Local quadratic extensions

Bill Casselman
University of British Columbia
cass@math.ubc.ca

Suppose $F$ to be a $p$-adic field of characteristic other than 2, $E = F(\sqrt{A})$. In this essay I’ll investigate the structure of $E$ in relation to that of $F$.

The main results will be a description of the integers in $E$, given $\mathfrak{o}_F$, and of the fine structure of the norm homomorphism from $E^\times$ to $F^\times$. This last amounts to a major component of local class field theory for quadratic extensions.

Much of my treatment has amounted to an exercise in reading §V.3 of [Serre:1968], which deals with the more general situation in which $E/F$ is a cyclic extension of prime degree. This is only slightly more difficult to deal with than the quadratic case. In all proofs of full local reciprocity that I am aware of, understanding prime cyclic extensions is a crucial step.

Contents

1. Squares ................................................................. 2
3. Integers ................................................................. 4
3. Different and trace ...................................................... 5
4. Norms and units ....................................................... 6
5. Norms and the Galois group ........................................... 9
6. Appendix. Hensel’s Lemma ............................................ 10
7. References ............................................................ 11

Throughout, $F$ will be an arbitrary local field of characteristic other than 2. In addition:

- $\mathfrak{o}_F$ = integers in $F$
- $\mathfrak{p}_F$ = maximal ideal of $\mathfrak{o}_F$
- $\varpi_F$ = a generator of $\mathfrak{p}_F$
- $U_F = \mathfrak{o}_F^\times$ (the units of $\mathfrak{o}_F$)
- $F_F = \mathfrak{o}_F/\mathfrak{p}_F$
- $q = |F_F|$ (a power of a prime $p$)
- $\varphi$ = the Frobenius automorphism $x \mapsto x^q$ of $F$, which fixes elements of $F$.

Similarly for $E$. I’ll often ignore subscripts when referring to $F$.

As I’ll recall in an appendix, Hensel’s Lemma implies that for every $x$ in $F$ there exists a unique $y = \tau(x)$ in $\mathfrak{o}$ reducing to $x$ modulo $\mathfrak{p}$, such that $y^q = y$. Such liftings are called Teichmüller elements. The group $U_F$ is therefore isomorphic to $F_F^\times \times (1 + \mathfrak{p})$.

I’ll write $x \equiv_n y$ if $x - y \in \mathfrak{p}_F^n$, $x \sim y$ if $x/y$ is a unit.

For each $n \geq 0$ let

$$U^{[n]} = 1 + p^n,$$

with the convention that $U^{[0]} = U$. These are the congruence subgroups of $U$.

Let $\theta$ be any section of the projection $\mathfrak{o} \to F$, so that $F^\theta$ is made up of representatives modulo $\mathfrak{p}$. Every element of $\mathfrak{o}$ can be written uniquely in a normal form

$$f_0 + f_1 \varpi + f_2 \varpi^2 + \cdots$$
Local quadratic extensions

with each \( f_i \) in \( F^\theta \).

If the characteristic of \( F \) is 2, define constants \( c_\circ \geq 1 \) in \( \mathbb{N} \) and \( u_\circ \neq 0 \) in \( F \) by the requirement that \( 2 \equiv c_\circ + 1 \) \( u_\circ \varpi^{e_\circ} \).

The map \( x \mapsto x^2 + x \) is an \( \mathbb{F}_2 \)-linear map from \( F \) to itself, with both kernel and cokernel of size 2. Let \( \mathcal{E} \) be a couple of representatives in \( F \) of the cokernel, with one of them equal to 0.

1. Squares

In this section I will describe the group \( F^2/(F^\times)^2 \). Since a choice of generator \( \varpi_F \) identifies \( F^\times \) with \( \mathbb{Z} \times U \), this reduces to describing \( U/U^2 \).

1.1. Lemma. The projection \( o \mapsto o/p \) induces an isomorphism of \( U/U_{[1]} \) with \( F \times \), and for \( n \geq 2 \) the map

\[
 x \mapsto 1 + x \varpi^{n-1}
\]

induces an isomorphism of \( F \) with \( U/[n]/U \).

The second isomorphism in Lemma 1.1 is not at all canonical, since for \( n \geq 1 \) it depends on a choice of \( \varpi \).

The canonical isomorphism is with \( p^n/p^{n+1} \), which may be identified with \( \otimes (p/p^2) \).

The starting point of the investigation is Corollary 6.5, which I repeat here:

1.2. Proposition. If \( A \equiv 2 c_\circ + 1 \) \( \pmod{4} \), then \( A \) is a square in \( U_F \).

I cannot resist offering a second proof.

1.3. Lemma. For \( \alpha \in 4p_F \), the binomial series

\[
 (1 + \alpha)^{1/2} = 1 + \frac{1}{2} \alpha + \frac{(1/2)(1/2 - 1)}{2} \alpha^2 + \frac{(1/2)(1/2 - 1)(1/2 - 2)}{3!} \alpha^3 + \cdots
\]

converges to \( \sqrt{1 + \alpha} \) in \( F \).

