1. The Issue

We are interested in studying the square classes in local fields, and the maps between them that arise under finite extensions. Moreover, we are particularly interested in studying $F^\times/N(L^\times)$ when L/F is a quadratic extension. It is 'well known', by local class field theory, that this group is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. In particular that the map from $L^\times/(L^\times)^2$ to $F^\times/(F^\times)^2$ has image of index 2. For an odd degree (abelian) extension $F^\times/N(L^\times)$ will be of odd degree, and one concludes that the map on square classes is surjective. We will discuss these issues further in what follows.

2. What happens

Proposition 2.1 (Hensel's Lemma)**.** *Let R be a ring complete with respect to $\mathfrak{m}$. Let $f(x) \in R[x]$ be a polynomial, let $z \in R$ be such that $f(z) \cong 0 \mod f'(z)^2\mathfrak{m}$. Then there exists $y \in R$ such that $f(y) = 0$, moreover $y \cong z \mod f'(z)\mathfrak{m}$.*

It is fairly easy to see that $F^\times/(F^\times)^2$ decomposes as $\mathcal{O}_F^\times/(\mathcal{O}_F^\times)^2 \times \mathbb{Z}/2\mathbb{Z}$ where the second factor corresponds to the valuation $\mod 2$.

What Hensel says about square classes of units:

Let $f(x) = x^2 - a$, then there exists $y \in R$ with $y^2 = a$ if and only if there exists $z \in R$ with $z^2 \cong a \mod 4z^2\mathfrak{m}$.

2.1. non-2-adic.

Now, for non 2-adic local rings, we have that $4 \in R^*$ and thus, this reduces to a is a square mod $z^2\mathfrak{m}$. Moreover, if we have chosen $a \in \mathcal{O}^*$ then any candidate solution must also be a unit, and thus, we have:

Proposition 2.2. *Let F be a non 2-adic local field, then $a \in \mathcal{O}_F^*$ is a square if and only if a is square mod $\mathfrak{m}$.*

2.2. 2-adic.

What about 2-adics? Again we are interested in the case of a a unit, we have that the condition is:

Proposition 2.3. *Let F be a 2-adic local field, suppose $(2) = \mathfrak{m}^k$ then, $a \in \mathcal{O}_F^*$ is a square if and only if it is a square mod $\mathfrak{m}^{2k+1}$.*

Now, what is the structure of $\mathcal{O}_F/\mathfrak{m}^{2k+1}$?

Every element can be written as:

$$a_0 + a_1\pi + a_2\pi^2 + \cdots a_{2k}\pi^2k$$

Or alternatively as:

$$b_0(1 + b_1\pi)(1 + b_2\pi^2)\cdots(1 + b_{2k}\pi^{2k})$$

Where $a_i \in \mathcal{O}_F/\mathfrak{m}$. We remark that all these elements of $\mathcal{O}_F/\mathfrak{m}$ are in fact squares (in $\mathcal{O}_F/\mathfrak{m}$).

We thus have for $l < k$ the squares:

$$(1 + b\pi^l)^2 = 1 + b^2\pi^{2l} + b\pi^{k+l} = (1 + b'\pi^{2l})$$

In particular $(1 + b\pi^{2l})$ is a square, modulo π^{2l+1} for all b.

We conclude that modulo π^{2k} all the square classes have representatives of the form:

$$1 + a_1\pi + a_3\pi^3 + \cdots + a_{2k-1}\pi^{2k-1}$$

Or that they can be generated by:

$$(1 + a\pi^{2l+1}$$

Where a runs over any set of representatives of $\mathcal{O}_F/\mathfrak{m}$, $l < k$.

Next noting that $(1+x\pi^k)^2 = 1 + (x^2 + \frac{2}{\pi^{2k}})\pi^{2k}$, we get that modulo π^{2k+1} the additional non square classes:

$$(1 + b\pi^{2k})$$

Where $b \in \mathcal{O}_F/(b^2 + b\frac{2}{\pi^k})$. The map $x^2 + x(2/\pi^k)$ is a linear map from $\mathcal{O}_F/\mathfrak{m}$ as a $\mathbb{Z}/2\mathbb{Z}$ vector space to itself with kernel $0, 1$. Thus, $\mathbb{O}_F/x^2 + \frac{2}{\pi^k}x$ is $\mathbb{Z}/2\mathbb{Z}$. With representative b any value such that $x^2 + \frac{2}{\pi^{2k}}x + b$ is irreducible over $\mathcal{O}/\mathfrak{m}$.

Proposition 2.4. *There are $2\,|\mathcal{O}_F/\mathfrak{m}|^k$ distinct square classes.*

2.3. **Norm-maps.** What happens with the norm map for extensions of F?

2.3.1. *odd degree extensions.* Suppose we have $F \subset L$ of odd degree, ramification degree e, inertial degree f.

Well k in F becomes ek in L. There are now $N^{ef}/2$ many square classes in L where there were N in F, Moreover every square class of F becomes a square class of L. The norm map from $N_{L/F} : \mathcal{O}_L^*/(\mathcal{O}_L^*)^2 \to \mathcal{O}_F^*/(\mathcal{O}_F^*)^2$ is a surjective map of abelian groups. It is thus $|\mathcal{O}_L/\mathfrak{m}|^{ef}$ to 1.

