HOMEWORK SET 5

Local Class Field Theory - Fall 2011

For questions, remarks or mistakes, write me at sivieroa@math.leidneuniv.nl.

Remark 1. *Recall on the structure of units for Local Fields. We recall the structure of the units for a Local Field of characteristic zero, result which is fundamental in the solutions of the first two exercises.*
Given a local field K with residue field κ of cardinality q and characteristic p, we well know the structure of $K^\times$ as a $\mathbb{Z}_p$-module and it's the following:

$$K^\times \cong \mathbb{Z} \oplus \mathbb{Z}/(q-1)\mathbb{Z} \oplus \mathbb{Z}/p^a\mathbb{Z} \oplus \mathbb{Z}_p^{[K:\mathbb{Q}_p]};$$

where p^a is the maximal p-th power such that K contains a primitive p^a-th root of unity.
As a good reference to this important result, I suggest to give a look at the book "Algebraic Number Theory" by Neukirch (Chapter 2, Theorem 5.7), where you can also find the analogous result for characteristic p.
As a consequence of this, we can also think to the general finite quotient $K^\times/(K^\times)^n$ in terms of this representation. For example

$$(K^\times)^2 \cong 2\mathbb{Z} \oplus 2(\mathbb{Z}/(q-1)\mathbb{Z}) \oplus 2(\mathbb{Z}/p^a\mathbb{Z}) \oplus 2\mathbb{Z}_p^{[K:\mathbb{Q}_p]}.$$

Now, if $p \neq 2$, then

$$(K^\times)^2 \cong 2\mathbb{Z} \oplus 2(\mathbb{Z}/(q-1)\mathbb{Z}) \oplus (\mathbb{Z}/p^a\mathbb{Z}) \oplus \mathbb{Z}_p^{[K:\mathbb{Q}_p]},$$

(remember that 2 is invertible in $\mathbb{Z}/n\mathbb{Z}$ if $(2,n)=1$ and 2 is invertible in $\mathbb{Z}_p$ if $p \neq 2$) which tells us that

$$K^\times/(K^\times)^2 \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z},$$

which is so always of cardinality 4.
Analogously, if $p = 2$,

$$K^\times/(K^\times)^2 \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^{[K:\mathbb{Q}_p]},$$

which is of cardinality $2^{2+[K:\mathbb{Q}_p]}$.
In the same spirit one can also prove the following result (where p is still the characteristic of the residue field)

$$|K^\times/(K^\times)^p| = \begin{cases} p^{2+[K:\mathbb{Q}_p]}, & \text{if } \mu_p \in K \\ p^{1+[K:\mathbb{Q}_p]}, & \text{if } \mu_p \notin K \end{cases}$$

where μ_p denotes a primitive p-th root of unity.

Exercise 5.1**.** Let p be a prime number below 50 and suppose that K is an abelian extension of $\mathbb{Q}_p$ of degree 15 which is totally ramified. Show that $p = 31$.

Solution using the characterization of the Norm in the totally ramified case.

Proof.

Remark 2 (Totally ramified extensions)**.** *Given K a local field of characteristic zero with π an uniformizer element, if we consider a finite extension L/K we have the following result*

$$L/K \text{ totally ramified } \Leftrightarrow \pi \in Nm(L^\times).$$

Proof. This fact is a consequence of the definition of the extension of the valution v_K over L given by the formula

$$v_L(\alpha) = \frac{1}{n} v_K(Nm(\alpha))$$

and the fact that

$$Im(v_L) = \frac{1}{e}\mathbb{Z},$$

where e is the ramification index of the extension.
($\Rightarrow$) If the extension is totally ramified then $e = n$ and, by the formula on v_L, it has to exist an element $\alpha \in L^\times$ such that $Nm(\alpha) = \pi$.
($\Leftarrow$) If it exists $\alpha \in L^\times$ such that $Nm(\alpha) = \pi$, then $v_l(\alpha) = \frac{1}{n}$ and so $e = n$.

