Math 254B, UC Berkeley, Spring 2002 (Kedlaya)
Kummer Theory

Reference. Serre, *Local Fields*, Chapter X, or just about any advanced algebra text (e.g., Lang's book). The last lemma is from Washington, *Introduction to Cyclotomic Fields*, Chapter 14.

Jargon watch. If G is a group, a *G-extension* of a field K is a Galois extension of K with Galois group G.

Before attempting to classify all abelian extensions of $\mathbb{Q}_p$, we recall an older classification result due to Kummer. This result will continue to be useful as we proceed to class field theory in general, and the technique in its proof prefigures the role to be played by group cohomology down the line. So watch carefully!

Theorem 1 (Kummer). *If $\zeta_n \in K$, then every $\mathbb{Z}/n\mathbb{Z}$-extension of K is of the form $K(\alpha^{1/n})$ for some $\alpha \in K^*$ with the property that $\alpha^{1/d} \notin K$ for any proper divisor d of n, and vice versa.*

I don't actually know how Kummer proved this; nowadays one uses the following. If G is a group and M is an abelian group on which G acts (written multiplicatively), one defines the group $H^1(G, M)$ as the set of functions $f : G \to M$ such that $f(gh) = f(g)^h f(h)$, modulo the set of such functions of the form $f(g) = x^g x^{-1}$ for some $x \in M$. (This is our first example of *group cohomology*; more on this later.)

Lemma 2 ("Hilbert's Theorem 90"). *Let L/K be a finite Galois extension with Galois group G. Then $H^1(G, L^*) = 0$.*

Proof. Let f be a function of the form described above. By the linear independence of automorphisms (see exercises), there exists $x \in L$ such that $t = \sum_{g\in G} x^g f(g)$ is nonzero. But now

$$t^h = \sum_{g\in G} x^{gh} f(g)^h = \sum_{g\in G} x^{gh} f(gh) f(h)^{-1} = f(h)^{-1} t.$$

Thus f is zero in $H^1(G, L^*)$. $\square$

Proof of Kummer's Theorem. On one hand, if $\alpha \in K^*$ is such that $\alpha^{1/d} \notin K$ for any proper divisor d of n, then the polynomial $x^n - \alpha$ is irreducible over K, and every automorphism must have the form $\alpha \mapsto \alpha\zeta_n^r$ for some $r \in \mathbb{Z}/n\mathbb{Z}$. Thus $\mathrm{Gal}(K(\alpha^{1/n})/K) \cong \mathbb{Z}/n\mathbb{Z}$.

On the other hand, let L be an arbitrary $\mathbb{Z}/n\mathbb{Z}$-extension of K. Choose a generator $g \in \mathrm{Gal}(L/K)$, and let $f : \mathrm{Gal}(L/K) \to L^*$ be the map that sends rg to ζ_n^r for $r \in \mathbb{Z}$. Then $f \in H^1(\mathrm{Gal}(L/K), L^*)$, so there exists $t \in L$ such that $t^{rg}/t = f(rg) = \zeta_n^r$ for $r \in \mathbb{Z}$. In particular, t^n is invariant under $\mathrm{Gal}(L/K)$, so $t^n = \alpha$ for some $\alpha \in K$ and $L = K(t) = K(\alpha^{1/n})$, as desired. $\square$

Another way to state Kummer's theorem is as a bijection

$$(\mathbb{Z}/n\mathbb{Z})^r\text{-extensions of } K \leftrightarrow (\mathbb{Z}/n\mathbb{Z})^r\text{-subgroups of } K^*/(K^*)^n.$$

(What we proved above was the case $r = 1$, but the general case follows easily.) Another way is in terms of the absolute Galois group of K. Define the *Kummer pairing*

$$\langle \cdot, \cdot \rangle : \mathrm{Gal}(\overline{K}/K) \times K^* \to \{1, \zeta_n, \dots, \zeta_n^{n-1}\}$$

as follows: given $\sigma \in \mathrm{Gal}(\overline{K}/K)$ and $z \in K^*$, choose $y \in \overline{K}^*$ such that $y^n = z$, and put $\langle \sigma, z \rangle = y^\sigma / y$. Note that this does not depend on the choice of y: the other possibilities are $y\zeta_n^k$ for $k = 0, \dots, n-1$, and $\zeta_n^\sigma = \zeta_n$ by the assumption on K, so it drops out.

Theorem 3 (Kummer reformulated). *The Kummer pairing induces an isomorphism*

$$K^*/(K^*)^n \to \mathrm{Hom}(\mathrm{Gal}(\overline{K}/K), \mathbb{Z}/n\mathbb{Z}).$$

Proof. The map comes from the pairing; we have to check it's injective and surjective. If $y \in K^* \setminus (K^*)^n$, then $K(y^{1/n})$ is a nontrivial Galois extension of K, so there exists some element of $\mathrm{Gal}(K(y^{1/n})/K)$ that doesn't preserve $y^{1/n}$. Any lift of that element to $\mathrm{Gal}(\overline{K}/K)$ pairs with y to give something other than 1; that is, y induces a nonzero homomorphism of $\mathrm{Gal}(\overline{K}/K)$ to $\mathbb{Z}/n\mathbb{Z}$. Thus injectivity follows.

