K^{nr} \arrow[r] \arrow[d] & L^{nr} \arrow[d] \\ K \arrow[r] & L \end{tikzcd} \tag{5.2.1.2}$$

commutes. Then L and K^{nr} are identified with subfields of L^{nr}, and the map

$$L_K \xrightarrow{\sim} (L^{nr})^f \qquad x \otimes y \mapsto (\sigma^{-i}(x)y)_{0 \le i < f} \tag{5.2.1.3}$$

is an isomorphism. In fact if L_0/K is the maximal unramified extension of K in L then $[L_0 : K] = f$ and there is a similar decomposition $K^{nr} \otimes_K L_0 \simeq (K^{nr})^f$, and the natural map $K^{nr} \otimes_{L_0} L \to L^{nr}$ is an isomorphism. With respect to 5.2.1.3 the K^{nr}-vector space structure of L_K is

$$a(x_0, x_1 \ldots, x_{f-1}) = (ax_0, \sigma^{-1}(a)x_1, \ldots, \sigma^{-(f-1)}(a)x_{f-1}) \tag{5.2.1.4}$$

and the natural embedding $L \to L_K$ is

$$a \mapsto (a, a, \ldots, a). \tag{5.2.1.5}$$

Then $\sigma_L|K = \sigma^f$ where σ_L is the lifting of Frobenius to L, and $\sigma : L_K \to L_K$ is

$$(x_0, x_1, \ldots, x_{f-1}) \mapsto (\sigma_L(x_{f-1}), x_0, x_1, \ldots, x_{f-2}) \tag{5.2.1.6}$$

with respect to 5.2.1.3.

It is easily checked that a choice of commutative diagram 5.2.1.2 amounts to a choice of $x \in \mathrm{Spec}(L_K)$ and an identification $\kappa(x) \simeq L^{nr}$: here x is the kernel of the morphism $L_K \to L^{nr}$ canonically determined by 5.2.1.2, and corresponds

to the composition of 5.2.1.3 with the projection onto the $i = 0$ summand; the other projections are this one composed with powers of σ. Finally, it is clear from 5.2.1.3 could be written more naturally as an isomorphism

$$L_K \xrightarrow{\sim} \bigoplus_{0 \le i < f} (\sigma^i)^* L^{nr} \tag{5.2.1.7}$$

of (K^{nr}, L)-bimodules, where the corresponding module structures arise from 5.2.1.2. The identification of the right hand sides of 5.2.1.3 and 5.2.1.7 comes from the identifications

$$L^{nr} \xrightarrow{\sim} (\sigma^i)^* L^{nr} \qquad x \mapsto 1 \otimes x.$$

When L/K is unramified we may identify $K^{nr} \simeq L^{nr}$ canonically, and the diagram 5.2.1.2 identifies L with a subfield of K^{nr}. The arithmetic Frobenius $\sigma_{arith} = 1 \otimes (\sigma|L)$ is a generator of $\mathrm{Gal}(L/K)$ and for the decomposition 5.2.1.3 is given by

$$\sigma_{arith}(a_0, a_1, \ldots, a_{f-1}) = ({}^\sigma a_1, {}^\sigma a_2, \ldots, {}^\sigma a_{f-1}, {}^\sigma a_0). \tag{5.2.1.8}$$

The field norm $N_{L/K} : L^\times \to K^\times$ extends to a homomorphism

$$N_{L/K} : L_K^\times \to (K^{nr})^\times \tag{5.2.1.9}$$

which is the norm for the ring extension $K^{nr} \to L_K$. If $x \in L_K^\times$ corresponds (x_i) under the decomposition 5.2.1.3, $N_{L/K}(a)$ is given by

$$N_{L/K}(x) = \prod_{0 \le i < f} \sigma^i(N_{L^{nr}/K^{nr}}(x_i)). \tag{5.2.1.10}$$

We denote by $w_{L/K} : L_K^\times \to \mathbb{Q}$ the homomorphism

$$w_{L/K}(x) = [L : K]^{-1} v(N_{L/K}(x)) \tag{5.2.1.11}$$

where the numerical factor guarantees that $w_{L/K}$ extends the valuation of $K^\times \subset L_K^\times$. If v_L is the unique valuation of L^{nr} extending those of L and K^{nr},

$$w_{L/K}(x) = \sum_{0 \le i < f} f^{-1} v_L(x_i). \tag{5.2.1.12}$$

5.2.2 "Lubin-Tate" F-isocrystals. If $\alpha \in L_K^\times$,

$$F_\alpha : L_K \to L_K \qquad F_\alpha(x) = \alpha \cdot {}^\sigma x \tag{5.2.2.1}$$

defines a Frobenius structure on L_K, and we denote by $L_K(\alpha)$ the F-isocrystal (L_K, F_α). We denote by $D(\alpha)$ the endomorphism ring of $L_K(\alpha)$; it is a central simple K-algebra of degree d^2, where as before $d = [L : K]$. Since $\sigma \otimes 1$ is L-linear, right multiplication defines an embedding $L \to D(\alpha)$.

5.2.2.1 Proposition *For any finite separable extension L/K and $\alpha \in L_K^\times$, the F-isocrystal $L_K(\alpha)$ is isopentic of slope $w_{L/K}(\alpha)$.*

Proof. The observation 5.1.6.5 shows that it suffices to prove that the dth iterate of $L_K(\alpha)$ has slope $dw_{L/K}(\alpha)$ for any fixed d. We will take $d = [L : K]$. If $\alpha \in L_K^\times$ and $x \in L_K$ decompose as $\alpha = (\alpha_i)$ and $x = (x_i)$ according to 5.2.1.3, the Frobenius structure F_α is

$$F_\alpha(x_i) = (\alpha_0 \cdot {}^{\sigma_L}x_{f-1}, \alpha_1 x_0, \ldots, \alpha_{f-1}x_{f-2})$$

by 5.2.1.6. Iterating f times yields

$$F_\alpha^f(x_i) = (\beta_i \cdot {}^{\sigma_L}x_i)$$

where $\sigma_L = \sigma^f$ as before, and

$$\beta_i = \alpha_0\alpha_1 \cdots \alpha_i \cdot {}^{\sigma_L}(\alpha_{i+1} \cdots \alpha_{f-1})$$

Since σ_L does not change the valuation of an element of L^{nr}, all of the β_i have the same valuation, namely

$$v_L(\beta_i) = \sum_{0 \le j < f} v_L(\alpha_j).$$

Set $e = e_{L/K}$; then $d = ef$ and

$$F^d(x_i) = F^e(\beta_i \cdot {}^{\sigma_L}x_i) = ({}^{1+\sigma_L+\cdots+\sigma_L^{e-1}}\beta_i {}^{\sigma_L^e}x_i)$$

and note that

$$v_L({}^{1+\sigma_L+\cdots+\sigma_L^{e-1}}\beta_i) = ev_L(\beta_i) = ef \sum_{0 \le j < f} \frac{1}{f} v_L(\alpha_j) = dw_{L/K}(\alpha).$$

Let $L_0 \subset L_K$ be the lattice corresponding to $(\mathcal{O}_{L^{nr}})^f \subset (L^{nr})^f$. Since $dw_{L/K}(\alpha) \in \mathbb{Z}$, the last equality says that

$$F^d(L_0) = \pi^{dw_{L/K}(\alpha)} L_0$$

for any uniformizer π of K. Then $F^{nd}(L_0) = \pi^{ndw_{L/K}} L_0$, and proposition 5.1.6.1 shows that (L_K, F_α^d) has slope $dw_{L/K}$, as required. ■

5.2.2.2 The unramified case. Let's consider the case when L/K unramified of degree $d = f$. Pick a $r \in \mathbb{Z}$ that is relatively prime to d and set

$$\alpha = (\pi^r, 1, \ldots, 1) \tag{5.2.2.2}$$

where as above we identify $L_K \simeq (L^{nr})^f = (K^{nr})^d$. By the proposition $L_K(\alpha)$ has slope r/d, and as it has rank d it must be isomorphic to $V_K(r/d)$. In fact this is easy to write down an explicit isomorphism from explicit formula for F_α in the proof of proposition 5.2.2.1.

5.2.2.3 Corollary *If L/K is a Galois extension of degree d, $\mathrm{Br}(L/K)$ is cyclic of order d.*

Proof. Since the $\mathrm{Br}(L/K) \simeq H^2(G, L^\times)$ is annihilated by d it must contained in the cyclic subgroup $(1/d)\mathbb{Z}/\mathbb{Z} \subseteq \mathbb{Q}/\mathbb{Z} \simeq \mathrm{Br}(K)$ of order d. Since this subgroup is the image of $w_{L/K}$, inv_K maps $\mathrm{Br}(L/K)$ onto this subgroup. ■

The *fundamental class* of the extension L/K is the element of $\mathrm{Br}(L/K)$ with invariant $-1/d$, where $d = [L : K]$. We identify this class with the elements of $\mathrm{Ext}(G, L^\times)$ and $H^2(G, L^\times)$ corresponding to it under the isomorphism 4.2.4.2, and in any case it will be denoted by $u_{L/K}$. Our definition here differs from that of most of the classical texts (e.g. [1], [12]) but coincides with that of Tate [14] and Deligne [5]. In particular the reciprocity map to be defined later has the opposite sign to that found in the older texts.

Our next is to give an explicit realization of the extension of G by $L^\times$ represented by $u_{L/K}$, or equivalently an explicit $L^\times$-valued 2-cocycle representing $u_{L/K}$. The division algebra corresponding to $u_{L/K}$ is the endomorphism ring of an isopentic F-isocrystal of rank d and slope $1/d$, so we first need to construction some endomorphisms of $V_K(1/d)$. In fact the same method works for any $V_K(\lambda)$.

5.2.2.4 Lemma *The sequence*

$$1 \to L^\times \to L_K^\times \xrightarrow{\sigma-1} L_K^\times \xrightarrow{w_{L/K}} d^{-1}\mathbb{Z} \to 0$$

is exact.

Proof. The only nonobvious point is that the image of $\sigma - 1$ is kernel of $w_{L/K}$, and it is clearly contained in the kernel. We first observe that the subgroup of $\mathbb{Z}^f$ consisting of (n_i) such that $\sum_i n_i = 0$ is spanned by elements with a 1 in position i, -1 in position $i+1$ (addition modulo f) and zeros elsewhere. From this it follows that any $(x_i) \in L_K^\times$ in the kernel of $w_{L/K}$ is congruent modulo the image of $\sigma - 1$ to a (x_i) such that $v_L(x_i) = 0$ for all x. Since $\sigma^f - 1$ is a retraction of $(L^{nr})^\times$ onto its subgroup of elements of valuation zero, for each i there is a c_i such that $b_i = \sigma^f(c_i)/c_i$. Then $b = \sigma^f(c)/c$ in $L_K^\times$, and since

$$\sigma^f - 1 = (\sigma - 1)(\sigma^{f-1} + \cdots + \sigma + 1)$$

we conclude that b is in the image of $\sigma - 1$. ■

Suppose now L/K is Galois with group G. For any $s \in G$, $w_{L/K}({}^{s-1}\alpha) = 0$ and the lemma shows that there is a $\beta_s \in L_K^\times$ such that

$$^{\sigma-1}\beta_s = {}^{s-1}\alpha \tag{5.2.2.3}$$

well defined up to a factor in $L^\times$. From 5.2.2.3 we see that

$$u_s : L_K \to L_K \qquad u_s(x) = \beta_s \cdot {}^s x \tag{5.2.2.4}$$

commutes with F_α:

$$\begin{aligned} F_\alpha(u_s(x)) &= \alpha \cdot {}^\sigma(\beta_s \cdot {}^s x) \\ &= \alpha \cdot {}^\sigma\beta_s \cdot {}^{\sigma s}x = {}^s\alpha \cdot \beta_s \cdot {}^{s\sigma}x \\ &= \beta_s \cdot {}^s(\alpha \cdot {}^\sigma x) = u_s(F_\alpha(x)). \end{aligned}$$

and is thus an automorphism of $L_K(\alpha)$.

A quick calculation shows that the u_s satisfy the relations

$$u_s u_t = a_{s,t} u_{st}, \quad u_s \ell = {}^s\ell u_s \tag{5.2.2.5}$$

for all $\ell \in L$ and s, $t \in G$, where

$$a_{s,t} = {}^s\beta_t \beta_{st}^{-1} \beta_s. \tag{5.2.2.6}$$

The 5.2.2.5 are the definiing relations for the crossed product algebra defined by the cocycle 5.2.2.6. The correspdonding extension class can be deduced from 5.2.2.6, but it can also be described directly.

5.2.2.5 Theorem *The endomorphism algebra $D_{L/K}(\alpha)$ is isomorphic to the crossed product algebra associated to the 2-cocycle 5.2.2.6 associated to α. The extension corresponding to $D_{L/K}(\alpha)$ is isomorphic to*

$$1 \to L^\times \xrightarrow{i} W(\alpha) \xrightarrow{p} G_{L/K} \to 1$$

where $W(\alpha)$ the set of pairs $(\beta, s) \in L_K^\times \times G$ satisfying

$${}^{\sigma-1}\beta = {}^{s-1}\alpha \tag{5.2.2.7}$$

with the composition law

$$(\beta, s)(\gamma, t) = (\beta \cdot {}^s\gamma, st) \tag{5.2.2.8}$$

and i, p are the evident inclusion and projection.

Proof. Only the second part needs to be explained. In fact if $i : K \to D_{L/K}(\alpha)$ is the canonical injection, the extension group corresponding to $D_{L/K}(\alpha)$ is the set of $u \in D_{L/K}(\alpha)$ satisfying $i \circ s = \mathrm{ad}(u) \circ i$. It is easily checked that these have the form $u = \beta s$ with $\beta \in L_K^\times$ satisfying 5.2.2.7. ■

5.2.2.6 Corollary *For any finite Galois extension L/K of degree d and any $\alpha \in L_K^\times$ such that $w_{L/K}(\alpha) = 1/d$, the 2-cocycle 5.2.2.6 represents the fundamental class of L/K.*

When $w_{L/K}(\alpha) = 1/d$, the extension $W(\alpha)$ representing the fundamental class is called the *Weil group* of L/K and denoted by $W_{L/K}$. Up to isomorphism of extensions it is independent of the choice of α; in fact since $H^1(G, L^\times) = 0$ it is well-defined up to inner automorphisms by elements of $L^\times$ (c.f. the discussion in section 3.1.4).

We note finally that just as the Galois group $\mathrm{Gal}(L/K)$ is (by definition!) an automorphism group, the same is true for $W(\alpha)$: by construction it consists of automorphisms u of $L_K(\alpha)$ satisfying $i \circ s = \mathrm{ad}(u) \circ i$ for some $s \in G$. When $K = \mathbb{Q}_p$, this observation is due to Morava [10].

5.2.2.7 The unramified case again. Suppose L/K is unramified, so that $f = d$ and we identify $K^{nr} \simeq L^{nr}$. The Galois group $G = \mathrm{Gal}(L/K)$ is generated by the "arithmetic Frobenius" $\sigma_{arith} = 1 \otimes (\sigma|L)$ and we identify $G \simeq \mathbb{Z}/d\mathbb{Z}$ by means of the generator σ_{arith}; in the formulas to follow we also identify elements of $\mathbb{Z}/d\mathbb{Z}$ with integers in the range $[0, d)$. Choose $a \in K^\times$ and let $\alpha = (a^{-1}, 1, \ldots, 1)$. Then 5.2.1.8 yields

$$^{\sigma^i_{arith}-1}\alpha = (a, 1, \ldots, 1, \underset{\substack{\uparrow \\ d-i}}{a}{}^{-1}, 1, \ldots, 1)$$

and a $\beta_i \in L_K^\times$ satisfying $^{\sigma-1}\beta_i = {}^{\sigma^i_{arith}-1}\alpha$ is

$$\beta_i = (a^{-1}, a^{-1}, \ldots, \underset{\substack{\uparrow \\ d-i-1}}{a^{-1}}, 1, \ldots, 1). \tag{5.2.2.9}$$

From this it follows easily that

$$\beta_i(\sigma^i_{arith}(\beta_j))\beta_{i+j}^{-1} = \begin{cases} a^{-1} & i+j < d \\ 1 & i+j \geq d \end{cases}.$$

The coboundary of the constant 1-cochain with value a is the constant 2-cocycle with value a. Adding this to the previous cocycle yields the 2-cocycle

$$a_{i,j} = \begin{cases} 1 & i+j < d \\ a & i+j \geq d \end{cases}$$

that we found earler.