Proof. If \( p \) is odd, then 2 is invertible and the coefficient of each \( \alpha^k \) lies in \( o_F \). Hence the series clearly converges for \( \alpha \in p_F \). If \( p = 2 \), we need to know that

\[
 \text{ord}_2(n!) = \left( \sum_k \left| \frac{n}{2^k} \right| \right) < \frac{n}{2} \left( \sum \frac{1}{1 - 1/2} \right) = n.
\]

Remark. Suppose \( A \equiv 1 + 4y \varpi \pmod{4p^2} \). A more rapid convergence is provided by Newton’s approximation

\[
 x_{n+1} = x_n - h_n \quad \left( h_n = \frac{x_n^2 - A}{2x_n} \right)
\]

with an initial estimate \( x_0 = 1 + (y/u_\circ) \varpi^{e_\circ+1} \). This converges quadratically, since

\[
 x_{n+1}^2 - A = h_n^2.
\]

It is not easy to implement the quadratic convergence, however, since division by \( x_n \) is not so easy. But one can obtain linear convergence conveniently by truncating terms. This is basically the same as an application of Hensel’s Lemma.
If \( p \) is odd, then every element of \( U[1] \) is a square, and hence any quadratic character is trivial on it. In this case, then, \( U/U^2 \) is isomorphic to \( F^\times/(F^\times)^2 \).

- From now on in this section I’ll assume that \( p = 2 \).

Let \( V = U/U[2e_\circ + 1] \). As a consequence of the Lemma:

1.4. Corollary. The canonical projection from \( U_F/U_F^2 \) to \( V/V^2 \) is an isomorphism.

Therefore we need only describe \( V/V^2 \).

1.5. Proposition. The natural map

\[
1 + F^\theta \varpi + F^\theta \varpi^3 + \cdots + F^\theta \varpi^{2e_\circ - 1} + 4E \longrightarrow V/V^2
\]

is a bijection.

I’ll call any expression of the form in this Proposition a square-free normal form. Of course it depends on choices of \( F^\theta \) and \( \varpi \).

Proof. There exists a practical algorithm that gives the square-free normal form of any element expressed in normal form. This follows from a few basic facts: (i) for every \( u \) in \( F \) there exists \( v \) in \( F \) with \( v^2 + u = 0 \); (ii) for \( k < e_\circ \)

\[
(1 + v \varpi^k)^2(1 + u \varpi^{2k}) \equiv 2k + 1 + (v^2 + u)\varpi^{2k},
\]

and (iii) we have

\[
(1 + 2x)^2 \equiv 2e_\circ + 1 + 4((x^2 + x).
\]

Example. Suppose \( F = \mathbb{Q}_2(\varpi) \) with \( \varpi^3 + 2\varpi + 2 = 0 \). What is the square-free normal form of \( A = 1 + \varpi^2 \)? Here \( e_\circ = 3, 2e_\circ + 1 = 7 \). The calculation begins:

\[
(1 + \varpi)^2 A = (1 + 2\varpi + \varpi^2)(1 + \varpi^2) = 1 + 2\varpi + 2\varpi^2 + 2\varpi^3 + \varpi^4 = 1 + 2\varpi^3,
\]

since \( 2\varpi + 2\varpi^2 + \varpi^4 = 0 \). But from then, by a sequence of substitutions

\[
2 = -2\varpi - \varpi^3
\]

and deletions from \( 1 + x + y \) to \( 1 + x \) when \( y \) lies in \( p^7 \):

\[
1 + 2\varpi^3 = 1 - 2\varpi^4 - \varpi^6 \\
\equiv 1 + 2\varpi^5 - \varpi^6 \\
\equiv 1 - 3\varpi^6 \\
\equiv 1 + \varpi^6.
\]

As we shall see in the next section, this implies that the field extension \( F(\sqrt{A}) \) is unramified.

A character \( \chi : F^\times \to C^\times \) is said to have conductor \( p^m \) if it is trivial on \( 1 + p^m \) but not trivial on \( 1 + p^{m-1} \). Conventionally, the trivial character is said to have conductor \( \varnothing \).

1.6. Corollary. (a) For \( 1 \leq k \leq e_\circ \) there are exactly \((q - 1)q^k \) quadratic characters of conductor \( p^{2k} \) and no quadratic characters of conductor \( p^{2k-1} \). (b) If \( k = e_\circ \), there are exactly \( q^k \) characters of conductor \( p^{2k+1} \). (c) If \( n \geq 1 \) there are no characters of conductor \( p^{2k+1+n} \).

Since the quadratic characters are partitioned by their conductors, this confirms the Proposition, since

\[
1 + (q - 1) + (q - 1)q + \cdots + (q - 1)q^{e_\circ - 1} + q^{e_\circ} = 2q^{e_\circ}.
\]


2. Integers

Suppose $A$ in $\mathbb{Z}$ to be square-free. It is well known that if $A \equiv 2$ or $3$ modulo $4$, then $1, \sqrt{A}$ form a $\mathbb{Z}$-basis of the integers in $\mathbb{Q}_2(\sqrt{A})$, but that if $A \equiv 1$ then $\alpha = (1 + \sqrt{A})/2$ is also integral, and in fact $1$ and $\alpha$ make a basis. This section will explain what happens more generally in local quadratic extensions.

