MATH 776
BACKGROUND ON LOCAL FIELDS AND KUMMER THEORY

ANDREW SNOWDEN

Our goal at the moment is to prove the Kronecker–Weber theorem. Before getting to this, we review some of the basic theory of local fields and Kummer theory, both of which will be used constantly throughout this course.

1. Structure of local fields

Let $K/\mathbf{Q}_p$ be a finite extension. We denote the ring of integers by $\mathcal{O}_K$. It is a DVR. There is a unique maximal ideal $\mathfrak{m}$, which is principal; any generator is called a **uniformizer**. We often write π for a uniformizer. The quotient $\mathcal{O}_K/\mathfrak{m}$ is a finite field, called the **residue field**; it is often denoted k and its cardinality is often denoted q.

Fix a uniformizer π. Every non-zero element x of K can be written uniquely in the form $u\pi^n$ where u is a unit of $\mathcal{O}_K$ and $n \in \mathbf{Z}$; we call n the **valuation** of x, and often denote it $v(x)$. We thus have $K = \bigcup_{n \geq 0} \pi^{-n}\mathcal{O}_K$. This shows that K is a direct union of the fractional ideals $\pi^{-n}\mathcal{O}_K$, each of which is a free $\mathcal{O}_K$-module of rank one. The additive group $\mathcal{O}_K$ is isomorphic to $\mathbf{Z}_p^d$, where $d = [K : \mathbf{Q}_p]$.

The decomposition $x = u\pi^n$ shows that $K^\times \cong \mathbf{Z} \times U$, where $U = \mathcal{O}_K^\times$ is the unit group. This decomposition is non-canonical, as it depends on the choice of π. The exact sequence

$$0 \to U \to K^\times \xrightarrow{v} \mathbf{Z} \to 0$$

is canonical. Choosing a uniformizer is equivalent to choosing a splitting of this exact sequence.

Let $k = \mathcal{O}_K/\mathfrak{m}$ be the residue field. Consider the reduction modulo $\mathfrak{m}$ map $U \to k^\times$. It is surjective (proof: every element of $k^\times$ admits a lift to $\mathcal{O}$, and is necessarily a unit). Its kernel consists of units congruent to 1 modulo $\mathfrak{m}$, and is often denote U_1; these are called **principal units**. We thus have an exact sequence

$$1 \to U_1 \to U \to k^\times \to 1.$$

This sequence splits canonically. Indeed, suppose $x \in k^\times$. Then $x^{q-1} = 1$, where $q = \#k$. Since the polynomial $T^{q-1} - 1$ splits into distinct linear factors over k, Hensel's lemma shows that every root over k lifts to a unique root in $\mathcal{O}_K$. Thus there is a unique $(q-1)$ root of unity $\omega(x) \in U$ mapps to x. One easily verifies that $\omega\colon k^\times \to U$ is a group homomorphism that splits the above sequence. It is called the **Teichmüller character**.

The group U_1 contains the group μ_{p^r} of all p-power roots of unity in K. The quotient U_1/μ_{p^r} is isomorphic to $\mathbf{Z}_p^d$ where $d = [K : \mathbf{Q}]$. Indeed, one has versions of the exponential and logarithm that give isomorphisms between $1 + \mathfrak{m}^n$ and $\pi^m\mathcal{O}_K$ for appropriate n and m, and this shows that $1 + \mathfrak{m}^n$ is isomorphic, as a group under multiplication, to $\mathbf{Z}_p^d$. Since U_1/μ_{p^r} is torsion-free, it too is isomorphic to this. In particular, U_1 is a p-group, and thus all elements have all prime-to-p roots canonically.

Date: January 29, 2019.

Putting this all together, we have a (non-canonical) isomorphism

$$K^\times \cong \mathbf{Z} \times \mathbf{Z}/(q-1)\mathbf{Z} \times \mathbf{Z}/p^r\mathbf{Z} \times \mathbf{Z}_p^d$$

where $q = \#k$, p^r is the number of p-power roots of unity in K, and $d = [K : \mathbf{Q}_p]$. Note that $\mathbf{Z}/(q-1)\mathbf{Z} \times \mathbf{Z}/p^r\mathbf{Z}$ can be identified with the group of all roots of unity in K.

