Local quadratic extensions

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

Suppose F to be a $\mathfrak{p}$-adic field of characteristic other than 2, E a separable quadratic extension field. 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

NOTATION. 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 $\mathfrak{o}_F$
ϖ_F = a generator of $\mathfrak{p}_F$
$U_F = \mathfrak{o}_F^\times$ (the units of $\mathfrak{o}_F$)
$\mathbb{F}_F = \mathfrak{o}_F/\mathfrak{p}_F$
$q = |\mathbb{F}_F|$ (a power of a prime p)
$\mathfrak{F}$ = the Frobenius automorphism $x \mapsto x^q$ of $\overline{\mathbb{F}}$, which fixes elements of $\mathbb{F}$.

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 $n \ge 0$ let

$$U_F^{[n]} = 1 + \mathfrak{p}_F^n ,$$

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

Certain methods of computation in F depend on some choices. Let θ be any section of the projection $\mathfrak{o} \to \mathbb{F}$, so that ***F*** is made up of representatives modulo $\mathfrak{p}$. Every element of $\mathfrak{o}$ can then be written uniquely in a **normal form**

$$f_0 + f_1\varpi + f_2\varpi^2 + \cdots$$

with each f_i in ***F***. In practice, one computes only in the finite rings $\mathfrak{o}/\mathfrak{p}^n$.

There is actually a canonical section. As I'll recall in an appendix, Hensel's Lemma implies that for every x in $\mathbb{F}_F$ there exists a unique $y = \tau(x)$ in $\mathfrak{o}$ reducing to x modulo $\mathfrak{p}_F$, such that $y^q = y$. Such liftings are called **Teichmüller** elements. Again, in practice, one works with finite approximations to Teichmüller elements. The main consequence for us is that the group U_F is isomorphic to $\mathbb{F}_F^\times \times (1 + \mathfrak{p}_F)$.

If the characteristic of $\mathbb{F}$ is 2, define constants $\boldsymbol{e} \geq 1$ in $\mathbb{N}$ and $\boldsymbol{u} \neq 0$ in $\mathbb{F}$ by the requirement that $2 \equiv_{\boldsymbol{e}+1} \boldsymbol{u}\varpi^{\boldsymbol{e}}$. The map $x \mapsto x^2 + x$ is an $\mathbb{F}_2$-linear map from $\mathbb{F}$ to itself, with both kernel and cokernel of size 2. Let $\mathcal{E}$ be a couple of representatives in $\mathbb{F}$ of the cokernel, with one of them equal to 0.

Notation will be similar for the quadratic extension E. I'll often ignore subscripts when referring to F.

1. Squares [squares.tex]

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

[graded-units] **1.1. Lemma.** *The projection $\mathfrak{o}\to\mathfrak{o}/\mathfrak{p}$ induces an isomorphism of $U/U^{[1]}$ with $\mathbb{F}^\times$, and for $n\ge 1$ the map $x\longmapsto 1+x\varpi^n$ induces an isomorphism of $\mathbb{F}$ with $U^{[n]}/U^{[n+1]}$.*

♡ [graded-units] The second isomorphism in Lemma 1.1 is not at all canonical, since for $n\ge 1$ it depends on a choice of ϖ. The canonical isomorphism is with $\mathfrak{p}^n/\mathfrak{p}^{n+1}$, which may be identified with $\otimes^n(\mathfrak{p}/\mathfrak{p}^2)$.

♡ [squares-units] The starting point of the investigation is Corollary 6.5 (in the Appendix), which I repeat here:

[congruence-squares] **1.2. Proposition.** *If $A\equiv_{2\boldsymbol{e}+1}1$, then A is a square in U_F.*

I cannot resist offering a second proof.

[square-root-series] **1.3. Lemma.** *For $\alpha\in 4\mathfrak{p}_F$, the binomial series*

$$
\begin{aligned}
(1+\alpha)^{1/2} &= 1+\frac{1}{2}\cdot\alpha+\frac{(1/2)(1/2-1)}{2}\cdot\alpha^2+\frac{(1/2)(1/2-1)(1/2-2)}{3!}\cdot\alpha^3+\cdots \\
&= 1+\frac{1}{2}\cdot\alpha+\frac{(-1)}{2^2\cdot 2}\cdot\alpha^2+\frac{(-1)(-3)}{2^3\cdot 3!}\cdot\alpha^3+\cdots
\end{aligned}
$$

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

Proof. If p is odd, then 2 is invertible and the coefficient of each α^k lies in $\mathfrak{o}_F$. Hence the series clearly converges for α in $\mathfrak{p}_F$. If $p=2$, we need to know that

$$
\mathrm{ord}_2(n!)=\left(\sum\nolimits_k\left\lfloor\frac{n}{2^k}\right\rfloor\right)<\frac{n}{2}\cdot\left(\frac{1}{1-1/2}\right)=n\,.
$$