Suppose $A \neq 0$ to be an integer in $\mathcal{O}_F$, and let $E = F[x]/(x^2 - A)$. Define $\sqrt{A}$ to be the image of $x$ in $E$.

What is the maximal order in $E$?

The discussion will go by cases.

[1] $A \sim \omega^{2k+1}$.

This is the simplest case. If $B = A/\omega^{2k}$, then $\sqrt{B}$ is a generator of $\mathcal{O}_E$, and

- The pair $1, \sqrt{B}$ form a basis of $\mathcal{O}_E$ over $\mathcal{O}_F$.

Otherwise, $A \sim \omega^{2k}$. We may replace $A$ by $A/\omega^{2k}$, and

- From now on assume $A$ to be a unit in $\mathcal{O}_F$.

[2] Suppose $p$ to be odd. Then $A$ is a square root if and only if its image modulo $p$ is a square, and if it is not a square then $E/F$ is the unique unramified quadratic extension.

So from now on, suppose $p = 2$. What happens now depends on the square-free normal form $\alpha$ of $A$. If $\alpha = 1$, then $A$ is a square and $\mathcal{O}_E = \mathcal{O}_F \oplus \mathcal{O}_F$.

[3] If $\alpha = 1 + 4x$ with $x \neq 0$ in $E$, let

$$\gamma = \frac{1 - \sqrt{\alpha}}{2}.$$  

It satisfies the equation

$$\gamma^2 - \gamma + \frac{1 - \alpha}{4} = 0,$$

and $E$ is the unramified extension of $F$. In this case $\mathcal{O}_E = \mathcal{O}_F[\gamma]$.

[4] Suppose $\alpha - 1 \sim \omega^{2k+1}$ with $k \leq e_0 - 1$. Set

$$\gamma = \frac{1 - \sqrt{\alpha}}{\omega^k}.$$

Then $\gamma$ is a root of the Eisenstein polynomial

$$x^2 + \left(\frac{2}{\omega^k}\right)x + \left(\frac{1 - A}{\omega^{2k}}\right).$$

and $\mathcal{O}_E = \mathcal{O}_F[\gamma]$.

Examples. Let $F = \mathbb{Q}_2$, $A$ a unit. Representatives of $U_F/U_F^2$ are $u = \pm 1, \pm 3$, and of $F^\times/(F^\times)^2$ these and the $2u$. The integers in the case of $A = -3$ have as basis $1, \zeta_3 = (-1 + \sqrt{-3})/2$. This is the unramified extension. In all other cases $1, \sqrt{A}$ make up a basis of $\mathcal{O}_E$. Note that in the case $A - 1 \sim \omega^{2k+1}$ we must have $k = 0$ since every element in $1 + (8)$ is a square, so that $2k + 1 < 3$. 

### 3. Different and trace

Suppose for the moment that $F$ is any $p$-adic field and $E/F$ is any finite field extension, say of degree $n$. Any element $\alpha$ of $E$ acts by multiplication on $E$ as an $F$-linear operator. The trace $\text{Tr}_{E/F}(x)$ is defined to be the trace of this operator. If the characteristic polynomial of this operator is

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

then $a_{n-1}$ is the trace of $\alpha$. If $E/F$ is Galois, this is also the sum of the conjugates of $x$.

A **lattice** in $E$ is any finitely generated $o_F$-module in $E$ that spans $E$ as a vector space. It is necessarily free over $o_F$. If $a$ is any lattice in $E$, its dual is the set

$$a^\perp = \{ x \in E \mid \text{Tr}(xa) \subseteq o_F \}.$$  

If $a = o_E$, its dual is a fractional ideal over $o_E$, and its inverse is the relative different $\vartheta_{E/F}$. This is an ideal of $o_E$.

I recall that an **order** of $E$ is a lattice that is also a ring. It is necessarily contained in $o_E$.

#### 3.1. Lemma

Suppose $r = o_F[\alpha]$ to be any monogenic order of $E$ with characteristic polynomial $f(T)$. Then $r^\perp$ is the $r$-module generated by $1/f'(\alpha)$.

**Proof.** The Lemma follows from the equations

$$\text{Tr} \left( \delta_i \right) = \begin{cases} 0 & \text{if } i < n-1 \\ 1 & \text{if } i = n-1 \end{cases},$$

where $\delta_i = \alpha^i / f'(\alpha)$.

This follows from the familiar partial fraction decomposition

$$\frac{1}{f(T)} = \sum_i \frac{1}{f'(x_i)} \cdot \frac{1}{T-x_i}$$

since the left hand side may be expressed as

$$\frac{1}{T^n} \cdot \sum_j c_j / T^{n-j} = \frac{1}{T^n} + \frac{a_1}{T^{n+1}} + \cdots$$

and the right as

$$\sum_i \frac{1}{f'(x_i)} \cdot \frac{1}{T} \cdot \frac{1-x_i/T}{1-x_i} = \sum_i \frac{1}{f'(x_i)} \left( \frac{1}{T} + \frac{x_i}{T^2} + \frac{x_i^2}{T^3} + \cdots \right).$$

From now, fix $F$ and let $E/F$ be a quadratic extension. The conjugation in $E$ is $x \mapsto \overline{x}$.