A class in $\mathrm{Br}(L/K)$ gives rise, via the isomorphisms

$$\mathrm{Br}(L/K) \simeq H^2(G, L^\times) \simeq \mathrm{Ext}^2_G(\mathbb{Z}, L^\times) \tag{5.2.2.10}$$

to a Yoneda 2-extension of $\mathbb{Z}$ by $L^\times$. We can identify the extension corresponding to the fundamental class:

5.2.2.8 Theorem *Suppose $[L : K] = d$ and write $w = w_{L/K}$. The class of $u_{L/K} \in \mathrm{Br}(L/K)$ is the the class of the extension*

$$0 \to L^\times \to L_K^\times \xrightarrow{\sigma-1} L_K^\times \xrightarrow{dw} \mathbb{Z} \to 0. \tag{5.2.2.11}$$

in $\mathrm{Ext}^2_G(\mathbb{Z}, L^\times)$.

Proof. We know from lemma 5.2.2.4 that the sequence is exact. Recall from section 4.1.2 how we associate a class in $\mathrm{Ext}^2_G(\mathbb{Z}, L^\times)$ to the 2-extension 5.2.2.11: if $P. \to \mathbb{Z}$ is a resolution of $\mathbb{Z}$ by projective $\mathbb{Z}[G]$-modules, there is a morphism of complexes

$$\begin{tikzcd}
\arrow[r] & P_3 \arrow[r, "d_3"] \arrow[d, "f_3"] & P_2 \arrow[r, "d_2"] \arrow[d, "f_2"] & P_1 \arrow[r, "d_1"] \arrow[d, "f_1"] & P_0 \arrow[r, "d_0"] \arrow[d, "f_0"] & \mathbb{Z} \arrow[r] \arrow[d, equal] & 0 \\
\arrow[r] & 1 \arrow[r] & L^\times \arrow[r] & L_K^\times \arrow[r, "\sigma-1"] & L_K^\times \arrow[r, "dw"] & \mathbb{Z} \arrow[r] & 0
\end{tikzcd} \tag{5.2.2.12}$$

unique up to homotopy. The map f_2 lies in the kernel of $\mathrm{Hom}(P_2, L^\times) \to \mathrm{Hom}(P_3, L^\times)$, and its image in $H^2(G, L^\times)$ is the class of 5.2.2.11. For $P_\cdot$ we take the bar complex and recall that

$$d_0([\ ]) = 1, \qquad d_1([s]) = s[\ ] - [\ ], \qquad d_2([s|t]) = s[t] - [st] + [s].$$

If we set

$$f_0([\ ]) = \alpha, \qquad f_1([s]) = \beta_s, \qquad f_2([s|t]) = a_{s,t}$$

the commutativity of 5.2.2.12 shows that

$$dw(\alpha) = 1, \qquad {}^{\sigma-1}\beta_s = {}^{s-1}\alpha, \qquad a_{s,t} = {}^{s}\beta_t \beta_{st}^{-1} \beta_s.$$

The first equality shows that $D_{L/K}(\alpha)$ represents the fundamental class $u_{L/K}$, and the others show that $(a_{s,t})$ represents $D_{L/K}(\alpha)$ in $H^2(G, L^\times)$. Since the class of 5.2.2.11 is $(a_{s,t})$ we are done. ■

5.3 The Reciprocity Isomorphism

5.3.1 The inverse reciprocity map. The next proposition and its corollary are essentially exercise 2 of [12, Ch. XIII §5]:

5.3.1.1 Proposition *The G-module $L_K^\times$ is cohomologically trivial.*

Proof. We first observe that the G-module $L_K^\times$ is induced from the I-module $(L^{nr})^\times$, where $I \subset G$ is the inertia subgroup. Replacing L/K and G by L^{nr}/K^{nr} and I respectively, we are reduced to showing that if L/K is totally ramified and the residue field of K is algebraically closed, $L^\times$ is a cohomologically trivial G-module. This is theorem 3.4.2.4. ■

5.3.1.2 Corollary *For all $r \in \mathbb{Z}$, the map*

$$\hat{H}^r(G, \mathbb{Z}) \xrightarrow{u_{L/K}\cup} \hat{H}^{r+2}(G, L^\times) \tag{5.3.1.1}$$

is an isomorphism.

Proof. Split the extension 5.2.2.11 into the short exact sequences

$$1 \to L^\times \to L_K^\times \to U \to 1$$
$$1 \to U \to L_K^\times \to \mathbb{Z} \to 0$$

and denote by

$$u_1 \in \mathrm{Ext}^1_G(U, L^\times),\ u_2 \in \mathrm{Ext}^1(\mathbb{Z}, U)$$

the corresponding extension classes; then $u_{L/K} \in \mathrm{Ext}^2_G(\mathbb{Z}, L^\times)$ is the product $u_1 \cdot u_2$ for the composition

$$\mathrm{Ext}^1_G(U, L^\times) \times \mathrm{Ext}^1_G(\mathbb{Z}, U) \to \mathrm{Ext}^1_G(\mathbb{Z}, L^\times).$$

On the other hand the cup products with u_1 and u_2 are the connecting homomorphisms for the corresponding exact sequences, which by the proposition are isomorphisms on Tate cohomology . ■

5.3.2 The norm residue symbol. We denote by

$$\eta_{L/K} : G^{ab} \to K^\times / N_{L/K}(L^\times) \tag{5.3.2.1}$$

the isomorphism 5.3.1.1 for $r = -2$; we will also use this to denote the induced homomorphism

$$\eta_{L/K} : G \to K^\times / N_{L/K}(L^\times).$$

The *reciprocity map*

$$\theta_{L/K} = \eta_{L/K}^{-1} : K^\times / N_{L/K}(L^\times) \to G^{ab} \tag{5.3.2.2}$$

is the inverse of $\eta_{L/K}$. We will also write $\theta_{L/K}$ for the composite

$$K^\times \to K^\times / N_{L/K} L^\times \to G^{ab}.$$

The traditional notation for $\theta_{L/K}$ notation, which is

$$(a, L/K) = \theta_{L/K}(a) \tag{5.3.2.3}$$

where a is indifferently an element of $K^\times$ or $K^\times / N_{L/K} L^\times$. The left hand side of 5.3.2.3 is also known as the *norm residue symbol* or the *Artin symbol*.

5.3.2.1 Theorem *Suppose L/K is a Galois extension of local fields with group G and set $d = [L : K]$. Let α be an element of $L_K^\times$ such that $w_{L/K}(\alpha) = 1/d$, and let $s \in G$. If $\beta \in L_K^\times$ satisfies*

$${}^{\sigma-1}\beta = {}^{s-1}\alpha$$

then

$$\eta_{L/K}(s) = N_{L/K}(\beta) \mod N_{L/K} L^\times. \tag{5.3.2.4}$$

Proof. It suffices to recall the formulas for the isomorphism $H^{-2}(G, \mathbb{Z}) \simeq G^{ab}$ and the procedure for computing the cup product with $u_{L/K}$. The first identifies the image $\bar{s}$ of $s \in G$ in G^{ab} with the class of

$$[s] \otimes_G 1 \in \check{B}_1 \otimes_G \mathbb{Z} = C_1(G, \mathbb{Z}) = Z_1(G, \mathbb{Z})$$

in $H_1(G, \mathbb{Z}) = H^{-2}(G, \mathbb{Z})$. As in 3.3.2.8 we identify $B^*_{-n-1} \simeq B_n$; then the homomorphism $f : B_{-2} \to \mathbb{Z}$ representing $\bar{s}$ is

$$f : B_1 \to \mathbb{Z} \qquad f([u]) = \begin{cases} 1 & u = s \\ 0 & u \neq s \end{cases}.$$

This vanishes on dB_0 and we denote by $\bar{f} : B_1/dB_0 \to \mathbb{Z}$ the induced map. Then $\bar{f}$ extends to a morphism of complexes

$$\begin{tikzcd}
B_1 \arrow[r] \arrow[d] & B_0 \arrow[r, "d_{-1}"] \arrow[d, "f_2"] & B_0 \arrow[r, "d_{-2}"] \arrow[d, "f_1"] & B_1 \arrow[r] \arrow[d, "f_0"] & B_1/dB_0 \arrow[r] \arrow[d, "\bar{f}"] & 0 \\
0 \arrow[r] & L^\times \arrow[r] & L_K^\times \arrow[r, "\sigma-1"] & L_K^\times \arrow[r, "dw_{L/K}"] & \mathbb{Z} \arrow[r] & 0
\end{tikzcd}$$

and f_0 can be any map making the rightmost square commutative. We choose

$$a_u = f_0([u]) = \begin{cases} \alpha & u = s \\ 1 & u \neq s \end{cases}$$

where α is any element of $L_K^\times$ such that $dw_{L/K}(\alpha) = 1$. If we set $\beta = f_1([\ ])$ and $c = f_2([\ ])$ and use the formulas

$$d_{-1}([\ ]) = \sum_{s \in G} s[\ ], \quad d_{-2}([\ ]) = \sum_{s \in G} (s-1)[s]$$

from 3.3.2.9 and 3.3.2.10 we find

$${}^{\sigma-1}\beta = {}^{s-1}\alpha, \quad c = N_G(\beta) = N_{L/K}(\beta).$$

Finally $u_{L/K} \cup \bar{s}$ is the image in $K^\times / N_{L/K} L^\times$ of $c = f_2([\ ])$, which completes the proof. ■

5.3.2.2 Corollary *If L/K is unramified and π is a uniformizer of K,*

$$\eta_{L/K}(\sigma_{arith}) = \pi^{-1} \mod N_{L/K} L^\times. \tag{5.3.2.5}$$

Proof. To compute $\eta_{L/K}(\sigma_{arith})$ we can use

$$\beta = (\pi^{-1}, 1, \ldots, 1)$$

as in 5.2.2.9, and then $N_{L/K}(\beta) = \pi^{-1}$. ■

In more traditional notation, this is

$$(\pi, L/K) = \sigma_{arith}^{-1} \tag{5.3.2.6}$$

when L/K is unramified. As we remarked before, the traditional normalization of the norm residue symbol would have σ_{arith} on the right hand side.

When L/K is totally ramified we may identify $L_K = L^{nr}$ and take $\alpha = \pi^{-1}$ for any uniformizer π of L^{nr}; in this case 5.3.2.4 is equivalent to the formula proven by Dwork [7]. The general formula can be deduced from a series of exercises in [12, Ch. XIII §5].

5.3.3 Successive extensions. In order to find the behavior of the norm residue symbol with respect to field automorphisms and successive extensions we need to extend the formalism developed in section 5.2.1. In the next few sections we fix a finite Galois extension E/K with group $G_{E/K}$ and a subfield L of G containing K. The Galois group of E/L will be denoted by $G_{E/L}$, and if L/K is Galois its group is $G_{L/K}$.

The transitivity isomorphism $K^{nr} \otimes_K E \simeq (K^{nr} \otimes_K L) \otimes_L E$ may be written

$$E_K \simeq L_K \otimes_L E. \tag{5.3.3.1}$$

This shows that E_K has a canonical structure of a free L_K-module, and we denote by

$$N^K_{E/L} : E^\times_K \to L^\times_K \tag{5.3.3.2}$$

the norm map. When $E/L/K$ is $L/K/K$ this is the norm map 5.2.1.9 introduced earlier. The norm $N^K_{E/L}$ is equivariant for the action of σ on E_K and L_K. If E/K is Galois with group $G_{E/K}$, it is also equivariant for the action of $G_{E/K}$ in the sense that

$$\begin{tikzcd} E^\times_K \arrow[r, "N^K_{E/L}"] \arrow[d, "s"'] & L^\times_K \arrow[d, "s"] \\ E^\times_K \arrow[r, "N^K_{E/s(L)}"'] & s(L)^\times_K \end{tikzcd} \tag{5.3.3.3}$$

commutes for any $s \in G_{E/K}$. Finally, for a 3-fold extension $F/E/L/K$ the norm is transitive:

$$N^K_{E/L} \circ N^K_{F/E} = N^K_{F/L}. \tag{5.3.3.4}$$

Applying this in the case $E/L/K/K$ and invoking 5.2.1.11, we find that

$$w_{L/K}(N_{E/L}(\beta)) = [E : L] w_{E/K}(\beta) \tag{5.3.3.5}$$

for $\beta \in E_K$.

The decomposition 5.2.1.3 extends in an obvious way to a decomposition of E_K as an E_L-module. As before we fix a completion L^{nr} of a maximal unramified extension of L and a morphism $K^{nr} \to L^{nr}$ making 5.2.1.2 commutative. Tensoring the isomorphism of L with E yields a direct sum decomposition

$$E_K \simeq L_K \otimes_L E \simeq \bigoplus_{0 \le i < f} (\sigma^i)^* L^{nr} \otimes_L E \simeq \bigoplus_{0 \le i < f} (\sigma^i)^* E_L \tag{5.3.3.6}$$

of $K^{nr} \otimes_K E$-bimodules. This direct sum decomposition is, like 5.2.1.7 canonically determined by a choice of diagram 5.2.1.2. The isomorphism 5.3.3.6 is equivariant for the action of $G_{E/L}$ on both sides.

For any 3-fold extension $F/E/L/K$ of local fields the norms $N^K_{F/E}$ and $N^L_{F/E}$ are related as follows: if

$$F_K \simeq \bigoplus_{0 \le i < f} (\sigma^i)^* F_L \qquad E_K \simeq \bigoplus_{0 \le i < f} (\sigma^i)^* E_L$$

are the decompositions 5.3.3.6 for F and E and

$$\gamma = (\gamma_0, \gamma_1, \dots \gamma_{f-1}) \in F_K \simeq \bigoplus_{0 \le i < f} (\sigma^i)^* F_L$$

then

$$N^K_{F/E}(\gamma) = (N^L_{F/E}(\gamma_0), N^L_{F/E}(\gamma_1), \dots, N^L_{F/E}(\gamma_{f-1}) \tag{5.3.3.7}$$

for the above decomposition of E_K. This can be seen by fixing a basis of F as an E-vector space and using the fact that determinants relative to a direct sum of rings respect the direct sum decomposition.

Recall that for the decomposition 5.2.1.3 of L_K the action of σ is given by 5.2.1.6 where σ_L is the Frobenius of L^{nr} with respect to its own residue field. It follows that the action of σ as $\sigma \otimes 1$ on $E_K = K^{nr} \otimes_K E$ is then given by

$$(\beta_0, \beta_1, \ldots, \beta_{f-1}) \mapsto (\sigma_L(\beta_{f-1}), \beta_0, \beta_1, \ldots, \beta_{f-2}) \tag{5.3.3.8}$$

for the decomposition 5.3.3.6, where now σ_L denotes the extension of σ_L acting on L^{nr} to $\sigma_L \otimes 1$ acting on E_L.