Remark. A more rapid convergence is provided in principle by Newton's approximation sequence

$$
\begin{aligned}
x_{n+1} &= x_n-h_n \qquad \left(h_n=\frac{x_n^2-A}{2x_n}\right) \\
&= \frac{1}{2}\left(x_n+\frac{A}{x_n}\right)
\end{aligned}
$$

with an initial estimate

$$
x_0=1+(y/\boldsymbol{u})\varpi^{\boldsymbol{e}+1}\quad (A=1+4y\varpi)\,.
$$

This converges quadratically, since

$$
x_{n+1}^2-A=h_n^2\,.
$$

This doesn't work all that well in practice, though.

Because of the Teichmüller section the group U/U^2 is isomorphic to $\mathbb{F}^\times/(\mathbb{F}^\times)^2\times(1+\mathfrak{p})/(1+\mathfrak{p})^2$. If p is odd, then every element of $1+\mathfrak{p}$ is a square, and U/U^2 is isomorphic to $\mathbb{F}^\times/(\mathbb{F}^\times)^2$.

- *From now on in this section I'll assume that $p=2$.*

Let $V=1+\mathfrak{p}_F$ and $\overline{V}=V/V^{[2\boldsymbol{e}+1]}$. Since U/U^2 is isomorphic to $\mathbb{F}^\times/(\mathbb{F}^\times)^2\times(1+\mathfrak{p})/(1+\mathfrak{p})^2$, we shall need only to describe V/V^2. The Lemma tells us that being a square modulo $\mathfrak{p}^{2\boldsymbol{e}+1}$ is equivalent to being a square in V. Hence the canonical projection from V/V^2 to $\overline{V}/\overline{V}^2$ is an isomorphism, and we need only to describe this latter (finite) group.

[sq-free] **1.4. Proposition.** *The natural map*

$$
1+\boldsymbol{F}\varpi+\boldsymbol{F}\varpi^3+\cdots+\boldsymbol{F}\varpi^{2\boldsymbol{e}-1}+4\mathcal{E}\longrightarrow\overline{V}/\overline{V}^2
$$

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 $\boldsymbol{F}$ and ϖ. The proof will be constructive, and in effect will show how to compute for every element of $1+\mathfrak{p}$ its unique square-free normal form. This will allow an explicit enumeration of $F/(F^\times)^2$ and thus also a classification of quadratic extensions of F.

The proof will come down to a counting argument, and will be in several steps. For a start I display the basic equation

[square] (1.5)
$$(1+x\varpi^i)^2 = 1 + 2x\varpi^i + x^2\varpi^2 \,.$$

Step 1. The order of the middle term on the right is $k+\boldsymbol{e}$, while that of the third is $2i$. If $i<\boldsymbol{e}$, then ♡ **[square]** $2i < i+\boldsymbol{e}$, so (1.5) gives us a map

$$\begin{aligned}(1+\mathfrak{p}^i)/(1+\mathfrak{p}^{i+1}) \longrightarrow (1+\mathfrak{p}^{2i})/(1+\mathfrak{p}^{2i+1}) \subset (1+\mathfrak{p}^{2i-1})/(1+\mathfrak{p}^{2i+1})\\ 1+x\varpi^i \longmapsto 1+x^2\varpi^{2i}\,.\end{aligned}$$

Since $x\mapsto x^2$ is an automorphism of $\mathbb{F}$ with itself, the image is exactly $(1+\mathfrak{p}^{2i})/(1+\mathfrak{p}^{2i+1})$.

Step 2. If $i=\boldsymbol{e}$, we still get a map

$$\begin{aligned}(1+\mathfrak{p}^{\boldsymbol{e}})/(1+\mathfrak{p}^{\boldsymbol{e}+1}) \longrightarrow (1+\mathfrak{p}^{2\boldsymbol{e}})/(1+\mathfrak{p}^{2\boldsymbol{e}+1} \subset (1+\mathfrak{p}^{2\boldsymbol{e}-1})/(1+\mathfrak{p}^{2\boldsymbol{e}+1})\\ 1+2x \longmapsto 1+4(x+x^2\,.\end{aligned}$$

but now the kernel has order two.

Step 3. The group $(1+\mathfrak{p})/(1+\mathfrak{p}^{\boldsymbol{e}+1}$ has order $q^{\boldsymbol{e}}$ and the group $(1+\mathfrak{p})/(1+\mathfrak{p}^{2\boldsymbol{e}+1}$ has order $q^{2\boldsymbol{e}}$. Summarizing, a simple argument about filtrations then shows that the size of $\overline{W}=\overline{V}^2$ is therefore $q^{\boldsymbol{e}}/2$, and that of $\overline{V}/\overline{W}$ is $2q^{\boldsymbol{e}}$.