#### 3.2. Lemma

If $o_E = o[\alpha]$ then $\vartheta_{E/F}$ is the ideal generated by $\alpha - \overline{\alpha}$.

**Proof.** Because if $\alpha$ is a root of the quadratic polynomial $f(x) = x^2 - ax + b$

$$f'(\alpha) = 2\alpha - a = \alpha - \overline{\alpha}.$$  

The main point of the different is this:

#### 3.3. Corollary

Suppose $\vartheta_{E/F} = p_E^m$ and $p_F = p_E^e$ ($e = 1$ or $2$). Then (a) $m = 0$ if and only if $e = 1$; (b) $m = 1$ if and only if $p$ is odd and $e = 2$; and (c) $m \geq 2$ if and only if $p = 2$ and $e = 2$. 
Local quadratic extensions

Proof. If \( E/F \) is ramified, then \( \varpi_E \) can be taken as \( \alpha \) in the Lemma, so that \( \vartheta_{E/F} \) is generated by \( 2\varpi_E - a \). If \( p \) is odd this has order 1, while if \( p = 2 \) both terms have order 2.

Very explicit formulas are not difficult, given results in the previous section.

3.4. Corollary. (a) The different \( \vartheta_{E/F} \) of the unramified extension of \( F \) is \( \mathfrak{o}_E \). (b) If \( p \) is odd and \( A \sim \varpi_F \) then \( \vartheta_{E/F} = \mathfrak{p}_F \). (c) If \( p = 2 \) and \( A - 1 \sim \varpi_F^{2k+1} \) with \( 0 \leq k < e_\circ \) the different is \( (2/\varpi_F^k) = \mathfrak{p}_F^{e_\circ-k} \). (d) If \( A \sim \varpi_F \) then \( \vartheta_{E/F} = 2p \).

Later on we shall need some simple consequences.

• From now on, assume \( e = 2 \) and let \( m \) be the order of \( \vartheta_{E/F} \).

3.5. Lemma. For all \( \ell \)  
\[
\text{TR}: \frac{\mathfrak{p}_E^{m+2\ell}}{\mathfrak{p}_E^{m+2\ell+2}} \twoheadrightarrow \frac{\mathfrak{p}_F^{m+\ell}}{\mathfrak{p}_F^{m+\ell+1}}.
\]

Proof. The definition of \( \vartheta_{E/F} \) tells us that \( \text{TR} \mathfrak{p}_E^{-m} = \mathfrak{o}_F \) and \( \text{TR} \mathfrak{p}_E^{-m-1} = \mathfrak{p}_F^{-1} \). Multiplying the second by \( \varpi_E \), we see that \( \text{TR} \mathfrak{p}_E^{-m+1} = \mathfrak{o}_F \). The trace is \( F \)-linear, so that upon multiplying both now by \( \mathfrak{p}_F^{m+\ell} = \mathfrak{p}_E^{2m+2\ell} \) we get

\[
\text{TR} \mathfrak{p}_E^{m+2\ell} = \mathfrak{p}_F^{m+\ell}
\]

Because of this, we have an induced map of \( F \)-linear spaces

\[
(3.6) \quad \text{TR}: \frac{\mathfrak{p}_E^{m+2\ell}}{\mathfrak{p}_E^{m+2\ell+2}} \twoheadrightarrow \frac{\mathfrak{p}_F^{m+\ell}}{\mathfrak{p}_F^{m+\ell+1}}.
\]

We can describe it explicitly. If \( E/F \) is ramified then \( \varpi_F^{m+\ell} \delta_i \) lies in \( \mathfrak{p}_E^{m+2\ell+i} \) since \( \delta_i \) lies in \( \mathfrak{p}_E^{-m+i} \), and the two \( \delta_i \) make up a basis of \( \mathfrak{p}_E^{m+2\ell}/\mathfrak{p}_E^{m+2\ell+2} \).

3.7. Proposition. For all \( \ell \) in \( \mathbb{Z} \) the tow elements \( \varpi_F^{m+\ell} \delta_i \) make a basis of \( \mathfrak{o}_E^{m+2\ell}/\mathfrak{o}_F^{2+2\ell+2} \), and the map \( (3.6) \) takes

\[
\varpi_F^{m+\ell} \delta_0 \mapsto 0
\]

\[
\varpi_F^{m+\ell} \delta_1 \mapsto \varpi_F^{m+\ell}.
\]

Proof. Immediate from Lemma 3.1.

4. Norms and units

Define \( \text{NM} = \) the norm map from \( E \) to \( F \): \( x \mapsto x^F \).

In this section I’ll investigate how the norm map \( x \mapsto x^F \) from \( E^\times \) to \( F^\times \) behaves on the unit group \( U_E \) with respect to the filtration by the congruence subgroups \( U_E^{[n]} \). In the next I’ll deal with the relations between the Galois group of \( E/F \) and the norm.