2. Extensions of local fields

Let $K/\mathbf{Q}_p$ be a finite extension, and let L/K be a finite extension. Let π (resp. ϖ) be a uniformizer of K (resp. L), and let k (resp. ℓ) be the residue field of K (resp. L). Then ℓ/k is an extension of finite fields; its degree is typically denoted $f = f(L/K)$. We can write $\pi = u\varpi^e$ for some unit u of L. The number $e = e(L/K)$ is independent of all choices, and called the **ramification index** of the extension. We have the fundamental relation $[L : K] = ef$. The extension is called **unramified** if $e = 1$, **tamely ramified** if $p \nmid f$, **wildly ramified** if $p \mid f$, and **totally ramified** if $f = 1$. There is a canonical intermediate field L^u of L/K such that L^u/K is unramified (of degree f) and L/L^u is totally ramified (of degree e). The group $\mathrm{Gal}(L/L^u) \subset \mathrm{Gal}(L/K)$ is called the **inertia group**, and denoted I. There is also a canonical intermediate field $L^u \subset L^t \subset L$ such that L^t/L^u is tamely ramified (of degree the prime-to-p part of e) and L/L^t is wildly ramified (of degree the p-part of e). The group $I^t = \mathrm{Gal}(L^t/L^u)$ is called the **tame inertia group**, which is a subgroup of I, while the group $I^w = \mathrm{Gal}(L/L^t)$ is called the **wild inertia group**, which is a quotient of I.

Unramified extensions correspond bijectively to extensions of the residue field. Precisely, suppose that L/K is an unramified extension. Write $\ell = k(\zeta)$ where ζ is a root of unity; this is possible by the theory of finite fields. By Hensel's lemma, ζ lifts to a unique root of unity in L, which we still call ζ. Thus $K(\zeta) \subset L$. Since both extensions are unramified and have residue field ℓ, they have the same degree over K, and thus they are equal. The extension L/K is always Galois, and the natural map $\mathrm{Gal}(L/K) \to \mathrm{Gal}(\ell/k)$ is an isomorphism. Thus $\mathrm{Gal}(L/K)$ is a cyclic group. There is a canonical generator lifting the Frobenius automorphism in $\mathrm{Gal}(\ell/k)$, which we still call the Frobenius element.

Next, suppose that L/K is tamely and totally ramified. Write $\varpi^e = u\pi$ for some unit u of L. Since $\ell^\times = k^\times$, we can find a unit v of K congruent to u modulo (ϖ); replacing π with $v^{-1}\pi$, we can thus assume $u \in U_1$. Since U_1 is a pro-p-group, it is e-divisible, that is, u has an eth root w in U_1. Replacing ϖ with $w\varpi$, we can thus assume $u = 1$. In other words, we can choose our uniformizers so that $\varpi^e = \pi$. We thus see that $L = K(\pi^{1/e})$, that is, any totally and tamely ramified extension is obtained by adjoining a root of a uniformizer. This extension is Galois if and only if K contains all eth roots of unity. Suppose this is the case. We then have a homomorphism

$$\mathrm{Gal}(L/K) \to \mu_e, \qquad \sigma \mapsto \frac{\sigma(\pi^{1/e})}{\pi^{1/e}},$$

where $\mu_e \subset K^\times$ denotes the group of eth roots of unity. One verifies that this is an isomorphism and independent of any choices (this is a special case of Kummer theory, which we cover below). Thus, again, $\mathrm{Gal}(L/K)$ is cyclic.

Now suppose that L/K is an arbitrary tamely ramified Galois extension. We then get a canonical exact sequence

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Gal}(L/L^u) & \longrightarrow & \mathrm{Gal}(L/K) & \longrightarrow & \mathrm{Gal}(L^u/K) & \longrightarrow & 1 \\ & & \| & & & & \| & & \\ & & \mu_e & & & & \mathrm{Gal}(\ell/k) & & \end{array}$$

One can show that this extension of groups is split (non-canonically), and so $\mathrm{Gal}(L/K)$ is the semi-direct product of the outside groups. The action of $\mathrm{Gal}(\ell/k)$ on $\mu_e \subset \ell^\times$ is the natural one.

Finally, suppose that L/K is a Galois extension that is totally and wildly ramified. Then $\mathrm{Gal}(L/K)$ is a p-group. In contrast to the other cases, it does not have to be cyclic, or even abelian. However, being a p-group, it is solvable. Combining all three cases, one sees that $\mathrm{Gal}(L/K)$ is always solvable.