Step 4. Since the number of square-free normal forms is also $2q^{\boldsymbol{e}}$, in order to prove the Proposition it suffices to come up with an algorithm that for any element in $1+\mathfrak{p}$ finds an element in square-free normal form equivalent to it modulo squares.

Step 5. I'll show now how this begins. Suppose given

$$1+x_1\varpi+y_2\varpi^2$$

with x_1 in $\boldsymbol{F}$, y in $\mathfrak{o}$. Write this as

$$(1+x_1\varpi)\left(\frac{1+y_2\varpi^2}{1+x\varpi}\right) = (1+x_1\varpi)(1+y_2\varpi^2+O(\varpi^3))\,.$$

Now
$$(1+a\varpi)^2\big(1+y_2\varpi^2+O(\varpi^3)\big) = \big(1+(a^2+y_2)\varpi^2+O(\varpi^3)\big)\,.$$

If we choose a such that $a^2+y_2\equiv_1 0$, this leads to

$$(1+a\varpi)^2(1+x_1\varpi+y_2\varpi^2) = 1+x_1\varpi+x_3\varpi^3+y_4\varpi^4+O(\varpi^5)$$

and we are one step closer to square-free normal form.

Step 6. We can keep going along these lines. Suppose given

$$1+x_1\varpi+x_3\varpi^3+\cdots+x_{2d-1}\varpi^{2d-1}+y_{2d}\varpi^{2d}$$

with each x_i in $\boldsymbol{F}$ and y_{2d} in $\mathfrak{o}$. If $d = \boldsymbol{e}$, then a simple multilication will reduce it to square-free normal form. If $d < \boldsymbol{e}$, then multiplicationby some $1 + x_{2i}\varpi^{2i}$ will bring it to the form

$$1 + x_1\varpi + x_3\varpi^3 + \cdots + x_{2d-1}\varpi^{2d-1} + x_{2d+1}\varpi^{2d+1} + y_{2d+2}\varpi^{2i+2}$$

If $d + 1 < \boldsymbol{e}$, we repeat the process, otherwise we perfom one more slightly different manipulation and we are through.

I repeat that *this gives us a way to tell whether any given element of $F^\times$ is a square, and also to list representatives of $F^\times/(F^\times)^2$.*

Example. Suppose $F = \mathbb{Q}_2(\varpi)$ with $\varpi^3 + 2\varpi + 2 = 0$. Here $\boldsymbol{e} = 3$, $2\boldsymbol{e} + 1 = 7$. The set $\mathcal{E} = \{0, 1\}$, and there are 4 square-free normal forms.

What is the square-free normal form of $A = 1 + \varpi^2$? The calculation goes:

$$\begin{aligned}
(1 + x\varpi)^2 A &= (1 + 2x\varpi + x^2\varpi^2)(1 + \varpi^2) \\
&= 1 + 2x\varpi + (x^2 + 1)\varpi^2 + 2x\varpi^3 + x^2\varpi^4 \\
&= 1 + 2\varpi + 2\varpi^2 + 2\varpi^3 + \varpi^4 \quad \text{(with } x = 1\text{)} \\
&= 1 + 2\varpi^3 \quad \text{(since } 2\varpi + 2\varpi^2 + \varpi^4 = 0\text{)} \\
&= 1 + (-\varpi^3 - 2\varpi)\varpi^3 \\
&\equiv_7 1 - \varpi^6 . \\
&\equiv_7 1 + \varpi^6 .
\end{aligned}$$

A character $\chi\colon F^\times \to \mathbb{C}^\times$ is said to have **conductor** $\mathfrak{p}^m$ if it is trivial on $1 + \mathfrak{p}^m$ but not trivial on $1 + \mathfrak{p}^{m-1}$. Conventionally, the trivial character is said to have conductor $\mathfrak{o}$.

[um-sq-dual] **1.6. Corollary.** *(a) For $1 \le k \le \boldsymbol{e}$ there are exactly $(q-1)q^k$ quadratic characters of conductor $\mathfrak{p}^{2k}$ and no quadratic characters of conductor $\mathfrak{p}^{2k-1}$; (b) there are exactly $q^{\boldsymbol{e}}$ characters of conductor $\mathfrak{p}^{2\boldsymbol{e}+1}$; (c) if $m \ge 1$ there are no characters of conductor $\mathfrak{p}^{2k+1+m}$.*

Since the quadratic characters are partitioned by their conductors, you can confirm this by the equation

$$1 + (q-1) + (q-1)q + \cdots + (q-1)q^{\boldsymbol{e}-1} + q^{\boldsymbol{e}} = 2q^{\boldsymbol{e}} .$$

2. Integers [basic.tex]

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 α make a basis. This section will explain what happens more generally in local quadratic extensions.

