Essays on metaplectic representations

Local quadratic extensions

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

Suppose $F$ to be a $p$-adic field. In this essay I’ll prove:

**Theorem.** If $E/F$ is a separable quadratic extension with norm $N$: $E \to F$ then $F^\times / NE^\times$ has order two.

In addition, I’ll discuss the structure of the quotient and its relation to the ramification of $E/F$. The exposition will be elementary and essentially self-contained.

This is a simple case of the fundamental theorem of local class field theory, which for any abelian extension $E/F$ constructs an explicit isomorphism of $F^\times / NE^\times$ with the Galois group. There will be nothing new in my treatment, which has been basically an exercise in reading §V.3 of [Serre:1968]. Serre in fact deals with the slightly more complicated case in which $E/F$ is a cyclic extension of prime degree.

The proof to be presented does not do that, but it does say something about a relationship between the Galois group and norms. In all proofs of full local reciprocity that I am aware of, the case of prime cyclic extensions is an important step.

The Theorem can be supplemented by a converse: given any subgroup $H$ of $F^\times$ of index two, there exists a separable quadratic extension $E/F$ with $NE^\times = H$. It is unique up to isomorphism. I have already shown why this is true if the residue characteristic is odd. I’ll prove this in some later version of this essay when the characteristic of $F$ itself is other than 2. I am not aware of any simple proof in the case that $F$ does have characteristic 2.

If $E/F$ is generated by a root of $x^2 + ax + b$, there are elegant formulas in all cases (to be found in Chapter XIV of [Serre:1968]) for deciding whether or not a given $x$ in $F^\times$ lies in $NE^\times$ or not. The proofs I know start with the general theorems of local class field theory.

Contents

1. Introduction
2. The different
3. Norms and the filtration of units
4. References

1. Introduction

Let

- $\mathfrak{o}_F$ = 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 $\mathfrak{o}_F$)
- $\mathbb{F}_F = \mathfrak{o}_F / \mathfrak{p}_F$. 
Also, let $\text{ord}$ be the map from $F^\times$ to $\mathbb{Z}$ taking $u \varpi_F^n$ (a unit) to $n$. And for each $n \geq 0$ let

$$U_F^n = \{ u \in U_F \mid u \equiv_n 1 \}.$$ 

Here $\equiv_n$ means congruence modulo $\mathfrak{p}^n$.

The quotients associated to the filtration of unit groups have simple structures:

**1.1. Lemma.** The projection $U_F \rightarrow \mathfrak{o}_F/\mathfrak{p}_F$ induces an isomorphism of $U_F^0/U_F^1$ with $\mathbb{F}_F^\times$, and for $n \geq 1$ the map

$$x \mapsto 1 + x \varpi_F^n$$

induces an isomorphism of $\mathbb{F}$ with $U_F^n/U_F^{n+1}$.

The second isomorphism is not at all canonical, since for $n \geq 1$ it depends on a choice of $\varpi_F$. The canonical isomorphism is with $\mathfrak{p}^n/\mathfrak{p}^{n+1}$, which may be identified with $\otimes^n(\mathfrak{p}/\mathfrak{p}^2)$.

Fix the quadratic extension $E/F$, and let the conjugation in $E$ be $x \mapsto \overline{x}$. Let

$$N = \text{the norm map from } E \rightarrow F: x \mapsto x \varpi$$

$$\text{TR} = \text{the trace from } E \rightarrow F: x \mapsto x + \overline{x}.$$ 

I’ll first finish with the easy cases of the Theorem. In the first, the extension $E/F$ is the unique unramified extension of $F$. This means that $\varpi_E = \varpi_F$ and that $F_E$ is a quadratic extension of $\mathbb{F}_F$. I leave it as an exercise to prove that in this case $N\mathfrak{o}_E^\times = \mathfrak{o}_F^\times$ (a consequence of Hensel’s Lemma), and that $NE^\times$ is the union of all subsets $\mathfrak{o}_E^\times \varpi_F^n$ for $n \in \mathbb{Z}$.