Consider the extension $\mathbf{Q}_p(\zeta_p)$ of $\mathbf{Q}_p$. It is a totally ramified extension of degree $p-1$, and thus tamely ramified, and therefore has the form $\pi^{1/p}$ for some uniformizer π of $\mathbf{Q}_p$. We can write $\pi = \gamma p$ for some unit γ of $\mathbf{Q}_p$. Since the group of principal units is a p-group, all principal units are $(p-1)$st powers, and so the extension is unchanged if we modify γ by a principal unit. We can thus assume that γ is a $(p-1)$st root of unity. The following proposition, which we require in our proof of local Kronecker–Weber, determines this root of unity:

Proposition 2.1. *We have $\gamma = -1$, that is, $\mathbf{Q}_p(\zeta_p) = \mathbf{Q}_p((-p)^{1/(p-1)})$.*

Proof. Let $\Phi_p(t)$ be the pth cyclotomic polynomial. We have

$$\Phi_p(t) = 1 + t + \cdots + t^{p-1} = \prod_{i=1}^{p-1}(t - \zeta_p^i)$$

Evaluating at 1, we thus find

$$\Phi_p(1) = p = \prod_{i=1}^{p-1}(1 - \zeta_p^i).$$

Now, we have

$$\frac{1-\zeta_p^i}{1-\zeta_p} = 1 + \zeta_p + \cdots + \zeta_p^{i-1},$$

which reduces to i in the residue field $\mathbf{F}_p$; in particular, it is a unit. Thus, putting $\pi = 1 - \zeta_p$, we see

$$\pi^{p-1} = \left[\prod_{i=1}^{p-1} \frac{1-\zeta_p}{1-\zeta_p^i}\right] \cdot \left[\prod_{i=1}^{p-1}(1-\zeta_p^i)\right] = up,$$

where u is a unit reducing to $1/(p-1)! = -1$ in $\mathbf{F}_p$. We can thus write $u = -v$ where v is a principal unit. As the group of principal units is a p-group, v is a $(p-1)$st power, say $v = w^{p-1}$. We thus see that $(w^{-1}\pi)^{p-1} = -p$, and so $w^{-1}\pi = (-p)^{1/(p-1)}$. This completes the proof. (Note that both fields have degree $p-1$ over $\mathbf{Q}_p$, so this containment shows that they are equal.) $\square$

3. Kummer theory

We will now prove the basic results of Kummer theory, which we will need for the proof of Kronecker–Weber, and in the remainder of the course. This will also allow us to see a small bit of group cohomology, which will figure prominently later.

Let G be a group and let M be a G-module. A **1-cocycle** of G with values in M is a function $f\colon G \to M$ satisfying $f(gh) = f(g) + gf(h)$. A **1-coboundary** is a function of the form $f(g) = gx - x$ for some $x \in M$. One readily verifies that the collection of 1-cocycles forms a group (under pointwise addition), and that the set of 1-coboundaries forms a subgroup. The quotient group, denote $\mathrm{H}^1(G, M)$, is the first group cohomology of G with coefficients in M.

The subject of **Galois cohomology** studies group cohomology in the setting where G is the Galois group of a field extension and M is somehow related to the fields involved. The first result in this subject is the following:

Theorem 3.1 (Hilbert's Theorem 90)**.** *Let L/K be a finite Galois extension with group G. Then $\mathrm{H}^1(G, L^\times) = 0$.*

Proof. Let $f\colon G \to L^\times$ be a 1-cocycle; we now use multiplicative notation, so that $f(gh) = {}^g f(h) \cdot f(g)$. The functions $g\colon L \to L$, for $g \in G$, are L-linear independent (exercise). Thus linear combination $\sum_{g\in G} f(g)\cdot {}^g(-)$ is non-zero. Let $x \in L^\times$ be such that $y = \sum_{g\in G} {}^g x \cdot f(g) \neq 0$. But then

$$ {}^h y = \sum_{g\in G} {}^{hg} x^h f(g) = \sum_{g\in G} {}^{hg} x f(hg) f(h)^{-1} = f(h)^{-1} y,$$

and so $f(h) = y \cdot {}^h y^{-1}$, proving that f is a 1-coboundary. □

Theorem 3.2 (Kummer Theory, version 1)**.** *Let K be a field containing all nth roots of unity, and suppose that $p \nmid n$ where $p = \mathrm{char}(K)$. Let L/K be a Galois extension with group $\mathbf{Z}/n\mathbf{Z}$. Then $L = K(a^{1/n})$ for some $a \in K$.*