Suppose $A \neq 0$ to be an integer in $\mathfrak{o}_F$, 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] $A \sim \varpi^{2k+1}$.

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

- *The pair $1, \sqrt{B}$ form a basis of $\mathfrak{o}_E$ over $\mathfrak{o}_F$.*

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

- *From now on assume A to be a unit in $\mathfrak{o}_F$.*

[2] Suppose p to be odd. Then A is a square if and only if its image modulo $\mathfrak{p}$ 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 α of A. If $\alpha = 1$, then A is a square and $\mathfrak{o}_E = \mathfrak{o}_F \oplus \mathfrak{o}_F$.

[3] If $\alpha = 1 + 4x$ with $x \neq 0$ in $\mathcal{E}$, 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 $\mathfrak{o}_E = \mathfrak{o}_F[\gamma]$.

[4] Suppose $\alpha - 1 \sim \varpi^{2k+1}$ with $k < \boldsymbol{e}$. Set

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

Then γ is a root of the Eisenstein polynomial

$$x^2 + \left(\frac{2}{\varpi^k}\right)x + \left(\frac{1-\alpha}{\varpi^{2k}}\right)\,.$$

and $\mathfrak{o}_E = \mathfrak{o}_F[\gamma]$.

Examples. • Let $F = \mathbb{Q}_2$. 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 $1, \zeta_3 = (-1+\sqrt{-3})/2$, and this is the unramified extension. The cases in which $A = 2\varepsilon$ with ε odd are straightforward. Here are the remaining two cases, in which A is a non-square unit not congruent to -3 modulo 8:

A	Eisenstein generator
-1	$1+\sqrt{-1}$
3	$1+\sqrt{3}$

• Let F be the field in the example at the end of the previous section, with the generator satisfying the Eisenstein equation

$$\varpi^3 + 2\varpi + 2 = 0\,.$$

If $A = 1 + \varpi^2$, what can we say about the extension $F(\sqrt{A})$? Its square-free normal form is $1 + \varpi^6$, so it falls immediately into the case above in which E/F is unramified.

3. Trace and different [different.tex]

Suppose for the moment that F is any $\mathfrak{p}$-adic field and E/F is any finite field extension, say of degree n. Any element α of E acts by multiplication on E as an F-linear operator. The trace $\mathrm{TR}_{E/F}(x)$ 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 α. If E/F is Galois, this is also the sum of the conjugates of x.

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

$$\mathfrak{a}^\perp = \{x \in E \,|\, \mathrm{TR}(x\mathfrak{a}) \subseteq \mathfrak{o}_F\}\,.$$

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

I recall that an **order** of E is a lattice that is also a ring. It is necessarily contained in $\mathfrak{o}_E$.

[different] **3.1. Lemma.** *Suppose $\mathfrak{r} = \mathfrak{o}_F[\alpha]$ to be any monogenic order of E with characteristic polynomial $f(T)$. Then $\mathfrak{r}^\perp$ is the $\mathfrak{r}$ module generated by $1/f'(\alpha)$.*

Proof. The Lemma follows from the equations

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

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

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

and the right as

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

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

[diff-roots] **3.2. Lemma.** *If $\mathfrak{o}_E = \mathfrak{o}[\alpha]$ then $\vartheta_{E/F}$ is the ideal generated by $\alpha - \overline{\alpha}$.*

Proof. Because if α 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:

[ram-diff] **3.3. Corollary.** *Suppose $\vartheta_{E/F} = \mathfrak{p}_E^m$ and $\mathfrak{p}_F = \mathfrak{p}_E^e$ ($e = 1$ 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 $e = 2$.*

Proof. If E/F is ramified, then ϖ_E can be taken as α 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.

《new notation?》 Very explicit formulas are not difficult, given results in the previous section.°

[different-sqrt] **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** the different is $(2/\varpi_F^k) = \mathfrak{p}_F^{\mathbf{e}-k}$. (d) If $A \sim \varpi_F$ then $\vartheta_{E/F} = 2\mathfrak{p}$.*

Later on we shall need some simple consequences.