We now define homomorphisms

$$\iota^E_{L/K},\ \delta^E_{L/K} : E_L^\times \to E_K^\times$$

by

$$\begin{aligned} \iota^E_{L/K}(\alpha) &= (\alpha, 1, \ldots, 1) \\ \delta^E_{L/K}(\beta) &= (\beta, \beta, \ldots, \beta) \end{aligned} \tag{5.3.3.9}$$

with respect to the decomposition 5.3.3.6. Since the decomposition 5.3.3.6 is equivariant for the action $G_{E/L}$, so are $\iota^E_{L/K}$ and $\delta^E_{L/K}$. Corresponding to the formula 5.3.3.5 we have, for $\alpha \in E_L^\times$,

$$w_{E/K}(\iota^E_{L/K}(\alpha) = \frac{1}{[L:K]} w_{L/K}(\alpha). \tag{5.3.3.10}$$

For any 3-fold extension $F/E/L/K$ the maps ι and δ are compatible with the norms. In fact 5.3.3.7 implies that the diagrams

$$\begin{tikzcd} F_L^\times \arrow[r, "\delta^F_{L/K}"] \arrow[d, "N^L_{F/E}"'] & F_K^\times \arrow[d, "N^K_{F/E}"] \\ E_L^\times \arrow[r, "\delta^E_{L/K}"'] & E_K^\times \end{tikzcd} \qquad \begin{tikzcd} F_L^\times \arrow[r, "\iota^F_{L/K}"] \arrow[d, "N^L_{F/E}"'] & F_K^\times \arrow[d, "N^K_{F/E}"] \\ E_L^\times \arrow[r, "\iota^E_{L/K}"'] & E_K^\times \end{tikzcd} \tag{5.3.3.11}$$

are commutative.

We need one more fact about these maps. The composite

$$L_L^\times \xrightarrow{\delta^L_{L/K}} L_K^\times \xrightarrow{N^K_{L/K}} K_K^\times$$

is a homomorphism $(L^{nr})^\times \to (K^{nr})^\times$. It is not the usual norm map, however:

5.3.3.1 Lemma *For $\ell \in L^\times \subset (L^{nr})^\times$,*

$$N^K_{L/K}(\delta^L_{L/K}(\ell)) = N_{L/K}(\ell) \tag{5.3.3.12}$$

where the norm on the right is the field norm for L/K.

Proof. Since $N^K_{L/K}$ is the map 5.2.1.9, the equality 5.2.1.10 shows that

$$N^K_{L/K}(\delta^L_{L/K}(\ell)) = \prod_{0\le i<f} \sigma^i(N_{L^{nr}/K^{nr}}(\ell)).$$

As before let L_0 be the maximal unramified extension of K in L, and identify it with a subfield of K^{nr}. Since $L^{nr} \simeq L \otimes_{L_0} K^{nr}$, $N_{L^{nr}/K^{nr}}(\ell) = N_{L/L_0}(\ell)$ and the product on the right hand side is

$$\prod_{0\le i<f} \sigma^i(N_{L/L_0}(\ell)) = N_{L_0/K}(N_{L/L_0}(\ell)) = N_{L/K}(\ell)$$

since $\sigma|L_0$ generates the Galois group of L_0/K. ■

5.3.4 Functorial properties. We can now express the behavior of the norm residue symbol with respect to field automorphisms and successive extensions, starting with the latter. In the above situation we suppose that L/K is Galois, and denote by

$$\pi^K_{E/L} : G_{E/K} \to G_{L/K}$$

the canonical homomorphism. To calculate $\eta_{E/K}$ we choose $\alpha \in E^\times_K$ such that $w_{E/K}(\alpha) = 1/[E:K]$: if $s \in G_{E/K}$ we pick $\beta \in E^\times_K$ such that ${}^{\sigma-1}\beta_s = {}^{s-1}\alpha$; then $\eta_{E/K}(s) = N_{L/K}(\beta_s)$ (note that $N_{L/K} = N^K_{L/K}$ here). On the other hand 5.3.3.5 says that

$$w_{L/K}(N^K_{E/L}(\alpha)) = \frac{[E:L]}{[E:K]} = \frac{1}{[L:K]}$$

and we may use $N_{E/L}(\alpha)$ to calculate $\eta_{L/K}$. By equivariance

$${}^{\sigma-1}N_{E/L}(\beta) = {}^{s-1}N_{E/L}(\alpha) \tag{5.3.4.1}$$

so from 5.3.3.4 and 5.3.2.4 we get

$$\eta_{E/K}(s) = \eta_{L/K}(\pi^K_{E/L}(s)) \mod N_{L/K}L^\times \tag{5.3.4.2}$$

or equivalently that

$$\begin{array}{ccc} G_{E/K} & \xrightarrow{\pi^K_{E/L}} & G_{L/K} \\ \downarrow{\scriptstyle \eta_{E/K}} & & \downarrow{\scriptstyle \eta_{L/K}} \\ K^\times/N_{E/K}E^\times & \longrightarrow & K^\times/N_{L/K}L^\times \end{array} \tag{5.3.4.3}$$

where the bottom arrow is the natural map. In the more traditional notation 5.3.2.3 this says that

$$\pi^K_{E/L}(a, E/K) = (a, L/K) \tag{5.3.4.4}$$

or in other words the norm residue symbol is compatible with passage to a larger Galois extension of K.

We next allow L to be any intermediate extension and take $s \in G_{E/L}$. To compute $\eta_{E/L}(s)$ we choose $\alpha \in E_L^\times$ such that $w_{E/L}(\alpha) = [E:L]^{-1}$ and $\beta \in E_L^\times$ such that ${}^{\sigma_L - 1}\beta = {}^{s-1}\alpha$; then $\eta_{E/L}(s)$ is the class of $N_{E/L}(\beta)$ in $L^\times/N_{E/L}E^\times$ (recall here that $N_{E/L}$ here is $N^L_{E/L}$). On the other hand by 5.3.3.10 we have $w_{E/K}(\iota^E_{L/K}(\alpha)) = 1/[E:K]$, so we can use $\iota^E_{L/K}(\alpha)$ to compute $\eta_{E/K}(s)$. The formula 5.2.1.6 for the action of σ on L_K shows that

$$ {}^{\sigma-1}\delta^K_{E/L}(\beta) = ({}^{\sigma_L-1}\beta, 1, \ldots, 1) = ({}^{s-1}\alpha, 1, \ldots, 1) = {}^{s-1}\iota^K_{E/L}(\alpha) $$

and thus

$$ \eta_{E/K}(s) = N^K_{E/K}(\delta^E_{L/K}(\beta)) \mod N_{E/K}E^\times. $$

To evaluate the right hand side we consider the diagram

$$ \begin{tikzcd} E_L^\times \arrow[r, "\delta^E_{L/K}"] \arrow[d, "N^L_{E/L}"'] & E_K^\times \arrow[d, "N^K_{E/L}"'] \arrow[dr, bend left, "N^K_{E/K}"] & \\ L_L^\times \arrow[r, "\delta^L_{L/K}"'] & L_K^\times \arrow[r, "N^K_{L/K}"'] & K_K^\times \end{tikzcd} $$

in which the square is the case $E/L/L/K$ of the commutative square on the left of 5.3.3.11, and the right hand triangle commutes by the transitivity of norms. From this we see that

$$ N^K_{E/K}(\delta^K_{E/L}(\beta)) = N^K_{L/K}(\delta^L_{L/K}(N^L_{E/L}(\beta))) = N^K_{L/K}(\delta^L_{L/K}(\eta_{E/L}(s))). $$

Since $N_{E/L}(\beta_L) \in L^\times$, lemma 5.3.3.1 shows that

$$ N^K_{L/K}(\delta^L_{L/K}(\eta_{E/L}(s))) = N_{L/K}(\eta_{E/L}(s)) $$

and combining the previous equalities yields

$$ \eta_{E/K}(s) = N_{L/K}(\eta_{E/L}(s)) \mod N_{E/K}E^\times. \tag{5.3.4.5} $$

In other words

$$ \begin{tikzcd} G_{E/L} \arrow[r, "i"] \arrow[d, "\eta_{E/L}"'] & G_{E/K} \arrow[d, "\eta_{E/K}"] \\ L^\times/N_{E/L}E^\times \arrow[r, "N_{L/K}"'] & K^\times/N_{E/K}E^\times \end{tikzcd} \tag{5.3.4.6} $$

commutes; in terms of the norm residue symbol this is

$$ (a, E/L) = (N_{L/K}(a), E/K) \tag{5.3.4.7} $$

for $a \in L^\times$.

Again with s, $t \in G_{E/K}$ and ${}^{\sigma-1}\beta_s = {}^{s-1}\alpha$, the equality

$$ {}^{\sigma-1}({}^t\beta_s) = {}^t({}^{\sigma-1}\beta_s) = {}^{ts-t}\alpha = {}^{tst^{-1}-1}({}^t\alpha) $$

implies that

$$ \eta_{E/t(L)}(tst^{-1})) = {}^t\eta_{E/L}(s) \tag{5.3.4.8} $$

modulo appropriate subgroups, i.e.

$$ \begin{tikzcd} G_{E/L} \arrow[r, "\mathrm{ad}(t)"] \arrow[d, "\eta_{L/K}"'] & G_{E/t(L)} \arrow[d, "\eta_{L^t/K}"] \\ L^\times/N_{E/L}L^\times \arrow[r] & K^\times/N_{E/t(L)}(t(L))^\times \end{tikzcd} \tag{5.3.4.9} $$

commutes, where $\mathrm{ad}(t) : G_{E/L} \to G_{E/t(L)} = tG_{E/L}t^{-1}$ is $s \mapsto tst^{-1}$. The corresponding formula for the norm residue symbol is

$$ s(a, E/L)s^{-1} = (s(a), E/s(L)) \tag{5.3.4.10} $$

for $s \in G_{E/K}$ and $a \in L$.

The last compatibility asserts that the transfer $\mathrm{Ver} : G^{ab}_{E/K} \to G^{ab}_{L/K}$ corresponds via the norm residue symbol to the map $K^\times/N_{E/K}E^\times \to L^\times/N_{E/L}E^\times$ induced by the inclusion. From our point of view this is best understood in terms of the ideas of the next section (proposition 5.4.1.4).

5.4 Weil Groups

The Weil groups have a formalism relative to successive extensions similar to that of the Galois groups. This formalism is related to and in fact re-expresses the functorial properties of the norm residue symbol that were worked out in the last section.

5.4.1 The formalism of Weil groups. We fix a Galois extension E/K with group $G_{E/K}$ and let L be an extension of K in E (not necessarily Galois over K). As before $G_{E/L}$ is the Galois group of E/L, and similarly for $G_{L/K}$ when L/K is Galois. Our aim in this section is to define morphisms $i : W_{E/L} \to W_{E/K}$ and, when L/K is Galois, $\pi_{E/L} : W_{E/K} \to W_{L/K}$. Since $W_{L/K}$ by definition is only defined up to inner automorphisms it will be necessary to "rigidify" it by a particular choice of "realization" $W(\alpha)$, which as before is the set of pairs $(\beta, s) \in L^\times_K \times G_{L/K}$ satisfying 5.2.2.7 with the composition law 5.2.2.8. To indicate the fields involved we write $W_{L/K}(\alpha)$ for $W(\alpha)$, so a homomorphism such as $\pi_{E/L} : W_{E/K} \to W_{L/K}$ should be understood as a homomorphism $W_{E/K}(\alpha') \to W_{L/K}(\alpha)$ for particular choices (usually implicit) of α, α' appropriate to L/K and E/K.

In fact everything we need is contained in the formulas 5.3.4.1 and 5.3.4.5. The first of them shows that $N_{E/L} : E_K^\times \to E_L^\times$ extends to a homomorphism

$$\begin{aligned} \pi_{E/L} : W_{E/K}(\alpha) &\to W_{L/K}(N_{E/L}(\alpha)) \\ \pi_{E/L}(\beta, s) &= (N_{E/L}(\beta), \pi_{L/K}(s)) \end{aligned} \tag{5.4.1.1}$$

making commutative the diagram

$$\begin{tikzcd} 1 \arrow[r] & E^\times \arrow[r] \arrow[d, "N_{E/L}"] & W_{E/K} \arrow[r] \arrow[d, "\pi_{E/L}"] & G_{E/K} \arrow[r] \arrow[d, "\pi_{E/L}"] & 1 \\ 1 \arrow[r] & L^\times \arrow[r] & W_{L/K} \arrow[r] & G_{L/K} \arrow[r] & 1 \end{tikzcd} . \tag{5.4.1.2}$$

The transitivity of the norm shows that the maps π just constructed are transitive:

$$\pi_{E/L}^K \circ \pi_{F/E}^K = \pi_{F/L}^K \tag{5.4.1.3}$$

for a 3-fold extension $F/E/L/K$; here of course the groups $W_{F/K}$, $W_{E/K}$ and $W_{L/K}$ are realized as $W_{F/K}(\alpha)$, $W_{E/K}(N_{F/L}(\alpha)$ and $W_{L/K}(N_{F/L}(\alpha)$ for appropriate α; from now on we will not be explicit about this.

In the special case when $E/L/K$ is $L/K/K$, we have $W_{K/K} = K^\times$, and the definition of $\pi_{L/K}^K$ shows that the diagram

$$\begin{tikzcd} W_{L/K} \arrow[r] \arrow[d, "\pi_{L/K}^K"'] & G_{L/K} \arrow[d, "\eta_{L/K}"] \\ K^\times \arrow[r] & K/N_{L/K}L^\times \end{tikzcd} \tag{5.4.1.4}$$

commutes, where the horizontal maps are the natural projections. In fact if $\alpha \in L_K^\times$ is used to define $W_{L/K}$, $(\beta, s) \in W_{L/K}$ implies that ${}^{\sigma-1}\beta = {}^{s-1}\alpha$, so that

$$(\pi_{L/K}(\beta, s) \mod N_{L/K}L^\times) = (N_{L/K}(\beta) \mod N_{L/K}L^\times) = \eta_{L/K}(s).$$

That 5.4.1.4 is commutative could be expressed by saying that $\pi_{L/K} : W_{L/K} \to K^\times$ is a lifting of the inverse reciprocity map. It could also be rephrased as saying that the diagram

$$\begin{tikzcd} W_{L/K}^{ab} \arrow[r, "\pi_{L/K}^{ab}"] \arrow[dr] & K^\times \arrow[d, "\theta_{L/K}"] \\ & G_{L/K}^{ab} \end{tikzcd} \tag{5.4.1.5}$$

is commutative.

Now 5.3.4.5 shows that $\delta_{E/L} : L_K^\times \to E_K^\times$ extends to a homomorphism

$$\begin{aligned} i_{E/L}^K : W_{L/K}(\alpha) &\to W_{E/K}(\iota_{E/L}(\alpha)) \\ i_{E/L}^K(\beta, s) &= (\delta_{E/K}(\beta), s) \end{aligned} \tag{5.4.1.6}$$

making commutative a diagram

$$\begin{tikzcd} 1 \arrow[r] & L^\times \arrow[r] \arrow[d] & W_{L/K} \arrow[r] \arrow[d, "i_{E/L}^K"] & G_{L/K} \arrow[r] \arrow[d] & 1 \\ 1 \arrow[r] & E^\times \arrow[r] & W_{E/K} \arrow[r] & G_{E/K} \arrow[r] & 1 \end{tikzcd} \tag{5.4.1.7}$$

where the extreme vertical arrows are the canonical inclusions. For a 3-fold extension $F/E/L/K$ we have

$$\delta_{F/E}^K \circ \delta_{E/L}^K = \delta_{F/L}^K \tag{5.4.1.8}$$

which shows that the i are transitive:

$$i_{F/E}^K \circ i_{E/L}^K = i_{F/L}^K. \tag{5.4.1.9}$$

Finally the right hand diagram of 5.3.3.11 implies that for any 3-fold extension $F/E/L/K$ the diagram

$$\begin{tikzcd} W_{F/L} \arrow[r, "\pi_{F/E}^K"] \arrow[d, "i_{L/K}^K"'] & W_{E/L} \arrow[d, "i_{L/K}^K"] \\ W_{F/K} \arrow[r, "\pi_{F/E}^K"'] & W_{E/K} \end{tikzcd} \tag{5.4.1.10}$$

is commutative. This can be expressed by saying that if we use the maps $i_{E/L}$ to identify $W_{E/L}$ with a subgroup of $W_{E/K}$, then these identifications are compatible with the canonical projection maps π (assuming as always that compatible choices of α are made in each place).