Now suppose $E/F$ to be ramified. The second, still simple, case is that in which the residue field characteristic is odd. There are two possibilities for $E$, which are obtained by adjoining a square root of either $\varpi_F$ or $\varepsilon \varpi_F$ for some non-square unit $\varepsilon$. It is then easy to see (again, say, by Hensel’s Lemma) that $N\mathfrak{o}_E^\times$ consists of those units in $\mathfrak{o}_F$ whose image in $\mathbb{F}_F$ is a square. If we choose $v \varpi_F$ to be the norm of one of the square roots, the subgroup $NE^\times$ then contains this as well as all $uv^n \varpi_F^n$ with $u$ in this group. Again, it clearly has index two in $F^\times$.

So we are reduced to the third case, in which $E/F$ is ramified and the residue field characteristic is 2. This is by far the most interesting. In this case $E$ has as $F$-basis elements 1, $\varpi_E$. The second satisfies an Eisenstein equation

$$x^2 - ax + b = 0.$$ 

with $a$ in $\mathfrak{p}$ and $b = u \varpi_F$ for some unit $u$. I may as well choose $\varpi_F$ to be $b$. With this assumption

$$\varpi_E + \overline{\varpi}_E = a, \quad \varpi_E \overline{\varpi}_E = \varpi_F.$$ 

**REDUCTION TO UNIT GROUPS.**

**1.2. Lemma.** The inclusion of $U_F/NU_E$ in $K^\times/NL^\times$ is an isomorphism.

**Proof.** This can be proved directly, but following Serre I exhibit it as a consequence of a well known result that will be applied several times. I leave its proof as an exercise:

**1.3. Lemma.** (The Snake Lemma) Given two exact sequences in a commutative diagram

$$\begin{array}{cccccc}
0 & \rightarrow & A_1 & \rightarrow & A_2 & \rightarrow & A_3 & \rightarrow & 0 \\
& & \downarrow f_1 & & \downarrow f_2 & & \downarrow f_3 & \\
0 & \rightarrow & B_1 & \rightarrow & B_2 & \rightarrow & B_3 & \rightarrow & 0
\end{array}$$
the following sequence is exact:

$$0 \rightarrow \text{Ker}(f_1) \rightarrow \text{Ker}(f_2) \rightarrow \text{Ker}(f_3) \rightarrow \text{Coker}(f_1) \rightarrow \text{Coker}(f_2) \rightarrow \text{Coker}(f_3) \rightarrow 0.$$ 

In our case, the diagram is

$$
\begin{array}{ccccccc}
0 & \rightarrow & U_E & \rightarrow & E & \rightarrow & Z \\
& & \downarrow N & & \downarrow N & & \downarrow I \\
0 & \rightarrow & U_F & \rightarrow & F & \rightarrow & Z \\
\end{array}
$$

The outer map is the identity on $Z$ since the norm of $\varpi_E$ is $\varpi_F$. This concludes the proof of Lemma 1.2.  

2. The different

So now we must prove that $U_F/NU_E$ has order two. Proving this will use the congruence filtrations $\{U^n\}$ of the unit groups and maps induced by the norm on associated quotients.

The different $\vartheta_{E/F}$ is by definition the smallest ideal $d$ of $o_E$ such that $\text{TR}(d^{-1}) \subseteq o_F$. I recall a couple of basic facts about it.

2.1. Proposition. The different $\vartheta_{E/F}$ is the ideal of $o_E$ generated by $\varpi_E - \varpi_F$.

Proof. Recall that $\varpi_E$ is a root of the polynomial $f(T) = T^2 - aT + \varpi_F$, and that $1, \varpi_E$ form a basis of $o_E$. Since

$$f'(\varpi_E) = 2\varpi_E - a = 2\varpi_E - (\varpi_E + \varpi_E) = \varpi_E - \varpi_E,$$

the Lemma follows from the equations

$$
\begin{align*}
\text{TR} \frac{1}{f'(\varpi_E)} &= 0 \\
\text{TR} \frac{\varpi_E}{f'(\varpi_E)} &= 1.
\end{align*}
$$

These equations are a special case of a more general result, which I include here because its proof is more illuminating:

2.2. Lemma. Suppose

$$f(T) = \sum_{i=0}^{n} c_i T^i = \prod_{i=1}^{n} (T - x_i).$$

Then

$$
\sum_{i} \frac{x_k^i}{f'(x_i)} = \begin{cases} 
0 & \text{if } 0 \leq k < n - 1 \\
1 & \text{if } k = n - 1.
\end{cases}
$$

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

$$
\frac{1}{T^n} \sum_{j} \frac{1}{T^n - j} = \frac{1}{T^n} + \frac{a_1}{T^{n+1}} + \ldots
$$
and the right as
\[ \sum_i \frac{1}{f'(x_i)} \frac{1}{T} \frac{1}{1 - x_i/T} = \sum_i \frac{1}{f'(x_i)} \left( \frac{1}{T} + \frac{x_i}{T^2} + \frac{x_i^2}{T^3} + \cdots \right). \]

This concludes the proof of Proposition 2.1.

From now on, let \( m \) be the order of \( \vartheta_{E/F} \), so that \( \vartheta_{E/F} = p_m^F \). The previous result says that
\[ m = \text{ord}(\varpi_E - \varpi_E). \]

This and the previous Proposition tell us how to calculate the different in terms of the trace of \( \varpi_E \).

2.3. Corollary. If \( \varpi_E \) satisfies the Eisenstein equation \( x - ax + \varpi_F = 0 \) then \( \vartheta_{E/F} \) is generated by \( 2\varpi_E - a \).

So that if \( 2 = u\varpi_F^1 \) and \( a = v\varpi_E^e \) with units \( u, v \) then
\[ m = \min \ 2d + 1, 2e. \]

2.4. Corollary. If \( \sigma \neq 1 \) in \( G(E/F) \) then
\[ \frac{\varpi E}{\varpi E} = 1 + x\varpi_E^{m-1} \]
with \( x \neq 1 \).

Explicitly,
\[ \frac{\varpi E}{\varpi E} = \frac{a - \varpi E}{\varpi E} = 1 - (2 - a/\varpi E). \]

2.5. Lemma. For \( n \geq 0 \)
\[ \text{TR} \ p_F^{m+\ell} = p_F^{m+[\ell/2]} \]

Here \( \lfloor x \rfloor \) is the greatest integer \( n \leq x \). For example, \( \lfloor 1/2 \rfloor = 0, \lfloor -1/2 \rfloor = -1 \).

Proof. The characterization of \( \vartheta_{E/F} \) tells us that \( \text{TR} \ p_F^{-m} = o_F \) and \( \text{TR} \ p_F^{-m-1} = p_F^{-1} \). The trace is \( F \)-linear, so that upon multiplying by \( p_F^{m+\ell} = p_F^{2m+2\ell} \) we get
\[ \text{TR} \ p_F^{m+2\ell} = p_F^{m+\ell} \]
\[ \text{TR} \ p_F^{m+2\ell-1} = p_F^{m+\ell-1}. \]

This proves the Lemma, since \( \lfloor (2\ell)/2 \rfloor = \ell, \lfloor (2\ell - 1)/2 \rfloor = \ell - 1 \).

Following this, for all \( \ell \) we have
\[ \text{(2.6)} \]
\[ \text{TR}(x\varpi_E^{m+2\ell-1}) = \tau_{m+\ell-1}x\varpi_E^{m+\ell-1} \]
for some unit \( \tau_{m+\ell-1} \).
3. Norms and the filtration of units

How does the norm map behave with respect to the congruence filtration of \( U_E \)? The basic formula is very simple. Suppose \( k > 0 \). Every element in \( U_E^k \) is of the form \( 1 + x \overline{\omega}_E^k \), and

\[
N(1 + x \overline{\omega}_E^k) = 1 + \text{tr}(x \overline{\omega}_E^k) + x^2 \overline{\omega}_F^k.
\]

According to Lemma 2.5, this implies immediately that

\[
NU_{E}^{m+\ell} \subseteq U_{F}^{r} \quad \text{with} \quad r = \min \left( m + \lfloor \ell/2 \rfloor, m + \ell \right) = \begin{cases} 
m + \ell & \text{if } \ell < 0 \\
m & \text{if } \ell = 0 \\
m + \lfloor \ell/2 \rfloor & \text{if } \ell > 0. \end{cases}
\]