Proof. Let $\sigma \in G$ be a generator, let $\mu_n \subset K$ be the group of nth roots of unity, and let $\zeta \in \mu_n$ be a generator. Let $f\colon G \to \mu_n \subset L^\times$ be the isomorphism given by $f(\sigma) = \zeta$. Then f is a 1-cocycle and so by Hilbert's Theorem 90, there exists $b \in L^\times$ such that $f(\sigma^i) = (\sigma^i b)/b$ for all i. In particular, with $i = 1$ we see that $\sigma b = \zeta b$, and so $\sigma(b^n) = b^n$. Thus $a = b^n$ is fixed by G, and so belongs to K. No smaller power of b belongs to K since ζ is primitive. Thus $L = K(b) = K(a^{1/n})$. □

The theorem can also be phrased in the following manner using the absolute Galois group $G_K = \mathrm{Gal}(\overline{K}/K)$.

Theorem 3.3 (Kummer Theory, version 2)**.** *With the same hypotheses as the previous theorem, we have a canonical isomorphism*

$$\varphi\colon K^\times/(K^\times)^n \to \mathrm{Hom}(G_K, \mu_n), \qquad \varphi(a) = (g \mapsto g(a^{1/n})/a^{1/n})$$

Note that $\mu_n \cong \mathbf{Z}/n\mathbf{Z}$ once we choose a primitive nth root of unity.

Proof. We first verify that φ is a well-defined group homomorphism. Let $a \in K^\times$. Then $a^{1/n} \in \overline{K}$, and so it makes sense to apply elements of G_K to it. Since $g(a^{1/n})$ is also an nth root of a, we have $g(a^{1/n})/a^{1/n} \in \mu_n$. Since $\mu_n \subset K$, the value of $g(a^{1/n})/a^{1/n}$ is independent of the choice of nth root of a. Furthermore, it clearly only depends on a in $K^\times/(K^\times)^n$. Thus

$\varphi(a)$ is well-defined, and one verifies that it is a homomorphism $G_K \to \mu_n$. Finally, it is easy to see that $\varphi(ab) = \varphi(a)\varphi(b)$, and so φ is a homomorphism.

We now show that φ is injective. Suppose that a belongs to the kernel, that is, $g(a^{1/n})/a^{1/n} = 1$ for all $g \in G_K$. Then $a^{1/n} \in K$, and so $a \in (K^\times)^n$. Thus $a = 1$ in the quotient $K^\times/(K^\times)^n$, as required.

Finally we show that φ is surjective. Thus let $f\colon G_K \to \mu_n$ be given. Basic facts about profinite gruops imply that f factors through $\mathrm{Gal}(L/K)$ for some finite Galois extension L/K; write still $f\colon \mathrm{Gal}(L/K) \to \mu_n$ for this map. As this is a 1-cocycle, Hilbert's Theorem 90 implies it is a 1-coboundary, and so there is $b \in L$ such that $f(\sigma) = \sigma b/b$ for all $\sigma \in \mathrm{Gal}(L/K)$. Since $f(\sigma) \in \mu_n$, we thus have $\sigma(b^n) = b^n$ for all σ, and so $a = b^n$ belongs to K. Thus $f(\sigma) = \sigma(a^{1/n})/a^{1/n}$, as required. □

Remark 3.4. The homomorphism φ can be converted into a pairing

$$\langle , \rangle\colon G_K \times K^\times/(K^\times)^n \to \mu_n, \qquad \langle g, a\rangle = g(a^{1/n})/a^{1/n}$$

Kummer theory asserts that this is a perfect pairing after replacing G_K with $G_K^{\mathrm{ab}} \otimes \mathbf{Z}/n\mathbf{Z}$. □

If K does not contain the nth roots of unity, classifying $\mathbf{Z}/n\mathbf{Z}$-extensions of K is difficult; in fact, this problem (for K a number field) is the subject of this course. There is one thing we can say using Kummer theory, however.

Proposition 3.5. *Let n be an odd prime power. Let K be a field of characteristic prime to n, let $L = K(\zeta_n)$, and let $M = L(a^{1/n})$ for some $a \in L^\times$. Consider the map*

$$\varphi\colon \mathrm{Gal}(L/K) \to L^\times/(L^\times)^n, \qquad \varphi(g) = {}^g a/a^{\chi(g)},$$

where χ is the cyclcotomic character. Then the following conditions are equivalent:

(a) M/K is an abelian extension.
(b) $\varphi(g) = 1$ for all g.