It is evident from the construction that $i_{E/L}^K : W_{E/L} \to W_{E/K}$ is injective. It is also true that $\pi_{E/L}^K : W_{E/K} \to W_{E/L}$ is surjective, but this is not so obvious.

5.4.1.1 Proposition *The connecting homomorphism $\partial : G_{E/L} \to L^\times/NE^\times$ arising from the diagram 5.4.1.2 is the inverse norm residue homomorphism $\eta_{E/L}$.*

Proof. For $s \in G_{E/L}$, $\partial(s)$ is computed as follows: lift s to an element $(\beta, s) \in W_{E/K}$; then $\pi_{E/L}(\beta, s) \in W_{L/K}$ lies in $L^\times \subset W_{L/K}$ and $\partial(s)$ is the image of $\pi_{E/L}(\beta, s)$ in $L^\times/N_{E/L}E^\times$. The commutative diagram 5.4.1.10 applied to

$E/L/L/K$ is

$$\begin{tikzcd} W_{E/L} \arrow[r, "\pi_{E/L}"] \arrow[d, "i_{L/K}"'] & W_{L/L} \arrow[d, "i_{L/K}"] \\ W_{E/K} \arrow[r, "\pi_{E/L}"'] & W_{L/K} \end{tikzcd}$$

which shows that $\partial(s)$ can also be computed by lifting s to $(\beta, s) \in W_{E/L}$, and then $\partial(s)$ is the class of $\pi_{E/L}(\beta, s) \in W_{L/L} = L^\times$ in $L^\times/N_{E/L}E^\times$. Now $\pi_{E/L}(\beta, s) = N_{E/L}(\beta)$ where $N_{E/L}$ is the norm $E_L^\times \to (L^{nr})^\times$, and if $\alpha \in E_L^\times$ is used to define $W_{E/L}$, β satisfies ${}^{\sigma-1}\beta = {}^{s-1}\alpha$, so $\partial(s) = \eta_{E/L}(s)$ by Dwork's formula. ■

5.4.1.2 Corollary *For any successive extension $E/L/K$ of local fields with E/K and L/K Galois, the homomorphism $\pi^K_{E/L} : W_{E/K} \to W_{L/K}$ is surjective.*

Proof. Since $\partial = \eta_{E/L}$ is surjective, this follows from the snake lemma. ■

5.4.1.3 Lemma *For any Galois extension of local fields the transfer* Ver : $W^{ab}_{L/K} \to L^\times$ *is the composite*

$$W^{ab}_{L/K} \xrightarrow{\pi^{ab}_{L/K}} K^\times \to L^\times$$

where we identify $W_{K/K} \simeq K^\times$, and the second map is the inclusion.

Proof. Recall the definition of the transfor $G^{ab} \to H^{ab}$ for a subgroup $H \subseteq G$ of finite index: choose a section $\theta : H \setminus G \to G$ of the projection $G \to H \setminus G$, and for s, $t \in G$ define $x_{s,t} \in H$ by $\theta(Ht)s = x_{t,s}\theta(Hts)$; then

$$\mathrm{Ver}(s) = \prod_{t \in H \setminus G} x_{t,s}$$

where the product is in H^{ab}. In our case $G = W_{L/K}$ and we identify $H = L^\times$ with its abelianization. For $t \in G_{L/K} = G/H$ we take $\theta(t) = (\beta_t, t)$ for some appropriate $\beta_t \in L_K^\times$; then

$$\theta(t)(\beta, s) = (\beta_t, t)(\beta, s) = (\beta_t \cdot {}^t\beta, ts) = (\beta_t {}^t\beta\beta_{ts}^{-1}, 1)\theta(ts)$$

where the last equality is justified since $\beta_t {}^t\beta\beta_{ts}^{-1} \in L^\times$. For this θ then we have $x_{t,s} = ({}^s\beta, 1)$, and then

$$\mathrm{Ver}(\beta, s) = \prod_{t \in G_{L/K}} (\beta_t {}^t\beta\beta_{ts}^{-1}, 1) = (N_{L/K}(\beta), 1)$$

which proves the assertion. ■

We can now prove the last compatibility for the norm residue symbol.

5.4.1.4 Proposition *For any 2-fold extension $E/L/K$ of local fields with E/K Galois,*

$$\begin{tikzcd} K^\times \arrow[r] \arrow[d, "\theta_{E/K}"'] & L^\times \arrow[d, "\theta_{E/L}"] \\ G^{ab}_{E/K} \arrow[r, "\mathrm{Ver}"] & G^{ab}_{E/L} \end{tikzcd} \tag{5.4.1.11}$$

is commutative, where the upper horizontal map is the inclusion.

Proof. In view of the diagram 5.4.1.5 applied to E/K and E/L, and since for any Galois extension L/K the projection $\pi_{E/K} : W_{E/K} \to K^\times$ is surjective, it suffices to show that the diagrams

$$\begin{tikzcd} W^{ab}_{E/K} \arrow[r, "\mathrm{Ver}"] \arrow[d] & W^{ab}_{E/L} \arrow[d] \\ G^{ab}_{E/K} \arrow[r, "\mathrm{Ver}"'] & G^{ab}_{E/L} \end{tikzcd} \qquad \begin{tikzcd} W^{ab}_{E/K} \arrow[r, "\mathrm{Ver}"] \arrow[d, "\pi^{ab}_{E/K}"'] & W^{ab}_{E/L} \arrow[d, "\pi^{ab}_{E/L}"] \\ K^\times \arrow[r, "incl"'] & L^\times \end{tikzcd} \tag{5.4.1.12}$$

are commutative. The first just expresses the functoriality of the transfer. The second can be embedded in the diagram

$$\begin{tikzcd} W^{ab}_{E/K} \arrow[r, "\mathrm{Ver}"] \arrow[d, "\pi^{ab}_{E/K}"'] & W^{ab}_{E/L} \arrow[d, "\pi^{ab}_{E/L}"] \arrow[ddr, bend left, "\mathrm{Ver}"] & \\ K^\times \arrow[r] \arrow[drr, bend right, "i"'] & L^\times \arrow[dr, "j"'] & \\ & & E^\times \end{tikzcd}$$

in which i and j are the inclusions. By lemma 5.4.1.3 $i \circ \pi^{ab}_{E/K}$ and $j \circ \pi^{ab}_{E/L}$ are the transfer homomorphisms for the subgroups $E^\times \subset W_{E/K}$ and $E^\times \subset W_{E/L}$ respectively. Since the transfer is transitive for chains of subgroups, the outside square in this diagram is commutative, and since $L^\times \to E^\times$ is injective, the inside square is as well. ■

In terms of the norm residue symbol, the commutativity of 5.4.1.11 says that

$$\mathrm{Ver}(a, E/K) = (a, E/L) \tag{5.4.1.13}$$

for $a \in K^\times$. Proposition 5.4.1.4 is less elementary than the previous compatibilities since the homomorphism $G^{ab}_{E/K} \to G^{ab}_{E/L}$ is not induced by a homomorphism $G_{E/K} \to G_{E/L}$.

The real reason that Weil groups behave similarly to Galois groups relative to successive extensions is that the latter are in fact quotients of the former, as

was shown by Shafarevich [13]. Suppose that $E/L/K$ are extensions of local fields with E/K and L/K Galois. We define a map

$$\mathrm{Sh} : G_{E/K} \to W_{L/K}/N_{E/L}E^\times \tag{5.4.1.14}$$

as follows: for $s \in G_{E/K}$ choose $x \in W_{E/K}$ mapping to s under the natural projection $W_{E/K} \to G_{E/K}$. Then $\pi^K_{E/L}(x) \in W_{L/K}$ is well-defined up to a factor in $N_{E/L}E^\times \subset L^\times \subset W_{L/K}$, and we define $\mathrm{Sh}(s)$ to be the class of $\pi^K_{E/L}(x)$ in $W_{L/K}/N_{E/L}E^\times$.

5.4.1.5 Theorem (Shafarevich) *Suppose that $E/L/K$ are extensions of local fields with E/K and L/K Galois. The diagram*

$$\begin{tikzcd} 1 \arrow[r] & G_{E/L} \arrow[r] \arrow[d, "\eta_{E/L}"] & G_{E/K} \arrow[r] \arrow[d, "\mathrm{Sh}"] & G_{L/K} \arrow[r] \arrow[d, equal] & 1 \\ 1 \arrow[r] & L^\times/N_{E/L}E^\times \arrow[r] & W_{L/K}/N_{E/L}E^\times \arrow[r] & G_{L/K} \arrow[r] & 1 \end{tikzcd} \tag{5.4.1.15}$$

is commutative. In particular if E/L is abelian, Sh *is an isomorphism.*

Proof. The commutativity of the right hand square is clear from the construction. As to the one on the left, suppose $W_{E/L}$ has been defined by some $\alpha \in E_L^\times$ and that $W_{E/K}$ is defined by $\iota^E_{L/K}(\alpha)$, as in our construction of $i : W_{E/L} \to W_{E/K}$. Then if $s \in G_{E/L}$, any lifting of it to $W_{E/K}$ lies in the image of $i^E_{L/K}$ and we may suppose it has the form $(\delta^E_{L/K}(\beta), s)$, with $\beta \in L_K^\times$ satisfying ${}^{\sigma-1}\beta = {}^{s-1}\alpha$. Now the diagram 5.4.1.10 in the case when $F/E/L/K$ is $E/L/L/K$ is

$$\begin{tikzcd} W_{E/L} \arrow[r, "\pi^L_{E/L}"] \arrow[d, "i^E_{L/K}"'] & W_{L/L} \arrow[d, "i^L_{L/K}"] \\ W_{E/K} \arrow[r, "\pi^K_{E/L}"'] & W_{L/K} \end{tikzcd}$$

which shows that $\mathrm{Sh}(s)$ can be identified with the image of

$$\pi^K_{E/L}(\beta, s) = (N_{E/L}(\beta), 1) \in W_{L/K}.$$

Since $N_{E/L}(\beta) = \eta_{E/L}(s)$ the left hand square is commutative. Finally if E/L is abelian $\eta_{E/L}$ is an isomorphism, hence so is Sh. ■

5.4.2 The kernel of $\pi^K_{E/L}$. Suppose $E/L/K$ are successive Galois extensions of local fields with L/K Galois. We have seen that $\pi^K_{E/L} : W_{E/K} \to W_{L/K}$ is surjective. The last part of the picture to fill in is the kernel. We need the following algebraic result of Artin and Tate [1, Ch. 13 Thm. 3]:

5.4.2.1 Proposition *Suppose*

$$0 \to A \to E \to G \to 0$$

is an extension of a finite group G by an abelian group A with cocycle $\eta \in H^2(G, A)$, and denote by $N : A \to A^G$ norm for the action of G on A. Then

$$I_G A \subseteq E^c \cap A \subseteq \mathrm{Ker}(N)$$

and the image of

$$\cup\eta : H^{-3}(G, \mathbb{Z}) \to H^{-1}(G, A) = \mathrm{Ker}(N)/I_G A$$

is $(E^c \cap A)/I_G A$.

Proof. It is clear that $I_G A$ and $E^c \cap A$ are contained in $\mathrm{Ker}(N)$. To show that $I_G A \subseteq E^c$ it suffices to observe that if the image of $e \in E$ is s then

$$eae^{-1}a^{-1} = {}^s aa^{-1} = {}^{s-1}a.$$

To prove the last statment it suffices to show that a character (i.e. homomorphism to $\mathbb{Q}/\mathbb{Z}$) of A vanishes on $E^c \cap A$ if and only if it vanishes on the inverse image in $\mathrm{Ker}(N)$ of the image of $\cup\eta$. We will establish that each of the following conditions are equivalent to f vanishing on $E^c \cap A$:

- f extends to a character of E: in fact any character of E necessarily vanishes on $E^c \cap A$; on the other hand if f vanishes on $E^c \cap A$ it defines a character of $A/(E^c \cap A) \simeq AE^c/E^c$, which then extends to a character of E since $\mathbb{Q}/\mathbb{Z}$ is an injective $\mathbb{Z}$-module.

- The pushout of the extension by f splits, or in other words $f_*(\eta) = 0$. In fact a splitting yields an extension of f to E; conversely an extension of f to a character of E yields a splitting by the universal property of pushouts.

- $(f_*\eta)(\xi) = 0$ for all $\xi \in \hat{H}^{-3}(G, \mathbb{Z})$: this follows since $H^2(G, \mathbb{Q}/\mathbb{Z})$ is the linear dual of $\hat{H}^{-3}(G, \mathbb{Z})$. Since $(f_*\eta)(\xi) = f_*(\eta \cup \xi)$, another equivalent condition is

- $f_*(\eta \cup \xi) = 0$ for all $\xi \in \hat{H}^3(G, \mathbb{Z})$. In other words, f_* vanishes on the subgroup
$$\eta \cup \hat{H}^{-3}(G, \mathbb{Z}) \subseteq \hat{H}^{-1}(G, A).$$

The last condition, finally is equivalent to that of the proposition. ■

5.4.2.2 Corollary *For any Galois extension L/K of local fields,*

$$\mathrm{Ker}(N_{L/K} : L^\times \to K^\times) = W^c_{L/K} \cap L^\times. \tag{5.4.2.1}$$

Proof. In this case $\eta = u_{L/K}$ and the cup product with $u_{L/K}$ is an isomorphism. ■

5.4.2.3 Theorem *Suppose $E/L/K$ are Galois extensions of local fields with E/K Galois. The homomorphism $i^K_{E/L} : W_{E/L} \to W_{E/K}$ identifies the kernel of $\pi^K_{E/L}$ with the commutator subgroup $W^c_{E/L}$. In particular there is an isomorphism*

$$W_{E/K}/W^c_{E/L} \xrightarrow{\sim} W_{L/K}. \tag{5.4.2.2}$$

Proof. Note first that any of the possible choices for $i^K_{E/L}$ are conjugate by an element of $L^\times \subset W_{E/L}$, so the image of $W^c_{E/L}$ in $W_{E/K}$ is fixed. The commutative diagram 5.4.1.2 shows that the kernel of $W_{E/K} \to W_{L/K}$ maps to the kernel of $G_{E/K} \to G_{L/K}$ and is therefore contained in $W_{E/L}$. The diagram 5.4.1.10 applied to $E/L/L/K$ is

$$\begin{tikzcd}
W_{E/L} \arrow[r, "\pi^L_{E/L}"] \arrow[d, "i^E_{L/K}"'] & W_{L/L} \arrow[d, "i^L_{L/K}"] \\
W_{E/K} \arrow[r, "\pi^K_{E/L}"'] & W_{L/K}
\end{tikzcd}$$

and since the vertical arrows are injective, $i^K_{E/L}$ identifies the kernel of $\pi^K_{E/L}$ with the kernel of $W_{E/L} \to W_{L/L} \to W_{L/K}$. Since $W_{L/L} = L^\times$ is abelian, $W^c_{E/L}$ is contained in the kernel.

To prove the converse inclusion we apply the snake lemma to the diagram 5.4.1.2. The result is yields an exact sequence

$$0 \to \mathrm{Ker}(N_{E/L}) \to \mathrm{Ker}(\pi^K_{E/K}) \to G_{L/K} \xrightarrow{\eta_{E/L}} L^\times/N_{E/L}E^\times \to 0$$

where $N_{E/L}$ is the field norm $E^\times \to L^\times$, and we have used corollary 5.4.1.2 and proposition 5.4.1.1. We know that the kernel of $\eta_{E/L}$ is $G^c_{E/L}$. Suppose now $x \in \mathrm{Ker}(\pi^K_{E/L})$; by the last remark its image in $G_{E/L}$ is in the commutator subgroup, so x is the product of an element of $W^c_{E/L}$ and an element of $\mathrm{Ker}(N_{E/L})$. But corollary 5.4.2.2 shows that elements of $\mathrm{Ker}(N_{E/L})$ are in $W^c_{E/L}$ as well, and we are done. ■

Note that the isomorphism 5.4.2.2 depends on the specific identifications of the groups $W_{E/K}$ and $W_{L/K}$, i.e. the choice of $\alpha \in E^\times_K$. As remarked in the proof however, the subgroup $W^c_{E/L} \subset W_{E/K}$ is independent of such choices.