Since we have that the composition:

$$\mathcal{O}_F^*/(\mathcal{O}_F^*)^2 \to \mathcal{O}_L^*/(\mathcal{O}_L^*)^2 \xrightarrow{N} \mathcal{O}_F^*/(\mathcal{O}_F^*)^2$$

is surjective, we conclude that $\mathcal{O}_L^*/(\mathcal{O}_L^*)^2\mathcal{O}_F^*$.

2.3.2. *even degree extensions.* What if $F \subset L$ is of degree 2. Then $f(x) = x^2 + a_1x + a_0$ is the minimal polynomial of some element.

Claim. *If $L = F(\sqrt{D})$ and $y \in F \setminus F^2$ satisfies $y = x^2$ for $x \in L$ then $y = fD$ for $f \in F^2$.*

Proof. Write $x = e + f\sqrt{D}$ then $x^2 = e^2 + 2ef\sqrt{D} + f^2D$. Then $e = 0$. $\square$

Then we have precisely one square class of F that stops being a square class. It is the square class of $1 - \frac{4a_0}{a_1^2}$.

Claim. *L/F is unramified if and only if we are adjoining the square root of $1 + b\pi^{2k}$ (where b makes this non-square).*

Proof. For any other non square we have $1 + a\pi^f$ as a lead term. $x^2 - (1 + a\pi^f)$ changing variables by $x \mapsto x + 1$ this becomes: $x^2 - a\pi^f + 2$. if $f < k$ set $x = \pi^{\frac{f-1}{2}}x$ to make this eisenstein. If $f > k$ and k odd, set $x = \pi^{\frac{k-1}{2}}x$ to make eisenstein. if $f > k$ and k even, set $x = \pi^{\frac{k}{2}}$ and repeat and be in first case. if $f = k$ we have $x^2 - (a+b)\pi^k$, where $b = 2/\pi^k$. If $a \neq b$ set $x = \pi^{\frac{k-1}{2}}x$ to make eisenstein.

Only case is $x^2 - (1+2) = x^2 - 3$, (noting we were in an odd degree extension of $\mathbb{Z}_2$ this makes sense to stay irreducible!.). But, this is the same extension as $x^2 + 2x - 2$, which is eisenstein.

That there exists an unramified extension completes the result!. (we also rigged up this 'unramified unit' to give an extension of the residue field) $\square$

Now what of norms:

Claim. *Let $u = 1 + b\pi^{2k}$ be the unramified unit, Let $1 - a\pi^{2l+1}$ be any ramified unit, let $a' = b/a$ in $\mathcal{O}_k/\mathfrak{m}$.*

- *u is a norm from $F(\sqrt{u})$.*
- *u is a norm from $F(\sqrt{1 - a\pi^{2l+1}})$.*

- *u is not a norm from $F(\sqrt{\pi(1-a\pi^{2l+1})})$.*
- *$1-a\pi^{2l+1}$ is a norm from $F(\sqrt{a\pi})$.*
- *$1-a\pi^{2l+1}$ is a norm from $F(\sqrt{1-c\pi^{2(k-l)+s}})$. for all c and all $s \geq 1$.*
- *$1-a\pi^{2l+1}$ is not a norm from $F(\sqrt{1-a'\pi^{2(k-l)-1}})$.*

Proof. Recall that X is a norm from $F(\sqrt{Y})$ if and only if Y is a norm from $F(\sqrt{X})$.

Observe that from $F(\sqrt{u})$ we have $N(1+b\pi^l) = 1 + \mathrm{Tr}(b)\pi^l$ modulo π^{l+1} we thus conclude that all the units are norms from $F(\sqrt{u})$ as the trace map is surjective.

We next observe that $a\pi$ can never be a norm from $F(\sqrt{u})$ as the valuations of the norms of elements are all even.

Usual formula yields:

$$(1-a\pi^{2l+1}, a\pi) = 1$$

indeed $1-a\pi^{2l+1} = 1^2 - a\pi(\pi^l)^2$.

Now the observation that for $s \geq 1$

$$1 = (1-a(1-c\pi^{2(k-l)+s})\pi^{2l+1}, a(1-c\pi^{2(k-l)+1})\pi) = (1-a\pi^{2l+1}, a(1-c\pi^{2(k-l)+s})\pi)$$

allows us to conclude $(1-a\pi^{2l+1}, 1-c\pi^{2(k-l)+s}) = 1$.

Finally we have:

$$(1-a(1-a'\pi^{2(k-l)-1})\pi^{2l+1}, a(1-a'\pi^{2(k-l)-1})\pi) = 1$$
$$(1-a\pi^{2l+1}+b\pi^{2k}, a(1-a'\pi^{2(k-l)-1})\pi) = 1$$
$$(1-a\pi^{2l+1}, a(1-a'\pi^{2(k-l)-1})\pi) = -1$$
$$(1-a\pi^{2l+1}, 1-a'\pi^{2(k-l)-1}) = -1$$

□

With the above we are given a complete description of a generator for the coset of square class which are not a norm from L.