3.3. Proposition. Suppose \( k \geq 1 \).

(a) If \( k < m - 1 \), the map induced by the norm on from \( U_k^m/U_k^{m+1} \) to \( U_k^m/U_k^{m+k} \) takes

\[
1 + x \overline{\omega}_E^k \mapsto 1 + x^2 \overline{\omega}_F^k.
\]

(b) If \( k = m - 1 \), the map induced by the norm on from \( U_{m-1}^m/U_{m-1}^{m+1} \) to \( U_{m}^m/U_{m}^{m+k} \) takes

\[
1 + x \overline{\omega}_E^{m-1} \mapsto 1 + (\tau_{m-1} x + x^2) \overline{\omega}_F^{m-1}.
\]

(c) If \( k = m + 2 \ell - 1 \) with \( \ell \geq 1 \), the map induced by the norm on from \( U_{m+2\ell-1}^m/U_{m+2\ell-1}^{m+1} \) to \( U_{m+2\ell}^m/U_{m+2\ell}^{m+1} \) takes

\[
1 + x \overline{\omega}_E^{m+2\ell-1} \mapsto 1 + \tau_{m+\ell-1} x \overline{\omega}_F^{m+\ell-1}.
\]

From now on, the proof of the Theorem takes several small steps.

Step 1. The first is:

3.4. Lemma. The norm map induces an isomorphism of \( U_{E}/U_{E}^{m-1} \) with \( U_{F}/U_{F}^{m-1} \).

Proof. Using a standard argument about filtrations (amounting to an inductive application of Lemma 1.3), this will follow from the claims (a) for \( k \leq m \) the norm takes \( U_k^m \) to \( U_k^m \) and (b) for each \( k < m - 1 \) the induced map

\[
U_k^m/U_k^{m+1} \longrightarrow U_k^m/U_k^{m+k}
\]

is an isomorphism.

Since \( U^0 = \mathbb{O}^\times \) and \( U^1 = 1 + \mathbb{P} \), both \( U^1_E/U^1_E \) and \( U^1_F/U^1_F \) may be identified with the units in the common residue field \( \mathbb{F}^\times \). On this, the induced norm map takes \( x \) to \( x^2 \), which is an automorphism of the residue field. This takes care of the case \( k = 0 \).

In the case \( 0 < k < m - 1 \), the claim follows from case (a) of the last Proposition, since \( x \mapsto x^2 \) is an automorphism of \( \mathbb{F} \).

Step 2. Consider now the commutative diagram

\[
\begin{array}{ccccccc}
0 & \longrightarrow & U_{E}^{m-1} & \longrightarrow & U_{E} & \longrightarrow & U_{E}/U_{E}^{m-1} & \longrightarrow & 0 \\
& & \downarrow N & & \downarrow N & & \downarrow N_{m-1} & & \\
0 & \longrightarrow & U_{F}^{m-1} & \longrightarrow & U_{F} & \longrightarrow & U_{F}/U_{F}^{m-1} & \longrightarrow & 0
\end{array}
\]

According to Lemma 3.4, the right-hand map is an isomorphism. Lemma 1.3 therefore implies:

3.5. Lemma. The map

\[
U_{F}^{m-1}/NU_{E}^{m-1} \longrightarrow U_{F}/NU_{E}
\]
induced by inclusions is an isomorphism.

Given this, in order to prove the Theorem it remains only to prove that $U_{F}^{-1}/NU_{E}^{-1}$ has order two.

**Step 3.** Next I'll prove:

3.6. **Lemma.** We have $NU_{E}^{m} = U_{F}^{m}$.

**Proof.** For $\ell \geq 0$ we have

\[
NU_{E}^{m+2\ell+1} \subseteq U_{F}^{m+\ell}
\]

\[
NU_{E}^{m+2\ell+2} \subseteq U_{F}^{m+\ell+1}.
\]

In order to prove Lemma 3.5, it will suffice to show that for each $\ell \geq 0$ the induced map

\[
U_{E}^{m+2\ell+1}/U_{E}^{m+2\ell+2} \longrightarrow U_{F}^{m+\ell}/U_{F}^{m+\ell+1}
\]

is surjective. This is case (c) of Proposition 3.3.