If \( E/F \) is ramified, we know that \( \mathfrak{o}_E = \mathfrak{o}_F[\varpi_E] \). Let \( \varpi_\bullet = \text{NM}(\varpi_E) \), which is a generator of \( \mathfrak{p}_F \). Continue to define \( m \) by the condition that \( \vartheta_{E/F} = \mathfrak{p}_F^m \).

I’ll begin with the simplest cases, then spend most of the time on the relatively complicated case in which \( E/F \) is ramified and the residue characteristic is 2.
The basic formula to be applied is very simple. Suppose \( k \geq 1 \). Every element in \( U_E^{[k]} \) is of the form \( 1 + x \omega_E^k \) with \( x \in \mathfrak{o}_E \), and

\[
NM(1 + x \omega_E^k) = 1 + \text{TR}(x \omega_E^k) + NM(x \omega_E^k).
\]

(4.1)

- In the simplest case, the extension \( E/F \) is the unique unramified extension of \( F \). This means that \( \omega_E = \omega_F \) and that \( F_E \) is a quadratic extension of \( F_F \). The norm takes

\[
U_E^{[k]} \to U_F^{[k]}
\]

for all \( k \geq 1 \), hence induces maps

\[
\frac{U_E^{[k]}}{U_E^{[1]}} \to \frac{U_F^{[k]}}{U_F^{[1]}} \quad \quad (a)
\]

\[
\frac{U_E^{[k]}}{U_E^{[k-1]}} \to \frac{U_F^{[k]}}{U_F^{[k-1]}} \quad \quad (b)
\]

It follows from (4.1) that the map in (a) may be identified with the residual norm map from \( F_E^x \) to \( F_F^x \). It also follows from it that in (b) is a non-zero multiple of the residual trace from \( F_E \) to \( F_F \). Since both the residual norm and the residual trace are both surjective:

4.2. Proposition. If \( E/F \) is unramified, the norm from \( U_E \) to \( U_F \) is surjective.

- Now suppose \( E/F \) to be ramified, which is to say \( e = 2 \). If \( p \) is odd then \( m = 1 \), but \( m \geq 2 \) if \( p = 2 \). The cases \( p = 2 \) and \( p \) odd behave rather differently, but they do have some features in common.

I am concerned at the moment with only the range \( k \geq m \). Since \( NM(p_E^{m+2\ell}) \subseteq p_F^{m+2\ell} \) and \( TR(p_E^{m+2\ell}) = p_F^{m+\ell} \) for \( \ell \geq 0 \), we see that

\[
NM(1 + p_E^{m+2\ell}) \subseteq 1 + p_F^{m+\ell}.
\]

We therefore have maps induced on the quotients

\[
(1 + p_E^{m+2\ell})/(1 + p_F^{m+2\ell+2}) \to (1 + p_E^{m+\ell})/(1 + p_F^{m+\ell+1}).
\]

Each space on the left is annihilated by \( p_F \), so in applying (4.1) we may take \( x \) to be in \( \mathfrak{o}_F \). The cases \( \ell = 0 \), \( \ell > 0 \) are slightly different. For \( \ell = 0 \):

\[
1 + x \omega_F^m \delta_1 \to 1 + x^2 NM(\omega_F)^m
\]

\[
1 + x \omega_F^m \delta_1 \to 1 + x \text{TR}(\omega_F^m \delta_1)
\]

\[
= 1 + x \omega_F^m.
\]

For \( \ell \geq 1 \)

\[
1 + x \omega_F^m \delta_0 \to 1
\]

\[
1 + x \omega_F^m \delta_1 \to 1 + x \omega_F^m.
\]

(These are modulo \( p_F^{m+\ell} \).) In all cases, the map is surjective. Consequently:

4.3. Lemma. For \( \ell \geq 0 \) the norm map from \( U_E^{[m+2\ell]} / U_E^{[m+2\ell+2]} \) to \( U_F^{[m+\ell]} / U_F^{[m+\ell+1]} \) is surjective.

Hence:

4.4. Proposition. The norm map from \( U_E^{[m]} \) to \( U_F^{[m]} \) is surjective.

For use elsewhere I put here the following consequence of the equations above:

4.5. Proposition. If \( x \) lies in \( 1 + p^{m+2\ell+1} \) and \( NM(x) \equiv 1 \) modulo \( p^{m+\ell+1} \) then \( x \equiv 1 \) modulo \( p^{m+2\ell+2} \).
Now suppose \( p \) to be odd. The residue fields for \( E \) and \( F \) are the same, and the norm map on these is \( x \mapsto x^2 \). Since \( p \) is odd, this has kernel \( \pm 1 \) and cokernel also of size 2.

4.6. Proposition. If \( p \) is odd and \( E/F \) is ramified, an element of \( U_F \) is a norm if and only if its image in \( F_F \) is a square.

We are now reduced to the third case, by far the most interesting.

- I assume from now on in this section that \( E/F \) is ramified and the residue field characteristic is 2.

There are three parts to the rest of this discussion.

- Suppose \( k = 0 \). Since \( U = \mathfrak{o}^\times \) and \( U[1] = 1 + p \), both \( U_E/U_E[1] \) and \( U_E/U_E[1] \) may be identified with the units in the common residue field \( F_F^\times \). On this, the induced norm map takes \( x \) to \( x^2 \), which is an automorphism of the residue field.