We can now solve the exercise using Local Class Field Theory and remembering that for Local Fields of characteristic zero the Norm subgroups are exactly the subgroup of finite index (since for Local Fields of characteristic zero any finite subgroup is open, look at the first Chapter of Milne or at Exercise 3).
By LCFT to find an abelian extension K of $\mathbb{Q}_p$ of degree 15 means to find a Norm subgroup $\mathrm{Nm}(K^\times)$ of $\mathbb{Q}_p^\times$ of index 15. Moreover, thanks to our second remark, if we want also that this extension be totally ramified our subgroup $\mathrm{Nm}(K^\times)$ has to contain p.
We look at the structure of units in $\mathbb{Q}_p$ given by our first remark and we recall that, when $p \neq 2$, $\mathbb{Q}_p$ does not contain a p-th root of unity (this can found in any book on the p-adic numbers and it easily comes down from the Eisenstein criterion applied in $\mathbb{Z}_p$):

$$\mathbb{Q}_p^\times \cong \mathbb{Z} \oplus \mathbb{Z}/(p-1)\mathbb{Z} \oplus \mathbb{Z}_p.$$

We can exlude the case $p = 2$, since in that case $\mathbb{Q}_2^\times \cong \mathbb{Z} \oplus \mathbb{Z}/2^a\mathbb{Z} \oplus \mathbb{Z}_2$ and any finite order subgroup has index divisible by 2 but 15 is odd.
Thus assuming that $p \neq 2$, we underline that if you try to prove the previous isomorphism you easily see that the component $\mathbb{Z}$ comes out exactly from the powers of p. So, since

we want $p \in \mathrm{Nm}(K^\times)$, the quotient $\mathbb{Q}_p/\mathrm{Nm}(K^\times)$ has to be a subgroup of order 15 of $\mathbb{Z}/(p-1)\mathbb{Z} \oplus \mathbb{Z}_p$. From that (using the fact that any finite index subgroup of $\mathbb{Z}_p$ is of the form $p^r\mathbb{Z}_p$) we deduce the condition

$$15 \,|\, p^r(p-1)$$

and so $15 = p^t \cdot a$, where $0 \leq t \leq r$ and $a \,|\, (p-1)$. If $t > 0$ then $p = 3$ or $p = 5$ but in both cases we get a contradiction since $p - 1 = 2$ or 4 (and 15 is not divisible by 2). So $t = 0$ and we deduce that $15 \,|\, p-1$, thus $p \equiv 1 \bmod 15$ and, since $p < 50$, we get $p = 31$. □

Solution using the inertia group.

Proof. We know by the theory (Milne Chap. 1), that the Artin map sends $\mathbb{Z}_p^\times$ to the Inertia group. Since we want a totally ramified extension, the Inertia group coincides with the Decomposition group which is equal to the Galois group of our extension, since we are working with Local Fields. So we get that in the totally ramified case $\mathbb{Z}_p^\times$ maps surjectivly to $\mathrm{Gal}(K/\mathbb{Q}_p)$, where K is the extension we are looking for. This implies that $\mathrm{Gal}(K/\mathbb{Q}_p)$ is isomorphic to a finite quotient of $\mathbb{Z}_p^\times$ and so $15|p^{r-1}(p-1)$ and we conclude as above. □

Solution using Kronecker-Weber.

Proof. By the Local Kronecker-Weber Theorem for $\mathbb{Q}_p$ (Milne Chap. 1, Cor. 4.12), any finite abelian extension of $\mathbb{Q}_p$ is contained in a cyclotomic extension and in order to be totally ramified, it has to be contained in an extension of the form $\mathbb{Q}_p(\zeta_{p^r})$.
Since $[\mathbb{Q}_p(\zeta_{p^r}) : \mathbb{Q}_p] = \phi(p^r) = p^{r-1}(p-1)$ (where ϕ denote the Euler function), we have that $15|p^{r-1}(p-1)$, which allows us to conclude as above. □

Exercise 5.2. Give an example of a prime p, a finite extension K of $\mathbb{Q}_p$ and an abelian extension L/K of exponent 2 and degree 64.

Proof. Using LCF, the maximal abelian extension of exponent 2 of K corresponds to the quotient $K^\times/(K^\times)^2$ and so $(K^\times)^2 \subset \mathrm{Nm}(L^\times)$. Since we want an extension of degree 64, already from this fact and the first remark, we deduce that p has to be equal to 2 (otherwise, looking at the first remark, $K^\times/(K^\times)^2$ is always of cardinality 4).
Moreover, looking again at the first remark, we also recall that for $p = 2$, the quotient $K^\times/(K^\times)^2$ is of cardinality $2^{2+[K:\mathbb{Q}_p]}$, so, since $64 = 2^6$, it's sufficient to take an extension K of $\mathbb{Q}_p$ of degree at least 4. For example take $K = \mathbb{Q}_p(\zeta_5)$ and $L = K[\sqrt{K}]$.

□

Exercise 5.3. Let K be a local field of characteristic 0. Show that every finite index subgroup of $K^\times$ is open. Bonus question: is the same true for characteristic p?

Proof. This exercise is actually solved by Remark 1.7 in the first Chapter of Milne's book, where it's also proved that for characteristic p the result is not true.