**Step 4.** I shall apply Lemma 1.3 one more time. Consider the commutative diagram

\[
\begin{array}{cccccc}
0 & \longrightarrow & U_{E}^{m} & \longrightarrow & U_{E}^{m-1} & \longrightarrow & U_{E}^{m-1}/U_{E}^{m} & \longrightarrow & 0 \\
\downarrow N & & \downarrow N & & \downarrow N & & \downarrow N & & \\
0 & \longrightarrow & U_{F}^{m} & \longrightarrow & U_{F}^{m-1} & \longrightarrow & U_{F}^{m-1}/U_{F}^{m} & \longrightarrow & 0
\end{array}
\]

Given the previous Lemma, Lemma 1.3 implies that

3.7. **Lemma.** The homomorphism induced by projections

\[
U_{F}^{m-1}/NU_{E}^{m-1} \longrightarrow \text{Coker}(N_{m-1})
\]

is an isomorphism.

**Step 5.** It remains now to examine the map from $U_{E}^{m-1}/U_{E}^{m}$ to $U_{F}^{m-1}/U_{F}^{m}$ induced by the norm map. This is case (b) of Proposition 3.3. Modulo $1 + p_{F}^{m}$ we have

\[
N(1 + x\tau_{E}^{m-1}) = 1 + (\tau + x^{2})\tau_{E}^{m-1}
\]

with $\tau = \tau_{m-1}$. The map on $\mathbb{F}$ taking $x$ to $\tau x + x^{2}$ has cokernel of order two, because

\[
\tau x + x^{2} = \tau^{2}(x/\tau + (x/\tau)^{2})
\]

and the map $x \mapsto x + x^{2}$ is an $\mathbb{F}_{2}$-linear map from $\mathbb{F}$ to itself with kernel the image of $\mathbb{F}_{2}$ in $\mathbb{F}$. So the image of $U_{E}^{m-1}$ in $U_{F}^{m-1}/U_{F}^{m}$ has order two.

This concludes the proof of the Theorem.

The proof shows that:

3.8. **Lemma.** All the arrows

\[
\text{Coker}(N_{m-1}) \leftarrow U_{F}^{m-1}/NU_{E}^{m-1} \longrightarrow U_{F}/NU_{E} \longrightarrow F^{\times}/NE^{\times}
\]

are isomorphisms.

**Remark.** I have remarked that although this proof does not give a direct isomorphism of the Galois group $G(E/F)$ with $F^{\times}/NE^{\times}$, there is an implicit relation with the Galois group. This is because the kernel of the induced norm map

\[
U_{E}^{m-1}/U_{E}^{m} \rightarrow U_{F}^{m-1}/U_{F}^{m}
\]
Local quadratic extensions

is the image of \( G \) under the map \( \sigma \mapsto \sigma(\mathcal{O}_E)/\mathcal{O}_E \). Since the groups \( U_{m-1}^n/E \) and \( U_{F}^m-1/F \) may both be considered vector spaces over \( F_2 \), its cokernel and kernel must have the same size.

**Remark.** The more general result in which \( E/F \) is cyclic of prime order is not much more difficult to prove. 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 \( F^\times = NE^\times \). This leads to one of the fundamental components in local class field theory, that all elements of the Brauer group of a local field split over its unramified extension.

**Remark.** (3.2) says that

\[
NU^m_E \subset U^r_F
\]

where

\[
r = \min \lfloor (m + k)/2 \rfloor, k.
\]

Suppose we plot all the points in the discrete graph of the function \( k \mapsto \min \lfloor (m + k)/2 \rfloor, k \), and then take the convex hull of the union of these points and the \( x \)-axis. Its top is the graph of the function

\[
x \mapsto \begin{cases} x & \text{if } 0 \leq x \leq m - 1 \\ (x + (m - 1))/2 & \text{if } m - 1 \leq x, \end{cases}
\]

which is closely related to what Serre calls the Herbrand function \( \varphi(x) \). This observation suggests that in general Serre’s function might be interpreted as a function whose graph is the convex hull of some interesting set of points. This is indeed true, according to some ideas of John Tate. I’ll take this up elsewhere.

4. References