Proof. If (b) holds then all $g \in \mathrm{Gal}(L/K)$ we see that $L(({}^g a)^{1/n})) = L(a^{\chi(g)/n}) = L(a^{1/n})$, and so M/K is Galois. Of course, if (a) holds then M/K is Galois too. It thus suffices to assume M/K is Galois and prove that it is abelian if and only if $\varphi = 1$.

Let $A \subset L^\times/(L^\times)^n$ be the subgroup generate by a. By Kummer theory, the Kummer pairing

$$\langle , \rangle\colon \mathrm{Gal}(M/L) \times A \to \mu_n, \qquad \langle g, b\rangle = g(b^{1/n})/b^{1/n}$$

is a perfect bilinear pairing. It is also equivariant for $\mathrm{Gal}(L/K)$, in the following sense: if $g \in \mathrm{Gal}(L/K)$ and $h \in \mathrm{Gal}(M/L)$ then

$${}^g\langle h, b\rangle = \langle {}^g h, {}^g b\rangle,$$

where ${}^g h = ghg^{-1}$; indeed, lifting g to $\mathrm{Gal}(M/K)$, we have

$${}^g\langle h, b\rangle = {}^g\left(\frac{{}^h(b^{1/n})}{b^{1/n}}\right) = \frac{{}^{ghg^{-1}g}(b^{1/n})}{{}^g(b^{1/n})} = \langle {}^g h, {}^g b\rangle.$$

On the other hand, the value of the Kummer pairing is a root of unity, and so $\mathrm{Gal}(M/K)$ acts on it through the cyclotomic character. Thus, with g and h as above, we have

$$\langle {}^g h, {}^g b\rangle = {}^g\langle h, b\rangle = \langle h, b\rangle^{\chi(g)} = \langle h, b^{\chi(g)}\rangle.$$

Since the Kummer pairing is perfect, we see that ${}^g h = h$ holds for all h if and only if ${}^g b = b^{\chi(g)}$ holds (in A) for all $b \in A$. We thus see that $\mathrm{Gal}(L/K)$ acts trivially on $\mathrm{Gal}(M/L)$ if and only if $\varphi = 1$.

Now observe that $\mathrm{Gal}(L/K)$ acts trivially on $\mathrm{Gal}(M/L)$ if and only if $\mathrm{Gal}(M/K)$ is abelian. Indeed, if $\mathrm{Gal}(M/K)$ is abelian, this is obvious. For the reverse direction, observe that $\mathrm{Gal}(L/K) \subset (\mathbf{Z}/n\mathbf{Z})^\times$ and $\mathrm{Gal}(M/L) \subset \mu_n$ are cyclic groups (this is where it is important that n is an odd prime power). Let $h \in \mathrm{Gal}(M/L)$ be a generator, and let $g \in \mathrm{Gal}(M/K)$ be a lift of a generator. Since the action is trivial, g and h commute. But these elements generate $\mathrm{Gal}(M/K)$, and so it's abelian. □

Exercise 3.6. *Since $\mathbf{Q}_p$ contains all $(p-1)$st roots of unity, Kummer theory gives an isomorphism*

$$G_{\mathbf{Q}_p}^{\mathrm{ab}} \otimes \mathbf{Z}/(p-1)\mathbf{Z} \cong \mathrm{Hom}(\mathbf{Q}_p^\times/(\mathbf{Q}_p^\times)^{p-1}, \mu_{p-1}).$$

We have a canonical short exact sequence

$$0 \to \mu_{p-1} \to \mathbf{Q}_p^\times/(\mathbf{Q}_p^\times)^{p-1} \xrightarrow{v} \mathbf{Z}/(p-1)\mathbf{Z} \to 0.$$

Applying $\mathrm{Hom}(-, \mu_{p-1})$*, we thus obtain a canonical exact sequence*

$$0 \to \mu_{p-1} \to G_{\mathbf{Q}_p}^{\mathrm{ab}} \otimes \mathbf{Z}/(p-1)\mathbf{Z} \to \mathbf{Z}/(p-1)\mathbf{Z} \to 0.$$

Show that μ_{p-1} is the tame inertia group I^t, and that the natural map $I^t \to \mu_{p-1}$ discussed in the previous section is the identity. Show also that the natural generator of the above $\mathbf{Z}/(p-1)\mathbf{Z}$ is the Frobenius element.

References

[K] K. Kedlaya. Notes on class field theory.
http://www.math.mcgill.ca/darmon/courses/cft/refs/kedlaya.pdf

[W] L. Washington. *Introduction to Cyclotomic Fields*, Chapter 14