Chapter 6

The Existence Theorem

The first result of (global) class field theory was the Kronecker-Weber theorem, which states that any abelian extension of $\mathbb{Q}$ is contained in a cyclotomic extension, i.e. some field $\mathbb{Q}(\mu_n)$ there μ_n is the group of nth roots of unity in $\bar{\mathbb{Q}}$. In other words the abelian extensions are generated by "torsion points" of the multiplicative group, and Kronecker was able to show similarly that all abelian extensions of an imaginary quadratic extension of $\mathbb{Q}$ could be generated from torsion points on suitable elliptic curves. The generalization to other number fields remains problematic.

In the local case the situation is more satisfactory. Any abelian extension of $\mathbb{Q}_p$ is cyclotomic, i.e. contained in an some extension $\mathbb{Q}_p(\mu_n)$ where now μ_n is the group of nth roots of unity in $\bar{\mathbb{Q}}_p$. For general local fields in characteristic zero, Lubin and Tate were constructed formal groups whose torsion points generate totally ramified abelian extensions of the given local field. The existence theorem will be deduced from this, and the Hasse-Arf theorem for local fields is an easy consequence.

6.1 Formal Groups

6.1.1 Formal Group Laws. Let R be a commutative ring (with identity, as always). A *one-dimensional formal group law over* R is a power series in two variables $F(X,Y) \in R[[X,Y]]$ such that

$$F(X,Y) \equiv X + Y \mod (X,Y)^2, \tag{6.1.1.1}$$

$$F(X,0) = F(0,X) = X, \tag{6.1.1.2}$$

$$F(X,Y) = F(Y,X), \tag{6.1.1.3}$$

$$F(F(X,Y),Z) = F(X,F(Y,x)). \tag{6.1.1.4}$$

One can show that 6.1.1.2 follows from 6.1.1.1 and 6.1.1.4. Furthermore 6.1.1.3 is a consequence of the remaining conditions if R has no $\mathbb{Z}$-torsion, but we will not need this fact. One can also deduce from 6.1.1.1 that there is a unique

power series $i(X)$ such that

$$F(X) \equiv -X \mod (X^2), \qquad F(i(X), X) = F(X, i(X) = 0 \tag{6.1.1.5}$$

which fact we wiil leave as an exercise. Formal groups in several variables are defined similarly. To cut down on the density of notation one sometimes uses the notation

$$X +_F Y = F(X, Y). \tag{6.1.1.6}$$

for the formal group law $F(X, Y)$.

If F and G are one-dimensional formal group laws a *morphism* $F \to G$ is a power series $f(X) \in R[X]$ such that

$$f(X) +_G f(Y) = f(X +_F Y). \tag{6.1.1.7}$$

and as usual we say that f is an *strict isomorphism* if there is a power series $g(X)$ such that $f(g(X)) = g(f(X) = X$. Then g is a morphism $G \to F$, as one easily sees from 6.1.1.7. An isomorphism f is a *strict isomorphism* if $f(X) \equiv X$ mod $(X^2$. More generally, if A is a commutative R-algebra, then a morphism (resp. isomorphism, strict isomorphism) over A is a power series $f \in A[[X]]$ satisfying 6.1.1.7 (resp. and is an isomorphism, resp. a strict isomorphism in the previous sense). As usual we denote by $\mathrm{Hom}_A(F, G)$ the set of morphisms $F \to G$ defined over A, and if $A = R$ we just write $\mathrm{Hom}(F, G)$. Similarly $\mathrm{End}_A(F)$ is the ring of endomorphisms of F defined over A, and if $A = R$ we drop the subscript.

We will see many examples later but for now just mention two: the *formal additive group* $\hat{\mathbb{G}}_a$ for which

$$\hat{\mathbb{G}}_a(X, Y) = X + Y \tag{6.1.1.8}$$

and the *formal multiplicative group* $\hat{\mathbb{G}}_m$ defined by

$$\hat{\mathbb{G}}_m(X, Y) = X + Y + XY = (1 + X)(1 + Y) - 1. \tag{6.1.1.9}$$

The "power operations" for a formal group F are defined in the usual way:

$$[0](X) = 0, \qquad [n + 1](X) = [n](X) +_F X \text{ for} n \geq 1 \tag{6.1.1.10}$$

(we do not usually specify F in the notation). For example, in the additive group $\hat{\mathbb{G}}_a$

$$[n](X) = nX \tag{6.1.1.11}$$

and in the multiplicative group $\hat{\mathbb{G}}_m$

$$[n](X) = (1 + X)^n - 1. \tag{6.1.1.12}$$

If R is a topological ring it makes sense to speak of the convergence of $F(X, Y)$ for appropriate values of X and Y, in which case F defines a group law (assuming it is "closed" in an obvious sense). The main case of interest to us is

when R has the I-adic topology for some ideal $I \subset R$. In this case it is clear from (6.1.1.1)-(6.1.1.4) that F induces a commutative group law on I which we denote by $F(I)$. For example $\hat{\mathbb{G}}_a(I)$ is isomorphic to I considered as an additive subgroup of R, while $\hat{\mathbb{G}}_m(I)$ is isomorphic to the subgroup $1 + I \subseteq R^\times$. We should emphasize though that the notion of a formal group law is a completely algebraic one, and that it makes sense, for example to speak of formal group law over $\mathbb{Z}$.

If R is a field of characteristic $p > 0$ one can show that either $[p](X)$ is zero or its first nonzero term is aX^{p^h} for some positive integer h. In the first case we say the formal group law has infinite height, and in the second it has height h. For example the formal additive group over a field of characteristic $p > 0$ has *infinite height*, while the formal multiplicative group has *height one*. Later on we will construct formal groups of any given height.

If R is the integer ring of a mixed characteristic valued field and F is a formal group law over R, the *height* of F is the height of its reduction modulo the maximal ideal of R.

6.1.2 Logarithms. Suppose R is an integral domain with fraction field K and $F(X, Y)$ is a formal group law over R. A *logarithm* for F is a power series $\ell(X) \in K[[X]]$ satisfying

$$\ell(X) \equiv X \mod (X)^2, \qquad \ell(F(X, Y)) = \ell(X) + \ell(Y). \tag{6.1.2.1}$$

A formal group law does not necessarily have a logarithm, and if it does it is not necessarily unique. The Lubin-Tate formal groups to be considered later do in fact have logarithms, and in some sense the logarithm is the more fundamental object than the formal group itself. Note that the first condition in 6.1.2.1 implies that ℓ has a functional inverse, and thus the formal group law F is uniquely determined by ℓ:

$$F(X, Y) = \ell^{-1}(\ell(X) + \ell(Y)). \tag{6.1.2.2}$$

Suppose F and F' are formal group laws over R with logarithms ℓ, ℓ'. A power series $h \in R[[X]]$ is a morphism $F \to F'$ if there is an $a \in R$ such that

$$\ell' \circ h = a\ell \tag{6.1.2.3}$$

as one sees immediately from 6.1.2.2. When 6.1.2.3 holds we have $h(X) \equiv aX \mod (X^2)$, so if $a \in R^\times$, h is an isomorphism.

The problems with existence and uniqueness only arise in positive characteristic.

6.1.2.1 Proposition *Suppose R is an integral domain whose fraction field has characteristic* 0. *Any formal group over R has a unique logarithm.*

Proof. Suppose first that F is a formal group law over R and ℓ is a logarithm for F. If we differentiate the equality in 6.1.2.1 with respect to Y we find

$$\ell'(F(X, Y))F_2(X, Y) = \ell'(Y)$$

where $F_2(X,Y)$ is the derivative F with respect to its second argument. Setting $Y=0$ and using 6.1.1.2 yields

$$\ell'(X)F_2(X,0) = \ell'(0) = 1. \tag{6.1.2.4}$$

The property 6.1.1.1 shows that $F_2(X,0) \equiv 1 \mod (X)$, so $F_2(X,0)$ is an invertible power series. Thus ℓ' is determined by F, and since ℓ has no constant term it is itself determined by F.

The equation 6.1.2.4 shows that in fact we should define $\ell(X)$ by

$$\ell(X) = \int_0^X \frac{dX}{F_2(X,0)} \tag{6.1.2.5}$$

where the right hand side is to be understood as the (unique) integral of the power series $F_2(X,0)^{-1}$. To show that the ℓ so defined satisfies 6.1.2.1 we first note that $\ell(X) \equiv X \mod (X^2)$ since $F_2(X,0)^{-1} \equiv 1 \mod (X)$. Second, differentiating the associativity law 6.1.1.4 with respect to Z yields

$$F_2(F(X,Y),Z) = F_2(X,F(Y,Z))F_2(Y,Z)$$

and setting $Z=0$ and using 6.1.1.2 results in

$$F_2(F(X,Y),0) = F_2(X,Y)F_2(Y,0).$$

If we write this as

$$\frac{1}{F_2(Y,0)} = \frac{1}{F_2(F(X,Y),0)}\frac{\partial}{\partial Y}(F(X,Y))$$

and integrate with respect to Y we get

$$\ell(Y) + g(X) = \ell(F(X,Y))$$

for some $g \in K[[X]]$. Switching X and Y and using the commutativity of the group law, we find that $g(X) = \ell(X)$, which proves 6.1.2.4. ■

6.1.2.2 Corollary *If R is a $\mathbb{Q}$-algebra then any formal group over R is isomorphic to $\hat{\mathbb{G}}_a$.*

Proof. In this case the logarithm lies in $R[[X]]$. ■

Equation 6.1.2.4 shows what can go wrong in positive characteristic: if $F = \hat{\mathbb{G}}_m$ is the formal multiplicative group 6.1.2.4 says that a logarithm ℓ must satisfy

$$\ell'(X) = \frac{1}{1+X} = \sum_{n>0}(-1)^n X^n$$

but in positive characteristic the series cannot be integrated. As for the question of uniqueness, note that any series of the form $\sum_{n\geq 0} a_n X^{p^n}$ is a logarithm for the formal additive group in characteristic $p>0$.

Suppose $h : F \to G$ is a morphism of formal group laws. Differentiating $G(h(X), h(Y)) = h(F(X,Y))$ with respect to Y yields

$$G_2(h(X), h(Y))h'(Y) = h'(F(X,Y))F_2(X,Y).$$

Setting $Y = 0$ and rearranging then gives

$$\frac{1}{F_2(X,0)} = \frac{h'(X)}{G_2(h(X),0)}.$$

and integrating yields the equality

$$\ell_F(X) = \ell_G(h(X)). \tag{6.1.2.6}$$

6.1.3 The Functional Equation Lemma. Hazewinkel's functional equation lemma is a powerful tool for constructing formal group laws with specified properties, but it can also be used for proving a variety of congruences and integrality statements. We refer the reader to [8] for some of the more exotic applications. Here we use it to construct the Lubin-Tate formal groups.

The setup of the functional equation lemma is the following: K is a commutative ring, $R \subseteq L$ is a subring and $\mathfrak{a} \subseteq R$ is an ideal. Furthermore p is a prime, q is a power of p and we assume that $p \in \mathfrak{a}$, so that $R/\mathfrak{a}$ is a ring of characteristic p. Finally there is an endomorphism $\sigma : L \to L$ stabilizing R, such that the induced action of σ on $R/\mathfrak{a}$ is the qth power Frobenius. For any power series $f(X) = \sum_{n>0} b_n X^n \in L[[X]]$ (note that there is no constant term) we define

$$\sigma(f) = \sum_{n>0} \sigma(b_n)X^n, \qquad \varphi(f) = \sum_{n>0} \sigma(b_n)X^{qn}.$$

The last ingredient is a sequence $s_i \in L$ for $i \geq 1$ such that $\sigma^r(s_i)\mathfrak{a} \subseteq R$ for all $i \geq 1$ and $r \geq 0$. Given $f \in K[[X]]$, the *functional equation condition* relative to (s_i) is the assertion

$$f(X) - \sum_{i>0} s_i \varphi^i(f) \in R[[X]]. \tag{6.1.3.1}$$

The functional equation lemma is the content of the next three propositions.

6.1.3.1 Proposition *Suppose $f = \sum_{n>0} b_n X^n \in K[[X]]$ satisfies the functional equation condition 6.1.3.1, and $b_1 \in R^\times$. Then*

$$F(X,Y) = f^{-1}(f(X) + f(Y)) \in R[[X,Y]].$$

6.1.3.2 Proposition *Suppose $f(X) \in K[[X]]$ satisfies the hypotheses of proposition 6.1.3.1. (i) If $\bar{f}(X) \in K[[X]]$ is any power series satisfying $\bar{f}(0) = 0$, $f'(0) \in R$ and 6.1.3.1 then $f^{-1}(\bar{f}(X)) \in R[[X]]$. (ii) If $f = \sum_{n>0} b_n X^n \in K[[X]]$ satisfies 6.1.3.1, and $h(X) \in R[[X]]$ then $f(h(X))$ satisfies 6.1.3.1 as well.*

6.1.3.3 Proposition *Suppose f satisfies 6.1.3.1 and $g(X)$, $h(X) \in R[[X]]$. For any $r > 0$, $g(X) \equiv h(X) \mod \mathfrak{a}^r$ if and only if $f(g(X)) \equiv f(h(X)) \mod \mathfrak{a}^r$.*

We will give the proofs later in this section. For now we note some consequences.

6.1.3.4 Corollary *(i) If $f \in K[[X]]$ satisfies 6.1.3.1 and $f(X) \equiv X \mod (X^2)$ then $F(X,Y) = f^{-1}(f(X) + f(Y))$ is a formal group law with logarithm $f(X)$. (ii) If $F \in R[[X,Y]]$ is a formal group law whose logarithm satisfies 6.1.3.1, a formal group law $G \in R[[X,Y]]$ is strictly isomorphic to F if and only if its logarithm satisfies 6.1.3.1 with the same sequence (s_i).*

Proof. Assertion (i) is clear. If h is a strict isomorphism $F \to G$ and ℓ_F, ℓ_G are the logarithms of F and G then $\ell_G(h(X)) = \ell_F(X)$. The corollary then follows from propositions 6.1.3.1 and 6.1.3.2. ■

As another example, let

$$\ell(X) = \sum_{n>0} \frac{X^{p^n}}{p^n}, \qquad \log(1+X) = \sum_{n>0} (-1)^{n+1} \frac{X^n}{n}.$$

A quick calculation shows that

$$\ell(X) - \frac{1}{p}\ell(X^p) = X, \qquad \log(X) - \frac{1}{p}\log(X^p) \in \mathbb{Z}_{(p)}[[X]]$$

and it follows from proposition 6.1.3.2 that the power series

$$AH(X) = \exp\left(\sum_{n>0} \frac{X^{p^n}}{p^n}\right) \tag{6.1.3.2}$$

has coefficients in $\mathbb{Z}_{(p)}[[X]]$; it is known as the *Artin-Hasse exponential*.

A more general result along this line is a famous lemma of Dwork. In this case we take K to be the completion of the maximal unramified extension of $\mathbb{Q}_p$, R is its integer ring, and σ is the lifting of the pth power Frobenius to R and K. Dwork's lemma states that a power series $h(X) \in K[[X]]$ with constant term 1 lies in $R[[X]]$ if and only if $\sigma(h(X^p))/h(X)^p \in 1 + pXR[[X]]$. In fact propostion 6.1.3.2 shows that $h \in R[[X]]$ if and only if

$$\log(h) - \frac{1}{p}\varphi(h) \in R[[X]]$$

and this condition is equivalent to $\varphi(h)/h^p \in 1 + pXR[[X]]$, as one sees by multiplying by $-p$ and exponentiating.

The rest of this section is devoted to the proof of propositions 6.1.3.1-6.1.3.3 We begin with some lemmas.