□

Exercise 5.4. Let K be a local field, let K^{sep} be the separable closure of K and let G_K be the profinite group $\mathrm{Gal}(K^{sep}/K)$. Show that $H^3(G_K, K^{sep\times}) = 0$.

Proof. Since $K^{sep} = \bigcup_{K\subset L\subset K^{sep},\,[L:K]<\infty} L = \bigcup_{H\subset G_K,\,open\ and\ normal}(K^{sep})^H$, by the definition of cohomology for profinite groups, we have

$$H^3(G_K, K^{sep\times}) = \varinjlim H^3(\mathrm{Gal}(L/K), L^\times)$$

where the limit is taken over all extensions $K \subset L \subset K^{sep}$ of finite degree. Thus, if we prove that for any finite extension L/K, $H^3(\mathrm{Gal}(L/K), L^\times) = 0$, we are done since then the limit will be trivial, too.
We know from the course, that for finite extensions of Local Fields we can apply Tate's theorem, so in particular we have

$$H^3(\mathrm{Gal}(L/K), L^\times) \cong H^1(\mathrm{Gal}(L/K), \mathbb{Z}) = \mathrm{Hom}_{cont}(\mathrm{Gal}(L/K), \mathbb{Z}).$$

Now it's easy to conclude, since we know that any homomorphism from a finite group into $\mathbb{Z}$ has to be trivial.

□

Exercise 5.5.Let p be a prime, $K = \mathbb{Q}_p$ and $n = p-1$. Recall that $\mu_n \subset K^\times$. For $a,\, b \in K^\times$, let $(a,\, b) \in \mu_n$ be the image of the pair (a mod $(K^\times)^n$, b mod $(K^\times)^n$) under the Hilbert symbol $K^\times/(K^\times)^n \times K^\times/(K^\times)^n \to \mu_n$. Show that $(a,\, b) \equiv (-1)^{v(a)v(b)} a^{v(b)} b^{-v(a)} \bmod p\mathbb{Z}_p$. Hint: use Example 3.13 of chapter 1 and you may also use that $\mathbb{Q}_p(\zeta_p) = \mathbb{Q}_p(\sqrt[p-1]{-p})$.

Proof. We start computing $(-p,\, b)$: using the formula linking the Hilbert symbol and the Artin map, we have

$$(-p,\, b) = \frac{\phi_{\mathbb{Q}_p}(b)(\sqrt[p-1]{-p})}{\sqrt[p-1]{-p}}$$

and, since $\mathbb{Q}_p(\zeta_p) = \mathbb{Q}_p(\sqrt[p-1]{-p})$, this is the same as computing $\dfrac{\phi_{\mathbb{Q}_p}(b)(\zeta_p)}{\zeta_p}$.
Using example 3.13 of Chapter 1 (Milne), we get that, if $b \in (\mathbb{Z}_p)^\times$,

$$(-p,\, b) = \frac{\phi_{\mathbb{Q}_p}(b)(\zeta_p)}{\zeta_p} \equiv b^{-1} \bmod p\mathbb{Z}_p. \tag{1}$$

From now on we put always the symbol $\equiv$ to denote the congruence mod $p\mathbb{Z}_p$. In the same spirit we have also

$$(-p,\, -1) = -1 \tag{2}$$

and

$$(a,\, b) \equiv 1 \text{ if } a \text{ and } b \in (\mathbb{Z}_p)^\times. \tag{3}$$

Now we can play with the properties of the Hilbert symbol: first of all we have

$$(-p,\, p) = (p,\, -p) = 1 \tag{4}$$

and since the Hilbert symbol is skew-symmetric we also get

$$(a,\, -p) \equiv a \text{ if } a \in (\mathbb{Z}_p)^\times. \tag{5}$$

Using 2 and 3, we deduce that

$$(p,\, -1) = -1 \tag{6}$$

and now from 4 and 6, we have

$$(p,\, p) = -1. \tag{7}$$

We are finally ready to conclude using all the formulas above, indeed if we take $a = p^{v(a)}u_a$ and $b = p^{v(b)}u_b$ (u_a and u_b belong to $(\mathbb{Z}_p)^\times$), using the bilinearity of the Hilbert symbol, we have

$$\begin{aligned}(a,\, b) &= (p^{v(a)},\, p^{v(b)})(p^{v(a)},\, u_b)(u_a,\, p^{v(b)})(u_a,\, u_b)\\ &\equiv (-1)^{v(a)v(b)}u_b^{-v(a)}u_a^{v(b)} \bmod p\mathbb{Z}_p\\ &\equiv (-1)^{v(a)v(b)}a^{v(b)}b^{-v(a)} \bmod p\mathbb{Z}_p.\end{aligned}$$

□