- If \( 1 \leq k \leq m \), then (4.1) implies that \( NM(1 + p_E^k) \subseteq 1 + p_F^k \). For \( 1 \leq k \leq m - 1 \) we therefore have quotient maps
  \[
  (1 + p_E^k)/(1 + p_F^{k+1}) \longrightarrow (1 + p_F^k)/(1 + p_F^{k+1}) .
  \]

It takes
  \[
  1 + x \omega_E^k \longmapsto 1 + x^2 \omega_F^k .
  \]

so that:


- Now suppose \( k = m - 1 \). The map induced by the norm from from \( U_E[1] \) to \( U_F[1] \) takes
  \[
  1 + x \omega_E^{m-1} \longmapsto 1 + (\tau x + x^2) \omega_F^{m-1} .
  \]

for some unit \( \tau \). It can be computed explicitly from Proposition 3.7. The map \( x \mapsto \tau x + x^2 \) is a variant of the Artin-Schreier map, with kernel and cokernel both of order 2. Let \( \chi_F \) be the character of \( F \) whose kernel is the image of this map. Define the character \( \chi_E/F \) on \( U_E[1] \):
  \[
  \chi_E/F : 1 + x \omega_E^{m-1} \longmapsto \chi_F(x) .
  \]

Now suppose \( u \) to be an arbitrary element of \( U_F \). According to Proposition 4.4 there exists an element \( v \) of \( U_E \) such that \( NM(v) \cdot u \) lies in \( U_E[1] \). So we may now assume \( u \) in \( U_E[1] \).

If \( \chi_E/F(u) = 1 \), we can find an element \( v \) of \( U_E[1] \) such that \( NM(v) \cdot u \) lies in \( U_E \). But then according to Proposition 4.4 \( u \) itself will lie in the image of \( NM \).

If \( \chi_E/F(u) = -1 \) then \( u \) does not lie in the image of \( NM \), because if it did it would be the norm of some element in \( U_E[1] \), and by definition it is not.

This argument allows us to define a quadratic character \( \chi_E/F \) on all of \( U \) with the property that \( \chi_E/F(u) = 1 \) if and only if \( u \) is in \( NM(U_E) \).

The element \( \omega_* = NM(\omega_E) \) is a generator of \( p_F \). We can extend the character \( \chi_E/F \) to all of \( F_F^\times \) by specifying
  \[
  \chi_E/F(u \omega_*^m) = \chi_E/F(u) .
  \]

Then:

4.8. Theorem. An element \( x \) of \( F_F^\times \) is in the image of \( NM_E/F \) if and only if \( \chi_E/F(x) = 1 \).
5. Norms and the Galois group

We now know that the quotient $F^\times /\text{norm}(E^\times)$ has order 2. It is not a coincidence that the Galois group of $E/F$ is also of order 2. There is in fact a natural isomorphism of the two groups.

If $E/F$ is unramified, then $\mathfrak{w}_E$ generates the quotient. The isomorphism taking $\mathfrak{w}_F$ to conjugation is the isomorphism we want.

What about when $E/F$ is ramified? When $p$ is odd, the quotient may be identified with the cokernel of the map from $F^\times$ to itself taking $x$ to $x^2$.

When $p = 2$, it may be identified with the cokernel of the map from $(1 + pE)^{m-1}/(1 + pF)^m$ taking

$$1 + x\mathfrak{w}_E^{m-1} \mapsto 1 + (\tau_0 x + \varepsilon^{m-1}x^2)\mathfrak{w}_E^{m-1}.$$ 

or in other words the cokernel of the additive map from $F$ to itself taking $x$ to $u_0 x + \varepsilon^{m-1}x^2$. In both cases, the kernel at hand is that of an algebraic map. It turns out—that for such maps the kernel and the cokernel are canonically isomorphic. But in both cases the kernel can be identified with the Galois group $G = \{1, \sigma\}$. If $p$ is odd then $\mathfrak{w}_E$ can be chosen to be $\sqrt{A}$ for some $A$ generating $pF$, and the map from $G$ to $F^\times$ takes

$$\sigma^i \mapsto \sigma^i(\sqrt{A}) = (-1)^i.$$ 

The image of $\sigma$ is $-1$, generates the kernel of $x \mapsto x^2$.

If $p = 2$, we know that $\mathfrak{w}_E - \mathfrak{w}_E \sim \mathfrak{w}_E^m$. We again map

$$\sigma^i \mapsto \sigma^i(\mathfrak{w}_E)/\mathfrak{w}_E.$$ 

so that

$$\sigma \mapsto \frac{\mathfrak{w}_E}{\mathfrak{w}_E}$$

and

$$\frac{\mathfrak{w}_E}{\mathfrak{w}_E} = 1 \sim \mathfrak{w}_E^{m-1},$$

so the image of $G$ is contained in $U^{m-1}$. But the norm of $\mathfrak{w}_E/\mathfrak{w}_E$ is 1, so here also it generates the kernel we are looking at.