6.1.3.5 Lemma *Suppose $f(X) = \sum_{n>0} a_n X^n$ satisfies 6.1.3.1 and $a_1 \in R^\times$ If we write $n = q^r m$ with $q \not| m$ then $a_n \mathfrak{a}^r \subseteq R$.*

Proof. We argue by induction on n, the case $n = 1$ being evident. By 6.1.3.1 we can write

$$f(X) = g(X) + \sum_{i>0} s_i \varphi^i(f)$$

with $g \in R[[X]]$. If $g = \sum_{n>0} b_n X^n$ then

$$a_n = b_n + s_1\sigma(a_{n/q}) + s_2\sigma^2(a_{n/q^2}) + \cdots + s_r\sigma^r(a_{n/q^r}).$$

The induction step follows on multiplying by $\mathfrak{a}^r$ since $s_i\mathfrak{a} \in R$. ■

6.1.3.6 Lemma *Suppose $f(X) \in K[[X]]$ satisfies 6.1.3.1 and $g \in R[[X_1, \ldots, X_d]]$. Then*

$$\varphi(f)^i \circ g \equiv \varphi^i(f \circ g) \mod \mathfrak{a}R[[X_1, \ldots, X_d]]$$

for all $i > 0$.

Proof. If we write $f = \sum_{n>0} a_n X^n$ then

$$\varphi^i(f)(g(X_.) = \sum_{n>0} \sigma^i(a_n) g(X_.)^{nq^i}.$$

Let $n = q^r m$. Since σ is a lift of the qth power Frobenius,

$$g(X_.)^{q^i} \equiv \sigma^i(g)(X_.^{q^i}) \mod \mathfrak{a}$$

and a straightforward induction shows that

$$g(X_.)^{q^{i+r}} \equiv (\sigma^i(g)(X_.^{q^i}))^{q^r} \mod \mathfrak{a}^{r+1}.$$

Raising the the mth power then yields

$$g(X_.)^{nq^i} \equiv (\sigma^i(g)(X_.^{q^i}))^n \mod \mathfrak{a}^{r+1}.$$

By lemma 6.1.3.5 we know that if $n = q^r m$ with $q \not| m$ then $a_n \mathfrak{a}^r \in R$. For such n we have

$$\sigma^i(a_n) g(X_.)^{nq^i} \equiv (\sigma^i(a_n g)(X_.^{q^i}))^n \mod \mathfrak{a}$$

and summing over n yields

$$\varphi^i(f)(g(X_.)) \equiv \sum_{n>0} \sigma^i(a_n)\sigma^i(g)(X_.^{q^i})^n \mod \mathfrak{a}$$

which is

$$\varphi(f)^i \circ g \equiv \varphi^i(f \circ g) \mod \mathfrak{a}.$$

■

Proof of proposition 6.1.3.1: The hypothesis is that $f = \sum_{n>0} b_n X^n \in K[[X]]$ satisfies 6.1.3.1 and $b_1 \in R^\times$, and in particular $f^{-1}(X)$ is defined. Write

$$F(X,Y) = f^{-1}(f(X) + f(Y)) = \sum_{n>0} F_n(X,Y)$$

with F_n homogenous of degree n. Since $f(X) \equiv b_1 X \mod (X^2)$ and $b_1 \in R^\times$, $F_1(X,Y) = X + Y \in R[X,Y]$. Suppose we have shown that $F_1, \ldots, F_{n-1} \in R[X,Y]$. Since F has no constant term,

$$(F_1 + \cdots + F_{n-1})^r \equiv F(X,Y)^r \mod (X,Y)^{n+1}$$

for all $r > 1$. Since $q > 1$,

$$s_i\varphi^i(f)(F_1 + \cdots + F_{n-1}) \equiv s_i\varphi^i(f)(F(X,Y)) \mod (X,Y)^{n+1}$$

for all $i > 0$. Applying lemma 6.1.3.6 and recalling that $s_i\mathfrak{a} \subseteq R$, we find

$$s_i\varphi^i(f)(F) \equiv s_i\varphi^i(f \circ F) \mod (R[[X,Y]] + (X,Y)^{n+1}) \tag{6.1.3.3}$$

for $i > 0$. As before we define $g(X) \in R[[X]]$ by

$$f(X) = g(X) + \sum_{i>0} s_i\varphi^i(f)(X).$$

Substituting $F(X,Y)$ for X and applying 6.1.3.3 yields

$$\begin{aligned} f(F(X,Y)) &\equiv g(F(X,Y)) + \sum_{i>0} s_i\varphi^i(f \circ F)(X,Y) \\ &\equiv g(F(X,Y)) + \sum_{i>0} s_i\varphi^i(f(X) + f(Y)) \\ &\equiv g(F(X,Y) + f(X) + f(Y) - g(X) - g(Y) \end{aligned}$$

where the congruences are modulo $R[[X,Y]] + (X,Y)^{n+1}$. Since $g \in R[[X]]$ and $f(F(X,Y)) = f(X) + f(Y)$,

$$g(F(X,Y)) \equiv 0 \mod (R[[X,Y]] + (X,Y)^{n+1}).$$

and since $g(X) \equiv b_1 X \mod (X^2)$ and $b_1 \in R^\times$, this shows that

$$F(X,Y) \equiv 0 \mod (R[[X,Y]] + (X,Y)^{n+1}).$$

Consequently $F_n(X,Y) \in R[X,Y]$ as required.

Proof of proposition 6.1.3.2: The proof of part (i) is similar to that of proposition 6.1.3.1 and we will just sketch it. Set $f^{-1}(\bar{f}(X)) = h(X)$, so that $\bar{f} = f \circ h$.

Then $h = \sum_{n>0} h_n X^n$ and we know that $h_1 \in R$. Suppose we have shown $h_1, \ldots, h_{n-1} \in R$. The same argument as before shows that

$$s_i\varphi^i(f)(h) \equiv s_i\varphi^i(f \circ h) \mod (R[[X]] + (X^{n+1}).$$

where the equivalence is modulo $R[[X]] + (X^{n+1})$. Then

$$\begin{aligned} f(h(X)) &\equiv g(h(X)) + \sum_{i>0} s_i\varphi^i(f \circ h)(X) \\ &\equiv g(h(X)) + \sum_{i>0} s_i\varphi^i(\bar{f}(X)) \mod R[[X]] + X^{n+1}K[[X]] \\ &\equiv g(h(X)) + \bar{f}(X) - g(X) \mod R[[X]] + X^{n+1}K[[X]] \end{aligned}$$

and as before we find $g(h(X)) \equiv 0$, then $h(X) \equiv 0$, and finally $h_n \in R$.

For part (ii) we set $\bar{f} = f \circ h$. With the notation of the previous paragraph we have $h \equiv 0$ and thus

$$\begin{aligned} \bar{f}(X) - \sum_{i>0} s_i\varphi^i(\bar{f})(X) &= f(h(X)) - \sum_{i>0} s_i\varphi^i(f \circ h)(X) \\ &\equiv f(h(X)) - \sum_{i>0} s_i\varphi^i(f)(h(X)) \\ &\equiv g(h(X)) \equiv 0. \end{aligned}$$

Proof of proposition 6.1.3.3: Suppose first that $g(X) \equiv h(X) \mod \mathbf{f}^r$. As before write $f(X) = \sum_{n>0} b_n X^n$, so that if $n = q^s m$ with $q \not| m$ then $b_n \mathfrak{a}^s \in R$ by lemma 6.1.3.5. The same computation as in the proof of lemma 6.1.3.6 shows that

$$g(X)^{q^s} \equiv h(X)^{q^s} \mod \mathfrak{a}^{r+s}$$

and thus

$$g(X)^n \equiv h(X)^n \mod \mathfrak{a}^{r+s}$$

for this n. Applying 6.1.3.5 once again then yields

$$f(g(X)) \equiv f(h(X)) \mod \mathfrak{a}^r.$$

From this we can deduce the more general assertion that

$$g(X) \equiv h(X) \mod \mathfrak{a}^r + X^n K[[X]] \implies f(g(X)) \equiv f(h(X)) \mod \mathfrak{a}^r + X^n K[[X]].$$

for any $n > 1$. In fact if we replace $g(X)$, $h(X)$ by power series $\bar{g}(X)$, $\bar{h}(X)$ with the same terms of degree less than n, and all terms of higher degree equal to zero then

$$f(g(X)) \equiv f(\bar{g}(X)) \equiv f(\bar{h}(X) \equiv f(h(X))$$

where all congruences are modulo $\mathfrak{a}^r + X^n K[[X]]$. Then $\bar{g}(X) \equiv \bar{h}(X) \mod \mathfrak{a}^r$ and the assertion follows.

To prove the converse implication we first show that if $h(X) \in \mathfrak{a}^r R[[X]]$ then $f^{-1}(h(X)) \equiv 0 \mod \mathfrak{a}^r$. As before, define $g(X) \in R[[X]]$ by $f = g + \sum_{i>0} s_i \varphi^i(f)$ and write $\bar{h}(X) = f^{-1}(h(X)) = \sum_{n>0} c_n X^n$. Since f, f^{-1} and g have no constant terms and their linear terms are $b_1 X$, $b_1^{-1} X$ and $b_1 X$ respectively we must have $c_1 \in \mathfrak{a}^r$. Suppose we have shown $c_i \in \mathfrak{a}^r$ for $i \leq n$. Once again write $n = q^s m$ with $q \not| m$; then $\bar{h}(X)^{q^s} \equiv 0 \mod \mathfrak{a}^{r+1} + X^{n+1} K[[X]]$ and therefore $f(\bar{h}(X)^{q^s}) \equiv 0 \mod \mathfrak{a}^{r+1} + X^{n+1} K[[X]]$ by the result of the previous paragraph. From this we deduce that

$$h \equiv f \circ \bar{h} \equiv g \circ \bar{h} + \sum_{i>0} s_i (\varphi^i f) \circ \bar{h} \equiv 0 \mod \mathfrak{a}^r + X^{n+1} K[[X]].$$

This shows that $g(\bar{h}(X)) \equiv \mathfrak{a}^r + X^{n+1} K[[X]]$, and since $g(X) \equiv b_1 X \mod x^2$, $\bar{h}(X) = f^{-1}(h(X)) \equiv \mathfrak{a}^r$ as required.

Suppose now $g(X)$, $h(X) \in R[[X]]$ and $f(g(X)) \equiv f(h(X)) \mod \mathfrak{a}^r$. If we set

$$j(X) = f^{-1}(f(h(X)) - f(g(X)))$$

then $j(X) \equiv 0 \mod \mathfrak{a}^r$ by what we have just shown. Then

$$f(h(X)) = f(j(X)) + f(g(X))$$

or

$$h(X) = F(j(X), g(X))$$

and consequently

$$h(X) \equiv F(j(X), g(X)) \equiv F(0, g(X)) \equiv g(X) \mod \mathfrak{a}^r$$

which was to be shown.

6.2 Lubin-Tate Groups

6.2.1 Construction of Lubin-Tate formal groups. Suppose now K is a local field with integer ring $\mathcal{O}_K$. Let π be a uniformizer of $\mathcal{O}_K$, and denote by p and q the characteristic and the cardinality of the residue field of $\mathcal{O}_K$. A *Lubin-Tate logarithm* for π is a power series $\ell(X) \in K[[X]]$ such that

$$\ell(X) \equiv X \mod (X^2), \qquad \ell(X) - \frac{1}{\pi}\ell(X^q) \in \mathcal{O}_K[[X]] \tag{6.2.1.1}$$

or in other words, $\ell(X)$ satisfies the functional equation condition 6.1.3.1 with $s_1 = \pi^{-1}$ and $s_i = 0$ for $i > 1$. Such power series exist in abundance; for example if $g(X) \in \mathcal{O}_K[[X]]$ is any power series such that $g(X) \equiv X \mod (X^2)$, the equation

$$\ell(X) = g(X) + \frac{1}{\pi}\ell(X^q) \tag{6.2.1.2}$$

can be solved by recursion, yielding an $\ell \in K[[X]]$ satisyfing 6.2.1.1. Thus if $g(X) = X$,

$$\ell(X) = X + \frac{X^q}{\pi} + \frac{X^{q^2}}{\pi^2} + \cdots \tag{6.2.1.3}$$

For any $\ell(X)$ satisfying 6.2.1.1 the functional equation lemma is applicable with K, q as above and σ equal to the identity on K. By corollary 6.1.3.4,

$$F_\ell(X, Y) = \ell^{-1}(\ell(X) + \ell(Y)) \tag{6.2.1.4}$$

is a one-dimensional formal group law over $\mathcal{O}_K$, and any two ℓ satisfying $\ell(X) \equiv X \mod (X^2)$ and 6.2.1.1 give rise to strictly isomorphic formal group laws. We will call them *Lubin-Tate formal groups* associated to π. If the specific choice of ℓ does not matter, we denote any of these formal group laws by F_π.

For any $a \in \mathcal{O}_K$ the power series

$$[a](X) = \ell^{-1}(a\ell(X)). \tag{6.2.1.5}$$

has coefficients in $\mathcal{O}_K$ by proposition 6.1.3.1. It is immediate that the $[a](X)$ is an endomorphism of the formal group law F_ℓ. Since $\ell(X) \equiv X \mod (X^2)$ we must have $[a](X) \equiv aX \mod (X^2)$, and this shows that $a \mapsto [a]$ is an injective ring homomorphism $\mathcal{O}_K \to \mathrm{End}(F_\ell)$. Observe that $[a]$ is an automorphism of F_ℓ if and only if a is a unit in $\mathcal{O}_K$. Since

$$\ell([a](X)) = a\ell(X) \tag{6.2.1.6}$$

by definition, we see that $[a](X)$ is the nth power endomorphism when $a = n$ is a natural number.

Let $\ell(X)$ be a Lubin-Tate logarithm and define $g(X)$ by 6.2.1.2. Setting $a = \pi$ in 6.2.1.6 and multiplying by π yields

$$\ell([\pi](X) = \pi\ell(X) = \pi g(X) + \ell(X^q) \equiv \ell(X^q) \mod (\pi).$$

Proposition 6.1.3.3 then implies that

$$[\pi](X) \equiv X^q \mod (\pi) \tag{6.2.1.7}$$

and on the other hand the definition 6.2.1.5 shows that

$$[\pi](X) \equiv \pi X \mod (X^2). \tag{6.2.1.8}$$

The next proposition and its corollary will show that the logarithm ℓ can be recovered from the series $[\pi]$, and that in fact any power series in $\mathcal{O}_K[[X]]$ satisfying 6.2.1.7 and 6.2.1.8 is $[\pi](X)$ for a unique Lubin-Tate logarithm. We will see later that it is useful to use a logarithm for which the endomorphism $[\pi](X)$ has a given form, e.g. a polynomial of degree q. In fact the original development of the theory starts with a power series $g(X)$ satisfying 6.2.1.7 and 6.2.1.8 and constructs the formal group law from $g(X)$.

6.2.1.1 Proposition *For any $g(X) \in R[[X]]$ such that*

$$g(X) \equiv \pi X \mod (X^2), \quad g(X) \equiv X^q \mod (\pi) \tag{6.2.1.9}$$

the limit

$$\ell(X) = \lim_{n\to\infty} \frac{1}{\pi^n} g^{\circ n}(X) \tag{6.2.1.10}$$

exists and is a Lubin-Tate logarithm. The associated formal group law satisfies $[\pi](X) = g(X)$.