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

[image-trace] **3.5. Lemma.** *For all ℓ*

$$\mathrm{TR}\,\mathfrak{p}_E^{m+2\ell} = \mathfrak{p}_F^{m+\ell}\,.$$

Proof. The definition of $\vartheta_{E/F}$ tells us that $\mathrm{TR}\,\mathfrak{p}_E^{-m} = \mathfrak{o}_F$ and $\mathrm{TR}\,\mathfrak{p}_E^{-m-1} = \mathfrak{p}_F^{-1}$. Multiplying the second by ϖ_F, we see that $\mathrm{TR}\,\mathfrak{p}_E^{-m+1} = \mathfrak{o}_F$. 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

$$\begin{aligned} \mathrm{TR}\,\mathfrak{p}_E^{m+2\ell} &= \mathfrak{p}_F^{m+\ell} \\ \mathrm{TR}\,\mathfrak{p}_E^{m+2\ell+1} &= \mathfrak{p}_F^{m+\ell}\,. \end{aligned}$$

Because of this, we have an induced map of $\mathbb{F}$-linear spaces

[tr-dual] **(3.6)**
$$\mathrm{TR}\colon\ \mathfrak{p}_E^{m+2\ell}/\mathfrak{p}_E^{m+2\ell+2} \longrightarrow \mathfrak{p}_F^{m+\ell}/\mathfrak{p}_F^{m+\ell+1}\,.$$

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 δ_i lies in $\mathfrak{p}_E^{-m+i}$, and the two δ_i make up a basis of $\mathfrak{p}_E^{m+2\ell}/\mathfrak{p}_E^{m+2\ell+2}$.

♡ [vartheta] [tr-dual] **3.7. Proposition.** *For all ℓ in $\mathbb{Z}$ the tow elements $\varpi_F^m\delta_i$ make a basis of $\mathfrak{o}_E^{m+2\ell}/\mathfrak{p}_E^{2+2\ell+2}$, and the map (3.6) takes*

$$\begin{aligned} \varpi_F^{m+\ell}\delta_0 &\longmapsto 0 \\ \varpi_F^{m+\ell}\delta_1 &\longmapsto \varpi_F^{m+\ell}\,. \end{aligned}$$

♡ [different] *Proof.* Immediate from Lemma 3.1.

4. Norms and units [norm.tex]

Define

$$\mathrm{NM} = \text{the norm map from } E \text{ to } F\text{: } x \mapsto x\overline{x}\,.$$

In this section I'll investigate how the norm map $x \mapsto x\overline{x}$ 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 $\varpi_\bullet = \mathrm{NM}(\varpi_E)$, which is a generator of $\mathfrak{p}_F$. Continue to define m by the condition that $\vartheta_{E/F} = \mathfrak{p}_E^m$.

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 $1 + x\varpi_E^k$ with $x \in \mathfrak{o}_E$, and

[norm-unit-formula] **(4.1)**
$$\mathrm{NM}(1 + x\varpi_E^k) = 1 + \mathrm{TR}(x\varpi_E^k) + \mathrm{NM}(x\varpi_E^k)\,.$$

• In the simplest case, the extension E/F is the unique unramified extension of F. This means that $\varpi_E = \varpi_F$ and that $\mathbb{F}_E$ is a quadratic extension of $\mathbb{F}_F$. The norm takes

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

for all $k \geq 1$, hence induces maps

$$U_E/U_E^{[1]} \to U_F/U_f^{[1]} \qquad \text{(a)}$$
$$U_E^{[k-1]}/U_E^{[k]} \to U_F^{[k-1]}/U_F^{[k]}\,. \qquad \text{(b)}$$

♡ [norm-unit-formula] It follows from (4.1) that the map in (a) may be identified with the residual norm map from $\mathbb{F}_E^\times$ to $\mathbb{F}_F^\times$. It also follows from it that in (b) is a non-zero multiple of the residual trace from $\mathbb{F}_E$ to $\mathbb{F}_F$. Since both the residual norm and the residual trace are both surjective:

[unram-norm] **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 $\mathrm{NM}(\mathfrak{p}_E^{m+2\ell}) \subseteq \mathfrak{p}_F^{m+2\ell}$ and $\mathrm{TR}(\mathfrak{p}_E^{m+2\ell}) = \mathfrak{p}_F^{m+\ell}$ for $\ell \geq 0$, we see that

$$\mathrm{NM}(1 + \mathfrak{p}^{m+2\ell}) \subseteq 1 + \mathfrak{p}^{m+\ell}\,.$$

We therefore have maps induced on the quotients

$$(1 + \mathfrak{p}_E^{m+2\ell})/(1 + \mathfrak{p}_E^{m+2\ell+2}) \longrightarrow (1 + \mathfrak{p}_E^{m+\ell})/(1 + \mathfrak{p}^{m+\ell+1})\,.$$

♡ [norm-unit-formula] Each space on the left is annihilated by $\mathfrak{p}_F$, 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 $\ell = 0$:

$$\begin{aligned} 1 + x\varpi_F^m\delta_0 &\longmapsto 1 + x^2\,\mathrm{NM}(\varpi_E)^m \\ 1 + x\varpi_F^m\delta_1 &\longmapsto 1 + x\,\mathrm{TR}(\varpi_F^m\delta_1) \\ &\qquad = 1 + x\varpi_F^m\,. \end{aligned}$$

For $\ell \geq 1$

$$\begin{aligned} 1 + x\varpi_F^m\delta_0 &\longmapsto 1 \\ 1 + x\varpi_F^m\delta_1 &\longmapsto 1 + x\varpi_F^m\,. \end{aligned}$$

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

[surjective-norm] **4.3. Lemma.** *For $\ell \ge 0$ 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:

[norm-m] **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:

[nm-one-filter] **4.5. Proposition.** *If x lies in $1+\mathfrak{p}^{m+2\ell+1}$ and $\mathrm{NM}(x) \equiv 1$ modulo $\mathfrak{p}^{m+\ell+1}$ then $x \equiv 1$ modulo $\mathfrak{p}^{m+2\ell+2}$.*

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 ± 1 and cokernel also of size 2.