Remark. The more general situation in which $E/F$ is cyclic of prime order is not much more difficult to deal with. Also, much of the argument goes through when the residue field is assumed to be algebraically closed and $E/F$ of degree equal to the residue field characteristic. In that case the conclusion is that $F^\times = \text{NM}(E^\times)$. This leads to one of the fundamental facts of local class field theory, that all elements of the Brauer group of a local field split over its unramified extension.

Algebraic homomorphisms of finite fields. (i) Suppose $n \geq 1$, and let $f$ be the homomorphism $x \mapsto x^n$ from $F^\times$ to itself. We may factor $n = ap^b$ with $a$ relatively prime to $p$. The kernel $\kappa$ of $f$ in $F^\times$ is cyclic of order $a$.

5.1. Lemma. In these circumstances, if all the elements in $\kappa$ lie in $F$, then the kernel and the cokernel of $f|F^\times$ are isomorphic.

Proof. We have an exact sequence of modules over the Galois group $G = \text{Gal}(F/F)$, which is generated by the Frobenius automorphism $x \mapsto x^q$:

$$1 \rightarrow \kappa \rightarrow F^\times \rightarrow F^\times \rightarrow 1.$$
This leads to a long exact sequence of cohomology
\[ 1 \longrightarrow \kappa^{\mathbb{G}} \longrightarrow \mathbb{F}^x \longrightarrow \mathbb{F}^x \longrightarrow H^1(G, \kappa) \longrightarrow H^1(G, \mathbb{F}^x). \]

Any group $H^1(G, A)$ is isomorphic to the quotient of $A$ by the subgroup of elements $a^\mathbb{G}/a$. But the map $x \mapsto x^{-1}$ is surjective so the last term in this exact sequence vanishes. By assumption, $\mathbb{G}$ acts trivially on $\kappa$, so that $\kappa^{\mathbb{G}} = \kappa$. Furthermore, $H^1(\text{Gal}, \kappa) = \kappa/(\mathbb{G} - 1)\kappa = \kappa$.

(ii) Now suppose $f$ to be an additive homomorphism from $\mathbb{F}$ to itself. It can be expressed in the form
\[ f(x) = x^{\mathbb{F}^m}(a_0x + a_1x^p + \cdots + a_kx^{p^k}) \]
with $a_0 \neq 0$. In this case the size of the kernel in $\mathbb{F}$ is $p^k$. A slight modification of the previous proof gives:

5.2. Lemma. In these circumstances, if $\kappa = \kappa^{\mathbb{G}}$ then the kernel and the cokernel of $f|\mathbb{F}$ are isomorphic.

6. Appendix. Hensel’s Lemma

In this section, suppose $f$ to be a polynomial in $\sigma[x] = \sigma[x_1, \ldots, x_d]$, $\overline{f}$ its image in $\mathbb{F}[x]$. If $a$ lies in $L = \sigma^d$ and $f(a) = 0$ then the image $a$ of $a$ in $\mathbb{F}^d$ will be a root of $\overline{f}$. Conversely, suppose $a$ in $\sigma^d$ with $\overline{f}(a) = 0$. That is to say, $f(a) \equiv f_1 0$. Is there $\alpha$ in $\sigma^d$ with $f(\alpha) = 0$ and $\alpha \equiv f_1 a$? One very simple example that we shall be concerned with later on is $f: x \mapsto x^2$. Another will be the norm map from a quadratic extension of $\mathbb{F}$.

Let $\nabla f$ be the derivative of $f$, which for each $a$ in $L$ is a linear function on $L$ with values in $\sigma$. Thus for $x$ in $L$, $h$ in $\sigma$
\[ |f(a + hx) - (f(a) + h\nabla f(a), x)| \leq C_2|h|^2 \]
for some constant $C_2$ bounding higher derivatives of $f$ at $a$.

The Non-Singular Case. Suppose for the moment that $a$ in $\mathbb{F}^d$ satisfies $f(a) \equiv f_1 0$, and that $\nabla f(a) \neq f_1 0$ modulo $p$. Thus $\nabla f(a)$ induces a non-trivial $\mathbb{F}$-linear map $\nabla f(a)$ from $L/pL$ to $\mathbb{F}$. Can we find $a + hx$ with $h$ in $p$ and $x$ in $\sigma^d$ such that $f(a + hx) = 0$? A solution will be found by an approximation process. We shall find inductively elements $a_n$ with $a_1 = a$, $a_{n+1} \equiv a_n$, $f(a_n) \equiv f_1 0$. Suppose, therefore, that $f(a_n) \equiv f_1 0$. Then
\[ f(a_n + x^n) = f(a_n) + x^n\langle \nabla f(a), x \rangle + O(x^{2n}). \]
But by assumption $f(a_n)/x^n$ lies in $\sigma$, so that if
\[ \langle \nabla f(a), x \rangle = -\frac{f(a_n)}{x^n}, \quad a_{n+1} = a_n + x^n \]
then $f(a_{n+1}) \equiv f_1 0$. There are $q^{d-1}$ possibilities for $x$ modulo $pL$ and hence also for $a_{n+1}$ modulo $p^{n+1}L$. The sequence $(a_n)$ converges to a root $\alpha$ of $f$. Hence:

6.1. Proposition. (Hensel’s Lemma, simple case) Suppose $a$ in $L$, $\overline{f}(a) = 0$, $\nabla f(a) \neq 0$. Then there exists $\alpha$ with $\overline{\alpha} = \overline{a}$ and $f(\alpha) = 0$.