Proof. Once we show that the limit is a Lubin-Tate logarithm the last statement is clear since

$$\ell(g(X)) = \lim_{n\to\infty} \frac{1}{\pi^n} g^{\circ(n+1)}(X) = \pi\ell(X) = \ell([\pi](X)).$$

For $n \geq 1$ set

$$g_n(X) = \frac{1}{\pi^n} g^{\circ n}(X).$$

Clearly $g_n(X) \equiv X \mod (X^2)$, so the rest of the proposition follows if we show that

$$g_{n+1}(X) \equiv g_n(X) \mod (\pi, X^q)^{n-1} + X^{n-1}K[[X]] \tag{6.2.1.11}$$

$$g_{n+1}(X) - \frac{1}{\pi} g_n(X^q) \in R[[X]] \tag{6.2.1.12}$$

for all $n \geq 1$. We first show that $\pi^n g_n(X) \in (\pi, X^q)^n$. For $n = 1$ this follows from 6.2.1.9 and if this has been proven for n then

$$\pi^{n+1} g_{n+1}(X) = g(\pi^n g_n(X)) \in \pi(\pi, X^q)^n + (\pi, X^q)^{qn} \subseteq (\pi, X^q)^{n+1}.$$

If we write

$$g(X) = \pi X + h(X) + X^q \quad \text{with} \quad h(X) \in \pi X^2 R[[X]].$$

then

$$\begin{aligned} g_{n+1}(X) &= \frac{1}{\pi^{n+1}} g(\pi^n g_n(X)) \\ &= \frac{1}{\pi^{n+1}} (\pi \cdot \pi^n g_n(X) + h(\pi^n g_n(X)) + (\pi^n g_n(X))^q) \\ &= g_n(X) + \frac{h(\pi^n g_n(X))}{\pi^{n+1}} + \frac{(\pi^n g_n(X))^q}{\pi^{n+1}}. \end{aligned}$$

Since $h(X) \in \pi X^2 R[[X]]$,

$$\frac{h(\pi^n g_n(X))}{\pi^{n+1}} \in \frac{1}{\pi^n} (\pi, X^q)^{2n} \subseteq (\pi, X^q)^n + X^{qn} K[[X]]$$

and similarly

$$\frac{(\pi^n g_n(X))^q}{\pi^{n+1}} \in \frac{1}{\pi^{n+1}} (\pi, X^q)^{qn} \subseteq (\pi, X^q)^{n(q-1)-1} + X^{n(q-1)-1} K[[X]].$$

The congruence 6.2.1.11 follows since $nq > n(q-1) - 1 \geq n - 1$.

The congruence 6.2.1.9 implies

$$g(X + \pi^n Y) \equiv g(X) \mod \pi^{n+1} R[[X, Y]]$$

and by induction we find

$$g^{\circ n}(X + \pi Y) \equiv g(X) \mod \pi^{n+1} R[[X, Y]]$$

for all $n \geq 1$. If we write $g(X) = \pi h(X) + X^q$ and substitute X^q and $h(X)$ for X and Y we find that

$$g^{\circ(n+1)}(X) = g^{\circ n}(X^q + \pi h(X)) \equiv g^{\circ n}(X^q) \mod \pi^{n+1}$$

and 6.2.1.11 follows on dividing by π^{n+1}. ■

6.2.1.2 Corollary *The logarithm $\ell(X)$ of a Lubin-Tate group associated to π satisfies*

$$\ell(X) = \lim_{n \to \infty} \frac{1}{\pi^n} [\pi^n](X). \tag{6.2.1.13}$$

Proof. This follows from 6.2.1.7–6.2.1.8 and $[\pi]^{\circ n} = [\pi^n]$. ■

Since F_ℓ depends only on π up to strict isomorphism we can denote it by F_π, if we do not need to specify the logarithm ℓ. On the other hand these formal groups really do depend on the choice of π, at least over $\mathcal{O}_K$. Nontheless:

6.2.1.3 Proposition *Suppose π, π' are uniformizers of $\mathcal{O}_K$ and $\pi' = u\pi$, so that $u \in \mathcal{O}_K^\times$. If ℓ and ℓ' are Lubin-Tate logarithms attached to π and π', there is a power series $h(X) \in \mathcal{O}_{\hat{K}^{nr}}[[X]]$ and $v \in \mathcal{O}_{\hat{K}^{nr}}^\times$ such that ${}^{\sigma-1}v = u$ and*

$$\ell' \circ h = v\ell, \tag{6.2.1.14}$$

$$h(X) \equiv vX \mod (X^2) \tag{6.2.1.15}$$

$${}^{\sigma}h = h \circ [u]. \tag{6.2.1.16}$$

Proof. The existence of $v \in \mathcal{O}_{\hat{K}^{nr}}^\times$ satisfying ${}^{\sigma-1}v = u$ follows from Lemma 1.3.6.2. Then

$$\begin{aligned} v\ell - \frac{1}{\pi'}\varphi(v\ell) &= v\ell - \frac{1}{\pi'}{}^{\sigma}v\varphi(\ell) \\ &= v\ell - \frac{1}{\pi}v\varphi(\ell) = v(\ell - \frac{1}{\pi}\varphi(\ell)) \in \mathcal{O}_{\hat{K}^{nr}}[[X]] \end{aligned}$$

and if we set

$$h(X) = (\ell')^{-1}(v\ell(X))$$

proposition 6.1.3.1 shows $h(X) \in \mathcal{O}_{\hat{K}^{nr}}[[X]]$. Furthermore 6.2.1.14 and 6.2.1.15 follow by construction, and

$$\begin{aligned} {}^{\sigma}h(X) &= (\ell')^{-1}({}^{\sigma}v\ell(X)) \\ &= (\ell')^{-1}(vu\ell(X)) \\ &= (\ell')^{-1}(v\ell([u](X))) \\ &= h([u](X)) \end{aligned}$$

establishes 6.2.1.16. ■

6.2.1.4 Corollary *If π and π' are any uniformizers of $\mathcal{O}_K$, the formal group laws F_π, $F_{\pi'}$ are isomorphic over the integer ring of the completion $\hat{K}^{nr}$ of the maximal unramified extension of K.*

Proof. In fact 6.2.1.14 shows that h is a morphism $F_\pi \to F_{\pi'}$, and since v is a unit 6.2.1.15 shows that it is an isomorphism. ■

A Lubin-Tate logarithm and its inverse have convergence properties analogous to the usual logarithm and exponential.

6.2.1.5 Proposition *Suppose $\ell(X)$ is a Lubin-Tate logarithm and F_ℓ is the associated formal group law. (i) The power series $\ell(X) = \sum_{n>0} a_n X^n$ converges for $|X| < 1$. (ii). Denote by $e(X)$ the functional inverse of $\ell(X)$, and for any extension L/K of nonarchimdean fields denote by D_L the open disk*

$$D_L = \{x \in \mathcal{O}_L \mid v(x) > (q-1)^{-1}\}$$

where v is the valuation of L such that $v(\pi) = 1$. Then $e(X)$ converges on D_L and $\ell(X)$ and $e(X)$ give inverse isomorphism of $F_\ell(L)$ with the additive group of D_L.

Proof. If $n = q^r m$ with $q \not| m$ then lemma 6.1.3.5 shows that $\pi^r a_n \in R$, so for any $x \in \mathcal{O}_L$,

$$v(a_n x^n) = v(a_n) + nv(x) > nv(x) - \log_q(n) \to \infty \text{ as } n \to \infty$$

which proves (i). If $x \in D_L$ and $n = q^r m$ as before,

$$v(a_n x^n) \geq v(a_n x^{q^r - 1}) + v(x) \geq \frac{q^r - 1}{q - 1} - r + v(x) \geq v(x)$$

which shows that ℓ maps D_L to itself, and that $v(\ell(x)) \geq v(x)$ for $x \in D_L$. Since $e(X)$ is a formal inverse to ℓ it suffices for (ii) to show that $e(X)$ converges on D_L and maps D_L to itself. ■

When K has characteristic $p > 0$, the logarithm 6.2.1.3 clearly satisfies

$$\ell(X + Y) = \ell(X) + \ell(Y). \tag{6.2.1.17}$$

Since the formal group law is determined by ℓ, the Lubin-Tate formal group associated to ℓ is just the formal additive group $\hat{\mathbb{G}}_a$. In this case the group itself is not of so much interest and one speaks instead of a formal $\mathcal{O}_K$-module structure on $\hat{\mathbb{G}}_a$, or simply a formal $\mathcal{O}_K$-module. The interest of this case is that this notion can be globalized, i.e. K can be replaced by the function ring of a smooth affine curve over a finite field. This leads to the notion of a Drinfeld module, which plays a central role in the global Langlands correspondence for function fields.

6.2.2 Division points. Fix a Lubin-Tate group F_π associated to a uniformizer π of K. The *division points* of F_π are the torsion points of $F_\pi(\mathfrak{m})$ considered as an $\mathcal{O}_K$-module. Since $[a]$ is an isomorphism for $a \in \mathcal{O}_K^\times$, the group of division points is the union of the kernels of the endomorphisms $[\pi^n]$ on $F_\pi(\mathfrak{m})$. We denote by A_n the kernel of $[\pi^n]$ on $F(\mathfrak{m})$. Since any two such groups are strictly isomorphic over $\mathcal{O}_K$ the $\mathcal{O}_K$-module $F_\pi(\mathfrak{m})$ is independent of the particular choice of F_π up to isomorphism (but not independent of π). The same then follows for the groups A_n.

Finally, since the coefficients of the series $[\pi](X)$, $[a](X)$ are in K, the absolute Galois group G_K of K acts on A_n, and this action is linear for the $\mathcal{O}_K$-module structure of A_n. Finally, for every n the inclusion $A_n \to A_{n+1}$ is $\mathcal{O}_K$-linear and Galois-equivariant, as is the map $A_{n+1} \to A_n$ induced by $[\pi]$. Using these maps we define

$$A_\infty = \varinjlim_n A_n \qquad T(F_\pi) = \varprojlim_n A_n. \tag{6.2.2.1}$$

The group $T(F_\pi)$ called the *Tate module* of F_π.

6.2.2.1 Lemma *For all n, A_n is isomorphic to $\mathcal{O}_K/\pi^n\mathcal{O}_K$ as an $\mathcal{O}_K$-module. Furthermore A_∞ is isomorphic to $K/\mathcal{O}_K$ and $T(F_\pi)$ is isomorphic to $\mathcal{O}_K$ as $\mathcal{O}_K$-modules.*

Proof. Since A_n is a finite group it is a finitely generated $\mathcal{O}_K$, and therefore a sum of cyclic $\mathcal{O}_K$-modules since $\mathcal{O}_K$ is a PID. By proposition 6.2.1.1 we can choose F_π such that $[\pi](X)$ is a polynomial

$$g(X) = \pi X + \cdots + X^q \tag{6.2.2.2}$$

of degree q. Since g is separable it has q roots, which means that A_1 has order q. This implies that $A_1 \simeq \mathcal{O}_K/\pi\mathcal{O}_K$ as an $\mathcal{O}_K$-module, and it follows that A_n as well. Since

$$g^{\circ n}(X) = \pi^n X + \cdots + X^{q^n}$$

A_n has cardinality q^n, so we must have $A_n \simeq \mathcal{O}_K/\pi^n\mathcal{O}_K$. The remaining statements are immediate. ■

6.2.2.2 Corollary *There is a homomorphism*

$$\kappa : G_K \to \mathcal{O}_K^\times \tag{6.2.2.3}$$

such that

$$s(x) = [\kappa(s)](x) \tag{6.2.2.4}$$

for all $x \in A_\infty$.

Proof. If $u \in A_n$ generates A_n as an $\mathcal{O}_K$-module there is a $\kappa_n(s) \in \mathcal{O}_K^\times$ such that $s(u) = [\kappa_n(s)](u)$, and then $s(x) = [\kappa_n(s)](x)$ for all $x \in A_n$. Since $\kappa_n(s)$ is well-defined modulo π^n we must have

$$\kappa_{n+1}(s) \equiv \kappa_n(s) \mod \pi^n$$

for all n, and $\kappa(s) = \varprojlim_n \kappa_n(s)$ satisfies 6.2.2.4. ■

We next define

$$K_\pi^n = K(A_n), \qquad K_\pi = K(A_\infty) = \bigcup_n K_\pi^n. \tag{6.2.2.5}$$

Note that K_π^n is generated by any generator of the $\mathcal{O}_K$-module. Thus if we assume, as we may that $[\pi](X) = \pi X + \cdots + X^q$ is a monic polynomial of degree q, K_π^n is the splitting field over K of the polynomial

$$\begin{aligned} f_n(X) = \frac{[\pi^n](X)}{[\pi^{n-1}](X)} = \frac{[\pi]([\pi^{n-1}](X))}{[\pi^{n-1}](X)} = g([\pi^{n-1}](X)) \\ \text{where} \quad g(X) = \frac{[\pi](X)}{X} = X^{q-1} + \cdots + \pi. \end{aligned} \tag{6.2.2.6}$$

Note also that $g(X)$ is an Eisenstein polynomial of degree $q-1$, so $f_n(X)$ is an Eisenstein polynomial of degree $(q-1)q^{n-1}$.

6.2.2.3 Theorem *The homomorphism 6.2.2.3 factors through an isomorphism*

$$\kappa_\pi : \mathrm{Gal}(K_\pi/K) \xrightarrow{\sim} \mathcal{O}_K^\times. \tag{6.2.2.7}$$

Proof. By construction κ factors through a homomorphism

$$\kappa_\pi : \mathrm{Gal}(K_\pi/K) \to \mathcal{O}_K^\times.$$

The groups $\mathrm{Gal}(K_\pi/K)$, $\mathcal{O}_K^\times$ have filtrations

$$G_n = \mathrm{Gal}(K_\pi^n/K) \subset \mathrm{Gal}(K_\pi/K), \qquad U_n = \mathrm{Ker}(\mathcal{O}_K^\times \to (\mathcal{O}_K/\pi^n)^\times)$$

and by construction $\kappa_\pi(G_n) \subseteq U_n$. Since $G \simeq \varprojlim_n G_n$ and $\mathcal{O}_K^\times \simeq \varprojlim_n U_N$ it suffices to show that κ_π induces isomorphisms $G_n \xrightarrow{\sim} U_n$ for all n. The question is independent of the particular choice of Lubin-Tate formal group, so we may assume that $[\pi](X)$ has the form assumed in 6.2.2.6.

Evidently $G_n \to U_n$ is injective, for if $s \in G_n$ maps to $u \in U_n$ it fixes every element of A_n. Thus it suffices to show that $|G_n| = |U_n|$ for all n. In fact $|U_n| = (q-1)q^{n-1}$, and since f_n is an Eisenstein polynomial of degree $(q-1)q^{n-1}$, $|G_n| = [K_\pi^n : K] = (q-1)q^{n-1}$. ■

6.2.2.4 Proposition *The uniformizer π is a norm from K_π^n for all $n > 0$.*

Proof. With the notation of 6.2.2.6 and the preceding proof, if $u \in A_n \setminus A_{n-1}$ then $N_{K_\pi^n/K}(-u) = \pi$. ■

6.3 The Lubin-Tate Reciprocity Law

6.3.1 Proof of the existence theorem. The existence theorem will be proven by showing that $K^{nr}K_\pi$ is the maximal abelian extension of K for any uniformizer π, and then relating the norm residue symbol to the homomorphism κ defined above.

By proposition 1.2.5.2 K^{nr} and K_π are linearly disjoint over K. This yields isomorphisms

$$K^{nr}K_\pi \simeq K^{nr} \otimes_K K_\pi \tag{6.3.1.1}$$

and

$$\mathrm{Gal}(K^{nr}K_\pi/K) \simeq \mathrm{Gal}(K^{nr}/K) \times \mathrm{Gal}(K_\pi/K). \tag{6.3.1.2}$$

From this it follows that the inertia group $I_\pi \subset \mathrm{Gal}(K^{nr}K_\pi/K)$ can be identified with $\mathrm{Gal}(K_\pi/K)$.