[p-norm-odd] **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 $\mathbb{F}_F$ 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 $U^{[1]} = 1 + \mathfrak{p}$, both $U_E/U_E^{[1]}$ and $U_E/U_E^{[1]}$ may be identified with the units in the common residue field $\mathbb{F}_F^\times$. On this, the induced norm map takes x to x^2, which is an automorphism of the residue field.

♡ [norm-unit-formula] ◦ If $1 \le k \le m$, then (4.1) implies that $\mathrm{NM}(1+\mathfrak{p}_E^k) \subseteq 1 + \mathfrak{p}_F^k$. For $1 \le k \le m-1$ we therefore have quotient maps

$$(1+\mathfrak{p}_E^k)/(1+\mathfrak{p}_E^{k+1}) \longrightarrow (1+\mathfrak{p}_F^k)/(1+\mathfrak{p}_F^{k+1}) \,.$$

It takes

$$1 + x\varpi_E^k \longmapsto 1 + x^2\varpi_F^k \,.$$

so that:

[phase1] **4.7. Lemma.** *The norm map induces an isomorphism of $U_E/U_E^{[m-1]}$ with $U_F/U_F^{[m-1]}$.*

◦ Now suppose $k = m-1$. The map induced by the norm from from $U_E^{[m-1]}/U_E^{[m]}$ to $U_F^{[m-1]}/U_F^{[m]}$ takes

$$1 + x\varpi_E^{m-1} \longmapsto 1 + (\tau x + x^2)\varpi_\bullet^{m-1} \,.$$

♡ [vartheta-exp] for some unit τ. 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 $\chi_{\mathbb{F}}$ be the character of $\mathbb{F}$ whose kernel is the image of this map. Define the character $\chi_{E/F}$ on $U_E^{[m-1]}$:

$$\chi_{E/F}\colon\ 1 + x\varpi_E^{m-1} \longmapsto \chi_{\mathbb{F}}(x) \,.$$

♡ [norm-m] 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 $\mathrm{NM}(v)\cdot u$ lies in $U^{[m-1]}$. So we may now assume u in $U^{[m-1]}$.

If $\chi_{E/F} = 1$, we can find an element v of $U_E^{[m-1]}$ such that $\mathrm{NM}(v)\cdot u$ lies in $U_E^{[m]}$. But then according to
♡ [norm-m] 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 $U_E^{[m-1]}$, 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 $\mathrm{NM}(U_E)$.

The element $\varpi_\bullet = \mathrm{NM}(\varpi_E)$ is a generator of $\mathfrak{p}_F$. We can extend the character $\chi_{E/F}$ to all of $F^\times$ by specifying

$$\chi_{E/F}(u\varpi_\bullet^n) = \chi_{E/F}(u) \,.$$

Then:

[norm-mid] **4.8. Theorem.** *An element x of $F^\times$ is in the image of $\mathrm{NM}_{E/F}$ if and only if $\chi_{E/F}(x) = 1$.*

Examples. Let $F = \mathbb{Q}_2$. Representatives of $F^\times/(F^\times)^2$ are ± 1, ± 3, ± 2, ± 6. There are 6 ramified quadratic field extensions $F(\sqrt{A})$, and here is a table of norms:

A	norm form	norms
-1	$x^2 + y^2$	$1,\ -3,\ 2,\ -6$
3	$x^2 - 3y^2$	$1,\ -3,\ -2,\ 6$
2	$x^2 - 2y^2$	$1,\ -1,\ -2,\ 2$
-2	$x^2 + 2y^2$	$1,\ 3,\ 2,\ 6$
6	$x^2 - 6y^2$	$1,\ 3,\ -2,\ -6$
-6	$x^2 + 6y^2$	$1,\ -1,\ 6,\ -6$

5. Norms and the Galois group [galois.tex]

We now know that the quotient $F^\times/norm(E^\times)$ 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 ϖ_F generates the quotient. The isomorphism taking ϖ_F to conjugation is the isomorhism 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 $\mathbb{F}^\times$ to itself taking x to x^2.