Because the number of possible choices multiplies by $q^{d-1}$ at each step:

6.2. Corollary. Suppose $f$ in $\sigma[x]$ has the property that whenever $f(a) = 0$ then $\nabla f(a) \neq 0$. Then for every $n \geq 1$ the ratio
\[ \frac{|\{a \in L/x^n L \mid f(a) \equiv f_1 0\}|}{q^{n(d-1)}} \]
is equal to
\[ \frac{|\{\overline{\alpha} \in F^d \mid \overline{f}(a) = 0\}|}{q^{d-1}}. \]
Example. Let \( d = 1, f(x) = x^d - x \). Every element of \( F \) is a root of \( f \). Furthermore, \( f' = -1 \). Hence for every element \( a \) in \( F \) there exists a unique \( \alpha \) in \( \mathfrak{o} \) such that \( \alpha^d = \alpha, \overline{\alpha} = a \). This is the Teichmüller lift of \( a \).

Example. Suppose \( p \neq 2, d = 1, f(x) = x^2, u \) in \( \mathfrak{o}^\times \). The square roots of \( u \) in \( \mathfrak{o}^\times \) are in bijection with the square roots of its image in \( F \).

**The Singular Case.** What if \( \nabla_f(a) \) reduces to 0 modulo \( p \)? Things will be a little more complicated. For example, \( x^2 - 5 = 0 \) has a root modulo 2, even modulo 4, but not modulo 8. The equation \( x^2 = 1 \) has 4 solutions modulo 8, namely \( x = \pm 1, \pm 3 \), but modulo 16 the solutions are \( \pm 1, \pm 7 \), which reduce modulo 8 only to \( \pm 1 \).

Suppose at least that \( f \) is not too singular at \( a \) in the sense that the hypersurface \( f(x) = 0 \) is not singular there. Then for some \( N \) we know that \( \nabla_f(a) \equiv_{N-1} 0 \) but \( \nabla_f(a) \not\equiv_N 0 \). That is to say, the map

\[
(\nabla_f(a), x) = \frac{(\nabla_f(a), x)}{\overline{\omega}^{N-1}}
\]

induces a well defined, non-trivial, \( F \)-linear map from \( L/\mathfrak{p}L \) to \( \mathfrak{o}/\mathfrak{p} \). In the equation

\[
f(a + \overline{\omega}^k x) = f(a) + \overline{\omega}^{k+N-1}(\nabla_f(a), x) + O(\overline{\omega}^{2k})
\]

all coefficients are therefore integral. If \( k \geq N \) then \( 2k > k + N - 1 \), so the error term is \( O(p^{k+N}) \). Hence:

**6.3. Proposition.** Suppose \( \nabla_f(a) \equiv 0 \mod p^{N-1} \) but not \( \mod p^N \). Then for every \( k \geq 0 \) the induced map

\[
\frac{a + p^{N+k}L}{a + p^{N+k+1}L} \rightarrow \frac{f(a) + p^{2N+k-1}L}{f(a) + p^{2N+k}}
\]

is a surjective \( F \)-linear map.

**6.4. Corollary.** Suppose \( k \geq 0, a \) in \( \mathfrak{o}^d \) such that \( f(a) \equiv_{2N+k-1} 0 \). There exists \( \alpha \) in \( L \) such that \( \alpha \equiv_{N+k} a \) with \( f(\alpha) = 0 \).

**6.5. Corollary.** Every \( a \equiv 1 \mod 4p \) has a square root in \( 1 + 2p \).

If \( p \) is odd, the condition on \( a \) is equivalent to requiring only that \( a \equiv 1 \).

**6.6. Corollary.** Suppose \( \nabla_f(a) \neq 0 \) for every \( a \) in \( L \) such that \( f(a) = 0 \). Then the limit

\[
\lim_{n \to \infty} \frac{|f^{-1}(p^nL)|}{q^n(d-1)}
\]

exists.

Of course, each inverse limit could be empty.

Roughly speaking, the important point is that if \( f \) is not too singular at \( a \) and we look close enough, the map \( f \) becomes approximately linear.

**Example.** Look at \( d = 2, F = \mathbb{Q}_2, f : x \rightarrow x^2, a = 1 \). The solutions of \( x^2 \equiv 1 \mod 2^n \) for \( n \geq 3 \) are the \( a = \pm 1 \mod 2^{n-1} \), making 4 solutions modulo \( 2^n \). Only two of these lift to solutions modulo \( 2^{n+1} \).

**Example.** If \( p = 2, f = x^2 + y^2 - 1 \), the limiting ratio in Corollary 6.6 is 2.

When \( f \) is a non-degenerate quadratic form, some interesting things happen even in the range \( 1 \leq k \leq N \).

**7. References**