6.3.1.1 Lemma *Suppose K is a nonarchimedean field, L/K is an algebraic extension and let $\hat{L}$ be the completion of L for the extension of the valuation of K to L. If $x \in \hat{L}$ is separable algebraic of L then $x \in L$.*

Proof. Let L^{sep} be a separable closure of L. We can identify the separable closure L' of L in $\hat{L}$ with a subfield of L^{sep}, so it suffices to show that $L' = L$. Equivalently we must show that $\mathrm{Gal}(L^{sep}/L) = \mathrm{Gal}(L^{sep}/L')$, but this is clear: by continuity, an automorphism of L^{sep} fixing L must by continuity fix L' as well, and conversely an automorphism fixing L' must fix L. ■

6.3.1.2 Proposition *Let K be a local field and let K^{nr} be its maximal unramified extension. For any two uniformizers π, π' of $\mathcal{O}_K$, $K^{nr}K_\pi = K^{nr}K_{\pi'}$.*

Proof. We take all fields in the proposition to be subfields of the completion of a fixed algebraic closure of K. By proposition 6.2.1.3 the formal group laws F_π, $F_{\pi'}$ are isomorphic over the integer ring of K^{nr}. This shows that $\hat{K}^{nr}K_\pi = \hat{K}^{nr}K_{\pi'}$. It follows that $K^{nr}K_\pi$ and $K^{nr}K_{\pi'}$ have the same completion, and then 6.3.1.1 shows that $K^{nr}K_\pi = K^{nr}K_{\pi'}$. ■

For the rest of this section we will write $L = K^{nr}K_\pi$ since this is independent of π. If π is a uniformizer of $\mathcal{O}_K$, any element of $K^\times$ has a unique expression as $\pi^n u$ with $u \in \mathcal{O}_K^\times$ and we can define a homomorphism $r_\pi : K^\times \to \mathrm{Gal}(L/K)$

by setting

$$r_\pi(\pi) = \begin{cases} \sigma_{arith} & \text{on } K^{nr} \\ 1 & \text{on } K_\pi \end{cases}$$
$$r_\pi(u) = \begin{cases} 1 & \text{on } K^{nr} \\ \kappa_\pi^{-1}(u^{-1}) & \text{on } K_\pi \end{cases} \quad \text{for } u \in \mathcal{O}_K^\times. \tag{6.3.1.3}$$

6.3.1.3 Lemma *The homomorphism $r_\pi : \mathrm{Gal}(L/K) \to K^\times$ is independent of π*

Proof. Since $K^\times$ is generated as a group by uniformizers it suffices to show that $r_\pi(\pi') = r_{\pi'}(\pi')$ for any two uniformizers π, π' of K. Since since both are σ_{arith} on K^{nr} it suffices to show they are equal on $K_{\pi'}$, and since $r_{\pi'}(\pi')$ is the identity on $K_{\pi'}$ we must show that the same is true for $r_\pi(\pi')$.

Let ℓ and ℓ' be logarithms associated to π and π' and let A_∞ and A'_∞ be the groups of division points of the associated formal groups. The isomorphism $A_\infty \to A'_\infty$ is given by the power series $h(X)$ in proposition 6.2.1.3, so with the above notation we must show that ${}^s h(x) = h(x)$. Since $h \in \mathcal{O}_{\hat{K}^{nr}}[[X]]$, s induces σ on $\hat{K}^{nr}$, while on A_∞ it induces $[u^{-1}]$. Then 6.2.1.16 shows that

$${}^s h(x) = {}^s h({}^s x) = {}^\sigma h([u^{-1}](x)) = (h \circ [u])([u^{-1}](x)) = h(x)$$

as required. ■

We can now compute the norm residue symbol on the maximal abelian extension K^{ab} of K.

6.3.1.4 Theorem *Let K be a local field with uniformizer π. (i) The field $K^{nr}K_\pi$ is the maximal abelian extension of K. (ii) Let π be a uniformizer of K and for all $x \in K^\times$ write $x = \pi^n u$ with $u \in \mathcal{O}_K^\times$. Then*

$$\theta(x)(a) = \begin{cases} \sigma^n(a) & a \in K^{nr} \\ [u^{-1}](a) & a \in K_\pi. \end{cases} \tag{6.3.1.4}$$

Proof. Denote by $r : K^\times \to \mathrm{Gal}(L/K)$ any of the "common value" of the maps r_π. Since $K^\times$ is generated by uniformizers, the correctness of 6.3.1.4 for $a \in L$ will follow if we show that $\theta(\pi) = r(\pi)$ for any uniformizer π. First, $\theta(\pi)$ and $r(\pi)$ both induce σ on K^{nr}, and 6.3.1.3 shows that $r(\pi)$ is the identity on K_π. On the other hand π is a norm from K_π^n for all n, so $\theta(\pi)$ is the identity on K_π as well. Therefore

$$\theta(x)|L = r(x) \tag{6.3.1.5}$$

which proves (ii). If $I_\pi \subset \mathrm{Gal}(L/K)$, $I \subset \mathrm{Gal}(K^{ab}/K)$ are the inertia subgroups 6.3.1.4 shows that the composite map

$$\mathcal{O}_K^\times \xrightarrow{\theta} I \to I_\pi \xrightarrow{\kappa_\pi} \mathcal{O}_K^\times$$

is $u \mapsto u^{-1}$. It is therefore an isomorphism, and as the first two maps are surjections and the last is an isomorphism, the canonical projection $I \to I_\pi$ must be an isomorphism as well. Then $\mathrm{Gal}(K^{ab}/K) \to \mathrm{Gal}(L/K)$ is an isomorphism, which proves (i). ■

6.3.1.5 Corollary *The reciprocity map $\theta : K^\times \to \mathrm{Gal}(K^{ab}/K)$ induces a topological isomorphism of $\mathcal{O}_K^\times$ with the inertia subgroup of $\mathrm{Gal}(K^{ab}/K)$.*

Proof. This follows from the identification $I \simeq \mathrm{Gal}(K_\pi/K)$ and 6.3.1.4, which shows that θ is the composition of two continuous bijections. Since all groups involved are compact, a continuous bijection is a homeomorphism. ■

The corollary is the main step in the proof of the existence theorem:

6.3.1.6 Theorem *Let K be a local field. (i) The reciprocity map $\theta : K^\times \to \mathrm{Gal}(K^{ab}/K)$ is a continuous injection with dense image. (ii) The topology induced on $K^\times$ is the topology defined by the open subgroups of finite index. (iii) For every open subgroup $U \subseteq K^\times$ of finite index there is a finite abelian extension L/K such that $N_{L/K}(L^\times) = U$.*

Proof. The topology of $K^\times$ is the product topology for any isomorphism $K^\times \simeq \mathcal{O}_K^\times \times \mathbb{Z}$ determined by a choice of uniformizer. That θ is continuous then follows from corollary 6.3.1.5. That it is an injection with dense image follows from the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{O}_K^\times \arrow[r] \arrow[d, "\theta"] & K^\times \arrow[r] \arrow[d, "\theta"] & \mathbb{Z} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & I \arrow[r] & \mathrm{Gal}(K^{ab}/K) \arrow[r] & \hat{\mathbb{Z}} \arrow[r] & 0
\end{tikzcd}$$

in which the rows are exact, the left vertical arrow is an isomorphism and the right vertical arrow is an injection with dense image. This establishes (i), and (ii) follows from (i). Finally (iii) follows from (ii) since an open subgroup of finite index in $K^\times$ containing a norm group is itself a norm group. ■

6.3.2 Cyclotomic Extensions. As a first application of these results we have the local Kronecker-Weber theorem:

6.3.2.1 Theorem *Any finite abelian extension of $\mathbb{Q}_p$ is a subfield of $\mathbb{Q}_p(\mu_n)$ for some n.*

Proof. The ordinary logarithm function is a Lubin-Tate logarithm for $\mathbb{Q}_p$, and the associated formal group is $\hat{\mathbb{G}}_m$. The division points of $\hat{\mathbb{G}}_m$ are the values $1 - \zeta$ where ζ runs through al p-power roots of unity. Finally any unramified extension of $\mathbb{Q}_p$ is obtained by adjoining to $\mathbb{Q}_p$ roots of unity of order prime to p. It follows from (i) of theorem 6.3.1.4 that the maximal abelian of extension of

$\mathbb{Q}_p$ is obtained by adjoining all roots of unity in $\bar{\mathbb{Q}}_p$ to $\mathbb{Q}_p$, and this establishes the theorem. ■

Shafarevich noticed that the global Kronecker-Weber theorem is a simple consequence of the local theorem 6.3.2.1. The proof needs just one nontrivial global result, a well-known theorem of Minkowski:

6.3.2.2 Theorem *If $K/\mathbb{Q}$ is a finite unramified extension then $K = \mathbb{Q}$.*

The proof can be found in any of the standard references, e.g. [11, Ch. 4].

6.3.2.3 Theorem *Any finite abelian extension of $\mathbb{Q}_p$ is a subfield of $\mathbb{Q}(\mu_n)$ for some n.*

Proof. Suppose $K/\mathbb{Q}$ is abelian, and for all primes p let K_p be the completion of K at some place $\mathfrak{p}$ of K above p. By the local Kronecker-Weber theorem 6.3.2.1,

$$K_p \subseteq \mathbb{Q}_p(\mu_{p^{n_p}})$$

for some integer n_p. Since K is ramified at finitely many primes, n_p is prime to p for all but finitely many p. Write $n_p = p^{e_p} m_p$ with $p \not| m_p$. Then $e_p = 1$ for almost all p and we set

$$n = \prod_p p^{e_p}.$$

We will show that $K \subseteq \mathbb{Q}(\mu_n)$.

The field $L = K(\mu_n)$ is an abelian extension of $\mathbb{Q}$. If we denote by L_p the completion of L at some place above the prime $\mathfrak{p}$ of K, then $L_p \simeq K_p(\mu_{p^e n'_p})$ for some n'_p not divisible by p. Thus p is ramified in K if and only if it is ramified in L. The inertia group I_p of L above p coincides with the inertia group of $L_p/\mathbb{Q}_p$, so $|I_p| = \phi(p^{e_p})$. Let $I \subseteq \mathrm{Gal}(L/\mathbb{Q})$ be the subgroup generated by the I_p. Since $\mathrm{Gal}(L/\mathbb{Q})$ is abelian,

$$|I| \leq \prod_p |I_p| = \prod_p \phi(p^{n_p}) = \phi(n) = [\mathbb{Q}(\mu_n) : \mathbb{Q}].$$

The fixed field L^I of I is unramified above $\mathbb{Q}$ at all primes p, so by $L^I = \mathbb{Q}$ by Minkowski's theorem 6.3.2.2. Then $I = \mathrm{Gal}(L/\mathbb{Q})$, and the last inequality implies that

$$[L : \mathbb{Q}] = |I| \leq [\mathbb{Q}(\mu_n) : \mathbb{Q}].$$

Since $\mathbb{Q}(\mu_n) \subseteq L$ we conclude that $L = \mathbb{Q}(\mu_n)$, and then $K \subseteq \mathbb{Q}(\mu_n)$. ■

Shafarevich also gave an elementary if somewhat lengthy proof of the local theorem 6.3.2.1. A somewhat simplied proof of this was given by Narkiewicz; an account can be found in [15].

6.3.3 The ramification filtration. We first compute the ramification filtration and the Herbrand function for the extensions K_π^n/K; the corresponding filtration for K_π/K and K^{ab}/K follows immediately from this. The computation is a direct generalization of the computation in the cyclotomic case.

As before we denote by $U^i \subseteq \mathcal{O}_K^\times$ the subgroup of units congruent to 1 modulo $\mathfrak{m}^i$. Suppose $u \in U^i \setminus U^{i+1}$ and set $s = \theta(u)$. If $\pi_n \in K_\pi^n$ is any uniformizer then $i(s) = v(s(\pi_n) - \pi_n)$ where v is the normalized valuation of K_π^n. We may take π_n to be a generator of A_π^n as an $\mathcal{O}_K$-module, so that $[\pi^n](\pi_n) = 0$ and $[\pi^{n-1}](\pi_n) \neq 0$. By theorem 6.3.1.4 we have

$$s(\pi_n) = [u^{-1}](\pi_n).$$

We can write $u^{-1} = 1 + \pi^i v$ with $v \in \mathcal{O}_K^\times$; then

$$s(\pi_n) = [1 + \pi^i v](\pi_n) = F_\pi(\pi_n, [\pi^i v](\pi_n)) \tag{6.3.3.1}$$

where F_π is the group law. Now $\beta = [\pi^i v](\pi_n)$ lies in $A^{n-i} \setminus A^{n-i-1}$, and is thus a uniformizer of the field K_π^{n-i}. Since K_π^n/K_π^{n-i} has degree q^i we must have $v(\beta) = q^i$. If we write

$$F_\pi(X, Y) = X + Y + \sum_{i,j>1} c_{ij} X^i Y^j$$

then 6.3.3.1 says that

$$s(\pi_n) = \pi_n + \beta + \sum_{i,j>1} c_{ij} \pi_n^i \beta^j.$$

Since $c_{ij} \in \mathcal{O}_K$ and π_n, β have positive valuation,

$$v(s(\pi_n) - \pi_n) = v(\beta) = q^i$$

and therefore

$$G_u = \theta(U^i) \quad \text{for } q^{i-1} - 1 < u \leq q^i - 1. \tag{6.3.3.2}$$

The computation of the Herbrand function is just like the cyclotomic case. For $u \in (q^{i-1} - 1, q^i - 1)$ we have

$$\varphi'_{K_\pi^n/K}(u) = [\mathcal{O}_K^\times : U^i] = \frac{1}{(q-1)q^{i-1}}$$

and so

$$G^v = \theta(U^i) \quad \text{for } i - 1 < v \leq i. \tag{6.3.3.3}$$

In the above discussion $i \leq n$, but since the upper numbering is compatible with quotients, 6.3.3.3 holds for the extension K_π/K as well. Finally K^{ab}/K and K_π have the same inertia group, so 6.3.3.3 holds for K^{ab}. We have thus proven the Hasse-Arf theorem for local fields: for any abelian extension L/K, the breaks of the ramification filtration in the upper numbering are at integers.

Bibliography

[1] Artin, E. and Tate, J., *Class Field Theory*, Benjamin, 1967.

[2] Bourbaki, N., *Algèbre, Chapitre 10* , Masson, 1980.

[3] Cartan, H. and Eilenberg, S., Princeton Univ. Press, 1956.

[4] Cassels, J.W.S and Fröhlich, A, eds., *Algebraic Number Theory, 2nd. ed.*, London Math. Soc., 2010.

[5] Deligne, P., *Les constants des équations fonctionelles des fonctions L*, Modular Functions of One Variable II (P. Deligne and W. Kuyk, ed.), Springer, 1973.

[6] Dieudonné, Jean, *Groupes de Lie et hyperalgèbres de Lie sur un corps de caractéristique $p > 0$. VII.*, Math. Ann. **134** (1957), 114–133.

[7] Dwork, B., *Norm residue symbol in local number fields*, Hamb. Abh. **22** (1958), 180–190.

[8] Hazewinkel, Michiel, *On formal groups. The functional equation lemma and some of its applications*, Journées de Géometrie Algébrique de Rennes (I) (Pierre Berthelot and Lawrence Breen, ed.), Astérisque, vol. 63, SMF, 1979, pp. 73–82.

[9] Manin, Yu. I., *The theory of commutative formal groups over fields of finite characteristic*, Russian Math. Surveys **18** (1963), 1–83.

[10] Morava, Jack, *The Weil Group as Automorphisms of the Lubin-Tate Group*, Journées de Géometrie Algébrique de Rennes (I) (Pierre Berthelot and Lawrence Breen, ed.), Astérisque, vol. 63, SMF, 1979, pp. 169–178.

[11] Samuel, Pierre, *Algebraic Theory of Numbers*, Hermann, 1970.

[12] Serre, Jean-Pierre, *Corps Locaux*, Hermann, 1968.

[13] Shafarevich, I. R., *On Galois groups of p-adic fields*, C. R. (Doklady) Acad. Sci. URSS (N.S.) **53** (1946), 4–5.

[14] Tate, John , *Number Theoretic Background*, Automorphic Forms, Representations, and L-functions (Borel, A. and Casselman, W., ed.), vol. XXXIII, PSPM, no. 2, AMS, 1979, pp. 3–26.

[15] Washington, Lawrence, *Introduction to Cyclotomic Fields*, Springer-Verlag, 1982.