When $p = 2$, it may be identified with the cokernel of the map from $(1+\mathfrak{p}_E^{m-1})/(1+\mathfrak{p}_E^m)$ to $(1+\mathfrak{p}_F^{m-1})/(1+\mathfrak{p}_F^m)^\circ$ taking 《u0?》

$$1 + x\varpi^{m-1} \longmapsto 1 + (\tau_0 x + \varepsilon^{m-1}x^2)\varpi_F^{m-1} \,.$$

or in other words the cokernel of the additive map from $\mathbb{F}$ to itself taking x to $u_0 x + \varepsilon^{m-1}x^2$. In both cases, the cokernel at hand is that of an algebraic map. It turns out—refer to the short discussion at the end of this section—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 ϖ_E can be chosen to be $\sqrt{A}$ for some A generating $\mathfrak{p}_F$, and the map from G to $\mathbb{F}^\times$ takes

$$\sigma^i \longmapsto \frac{\sigma^i(\sqrt{A})}{\sqrt{A}} = (-1)^i$$

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

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

$$\sigma^i \longmapsto \frac{\sigma^i(\varpi_E)}{\varpi_E} \,.$$

so that

$$\sigma \longmapsto \frac{\overline{\varpi}_E}{\varpi_E}$$

and

$$\frac{\overline{\varpi}_E}{\varpi_E} - 1 \sim \varpi_E^{m-1} \,,$$

so the image of G is contained in $U^{[}m-1_E$. But the norm of $\overline{\varpi}_E/\varpi_E$ 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 $F^\times = \mathrm{NM}(E^\times)$. 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 $\overline{\mathbb{F}}^\times$ to itself. We may factor $n = ap^b$ with a relatively prime to p. The kernel κ of f in $\overline{\mathbb{F}}^\times$ is cyclic of order a.

[kernel-mult] **5.1. Lemma.** *In these circumstances, if all the elements in κ lie in $\mathbb{F}$, then the kernel and the cokernel of $f|\mathbb{F}^\times$ are isomorphic.*

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

$$1 \longrightarrow \kappa \longrightarrow \overline{\mathbb{F}}^\times \longrightarrow \overline{\mathbb{F}}^\times \longrightarrow 1 \,.$$

This leads to a long exact sequence of cohomology

$$1 \longrightarrow \kappa^{\mathfrak{F}} \longrightarrow \overline{\mathbb{F}}^{\times} \longrightarrow \overline{\mathbb{F}}^{\times} \longrightarrow H^1(G, \kappa) \longrightarrow H^1(G, \overline{\mathbb{F}}^{\times}) \,.$$

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

(ii) Now suppose f to be an additive homomorphism from $\overline{\mathbb{F}}$ to itself. It can be expressed in the form

$$f(x) = x^{p^m}(a_0 x + a_1 x^p + \cdots + a_k x^{p^k})$$

with $a_0 \neq 0$. In this case the size of the kernel in $\overline{\mathbb{F}}$ is p^k. A slight modification of the previous proof givres:

[kernel-add] **5.2. Lemma.** *In these circumstances, if $\kappa = \kappa^{\mathfrak{F}}$ then the kernel and the cokernel of $f|\mathbb{F}$ are isomorphic.*

6. *Appendix.* Hensel's Lemma [hensels.tex]

In this section, suppose f to be a polynomial in $\mathfrak{o}[x] = \mathfrak{o}[x_1, \ldots, x_d]$, $\overline{f}$ its image in $\mathbb{F}[x]$. If a lies in $L = \mathfrak{o}^d$ and $f(a) = 0$ then the image $\overline{a}$ of a in $\mathbb{F}^d$ will be a root of $\overline{f}$. Conversely, suppose a in $\mathfrak{o}^d$ with $\overline{f}(\overline{a}) = 0$. That is to say, $f(a) \equiv_1 0$. Is there α in $\mathfrak{o}^d$ with $f(\alpha) = 0$ and $\alpha \equiv_1 a$? One very simple example that we shall be concerned with later on is $f\colon x \mapsto x^2$. Another will be the norm map from a quadratic extension of F.

Let ∇_f be the derivative of f, which for each a in L is a linear function on L with values in $\mathfrak{o}$. Thus for x in L, h in $\mathfrak{o}$

$$\big| f(a + hx) - (f(a) + h\langle \nabla_f(a), x\rangle)\big| \le C_a |h|^2$$

for some constant C_a bounding higher derivatives of f at a.

THE NON-SINGULAR CASE. Suppose for the moment that a in $\mathbb{F}^d$ satisfies $f(a) \equiv_1 0$, and that $\nabla_f(a) \not\equiv_1 0$ modulo $\mathfrak{p}$. Thus $\nabla_f(a)$ induces a non-trivial $\mathbb{F}$-linear map $\overline{\nabla}_f(a)$ from $L/\mathfrak{p}L$ to $\mathbb{F}$. Can we find $a + hx$ with h in $\mathfrak{p}$ and x in $\mathfrak{o}^d$ such that $f(a + hx) = 0$? A solution will be found by an approximation process. We shall find inductively elements a_n with $a_1 = a$, $a_{n+1} \equiv_n a_n$, $f(a_n) \equiv_n 0$. Suppose, therefore, that $f(a_n) \equiv_n 0$. Then

$$f(a_n + \varpi^n x) = f(a_n) + \varpi^n \langle \nabla_f(a), x\rangle + O(\varpi^{2n}) \,.$$

But by assumption $f(a_n)/\varpi^n$ lies in $\mathfrak{o}$, so that if

$$\langle \nabla_f(a), x\rangle = -\frac{f(a_n)}{\varpi^n}, \quad a_{n+1} = a_n + \varpi^n x$$

then $f(a_{n+1}) \equiv_{n+1} 0$. There are q^{d-1} possibilities for x modulo $\mathfrak{p}L$ and hence also for a_{n+1} modulo $\mathfrak{p}^{n+1}L$. The sequence (a_n) converges to a root α of f. Hence:

[hensels-nonsing] **6.1. Proposition.** (Hensel's Lemma, simple case) *Suppose a in L, $\overline{f}(\overline{a}) = 0$, $\overline{\nabla}_f(a) \ne 0$. Then there exists α with $\overline{\alpha} = \overline{a}$ and $f(\alpha) = 0$.*

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

[weil-density] **6.2. Corollary.** *Suppose f in $\mathfrak{o}[x]$ has the property that whenever $f(a) = 0$ then $\overline{\nabla}_f(a) \ne 0$. Then for every $n \ge 1$ the ratio*

$$\frac{|\{a \in L/\varpi^n L \mid f(a) \equiv_n 0\}|}{q^{n(d-1)}}$$

is equal to

$$\frac{|\{\overline{a} \in \mathbb{F}^d \mid \overline{f}(\overline{a}) = 0\}|}{q^{d-1}} \,.$$

Example. Let $d = 1$, $f(x) = x^q - x$. Every element of $\mathbb{F}$ is a root of $\overline{f}$. Furthermore, $f' = -1$. Hence for every element a in $\mathbb{F}$ there exists a unique α in $\mathfrak{o}$ such that $\alpha^q = \alpha$, $\overline{\alpha} = a$. This is the **Teichmüller lift** of a.

Example. Suppose $p \ne 2$, $d = 1$, $f(x) = x^2$, 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 $\mathbb{F}$.

THE SINGULAR CASE. What if $\nabla_f(a)$ reduces to 0 modulo $\mathfrak{p}$? 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 ± 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

$$\langle \overline{\nabla}_f(a), x\rangle = \frac{\langle \nabla_f(a), x\rangle}{\varpi^{N-1}}$$

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

$$f(a+\varpi^k x) = f(a) + \varpi^{k+N-1}\langle\overline{\nabla}_f(a), x\rangle + O(\varpi^{2k})$$

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

[hensels-singular] **6.3. Proposition.** *Suppose $\overline{\nabla}_f(a) \equiv 0 \bmod \mathfrak{p}^{N-1}$ but not $\bmod \mathfrak{p}^N$. Then for every $k \geq 0$ the induced map*

$$\frac{a+\mathfrak{p}^{N+k}L}{a+\mathfrak{p}^{N+k+1}L} \longrightarrow \frac{f(a)+\mathfrak{p}^{2N+k-1}L}{f(a)+\mathfrak{p}^{2N+k}}$$

is a surjective $\mathbb{F}$-linear map.

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

[squares-units] **6.5. Corollary.** *Every $a \equiv 1 \bmod 4\mathfrak{p}$ has a square root in $1+2\mathfrak{p}$.*

If p is odd, the condition on a is equivalent to requiring only that $a \equiv_1 1$.

[siegel-density] **6.6. Corollary.** *Suppose $\nabla_f(a) \neq 0$ for every a in L such that $f(a) = 0$. Then the limit*

$$\frac{\lim_{n\to\infty} |f^{-1}(\mathfrak{p}^n L)|}{q^{n(d-1)}}$$

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 $d = 2$, $F = \mathbb{Q}_2$, $f\colon x \mapsto x^2$, $a = 1$. The solutions of $x^2 \equiv 1$ modulo 2^n for $n \geq 3$ are the $a = \pm 1 \bmod 2^{n-1}$, making 4 solutions modulo 2^n. Only two of these lift to solutions modulo 2^{n+1}.

♡ [siegel-density] **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 [hensels.tex]

1. Helmut Hasse, **Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper**, Physica-Verlag, Würzburg–Wien, 1965.

2. Jean-Pierre Serre, **Corps locaux**, Hermann, 1968.