On the other hand, suppose $f : \mathrm{Gal}(\overline{K}/K) \to \mathbb{Z}/n\mathbb{Z}$ is a homomorphism whose image is the cyclic subgroup of $\mathbb{Z}/n\mathbb{Z}$ of order d. Let H be the kernel of f; then the fixed field L of H is a $\mathbb{Z}/d\mathbb{Z}$-extension of K with Galois group $\mathrm{Gal}(\overline{K}/K)/H$. By Kummer theory, $L = K(y^{1/d})$ for some y. But now the homomorphisms induced by $y^{mn/d}$, as m runs over all integers coprime to d, give all possible homomorphisms of $\mathrm{Gal}(\overline{K}/K)/H$ to $\mathbb{Z}/d\mathbb{Z}$, so one of them must equal f. Thus surjectivity follows. $\square$

But what about $\mathbb{Z}/n\mathbb{Z}$-extensions of a field that does not contains ζ_n? These are harder to describe, and indeed describing such extensions of $\mathbb{Q}$ is the heart of this course. There is one thing one can say: if L/K is a $\mathbb{Z}/n\mathbb{Z}$-extension, so is $L(\zeta_n)/K$, and the latter is a Kummer extension.

Lemma 4. *Let K be a field of characteristic coprime to n, let $L = K(\zeta_n)$, and let $M = L(a^{1/n})$ for some $a \in L^*$. Define the homomorphism $\omega : \mathrm{Gal}(L/K) \to (\mathbb{Z}/n\mathbb{Z})^*$ by the relation $\zeta_n^{\omega(g)} = \zeta_n^g$. Then M/K is Galois and abelian if and only if*

$$a^g / a^{\omega(g)} \in (L^*)^n \qquad \forall g \in \mathrm{Gal}(M/K). \tag{1}$$

Note that $\omega(g)$ is only defined up to adding a multiple of n, so $a^{\omega(g)}$ is only defined up to an n-th power, i.e., modulo $(M^*)^n$.

Proof. If $a^g/a^{\omega(g)} \in (L^*)^n$ for all $g \in \mathrm{Gal}(M/K)$, then a, $a^{\omega(g)}$ and a^g all generate the same subgroup of $(L^*)/(L^*)^n$. Thus $L(a^{1/n}) = L((a^g)^{1/n})$ for all $g \in \mathrm{Gal}(M/K)$, so M/K is Galois.

Thus it suffices to assume M/K is Galois, then prove that M/K is abelian if and only if (1) holds. In this case, we must have $a^g/a^{\rho(g)} \in (M^*)^n$ for some map $\rho : \mathrm{Gal}(M/K) \to (\mathbb{Z}/n\mathbb{Z})^*$.

Note that $\mathrm{Gal}(M/K)$ has a homomorphism ω to a cyclic group whose kernel $\mathrm{Gal}(M/L) \subseteq \mathbb{Z}/n\mathbb{Z}$ is also abelian. Thus $\mathrm{Gal}(M/K)$ is abelian if and only if g and h commute for any $g \in \mathrm{Gal}(M/K)$ and $h \in \mathrm{Gal}(M/L)$, i.e., if $h = ghg^{-1}$. (Since g commutes with powers of itself, g then commutes with everything.)

Let $A \subseteq L^*/(L^*)^n$ be the subgroup generated by a. Then the Kummer pairing gives rise to a pairing

$$\mathrm{Gal}(M/L) \times A \to \{1, \zeta_{n-1}, \dots, \zeta_n^{n-1}\}$$

which is bilinear and nondegenerate, so $h = ghg^{-1}$ if and only if $\langle h, s^g \rangle = \langle ghg^{-1}, s^g \rangle$ for all $s \in A$. But the Kummer pairing is *equivariant* with respect to $\mathrm{Gal}(L/K)$ as follows:

$$\langle h, s \rangle^g = \langle g^{-1}hg, s^g \rangle,$$

because

$$\left(\frac{(s^{1/n})^h}{s^{1/n}}\right)^g = \frac{((s^g)^{1/n})^{g^{-1}hg}}{(s^g)^{1/n}}.$$

(Here by $s^{1/n}$ I mean an arbitrary n-th root of s in M, and by $(s^g)^{1/n}$ I mean $(s^{1/n})^g$. Remember the value of the Kummer pairing doesn't depend on which n-th root you choose.) Thus $h = ghg^{-1}$ if and only if $\langle h, s^g \rangle = \langle h, s \rangle^g$ for all $s \in A$, or equivalently, just for $s = a$. But

$$\langle h, a \rangle^g = \langle h, a \rangle^{\omega(g)} = \langle h, a^{\omega(g)}.$$

Thus g and h commute if and only if $\langle h, a^g \rangle = \langle h, a^{\omega(g)}$, if and only if (by nondegeneracy) $a^g/a^{\omega(g)} \in (L^*)^n$, as desired. $\square$

Exercises.

1. Prove the linear independence of automorphisms: if $g_1, \dots, g_n$ are distinct automorphisms of L over K, then there do not exist $x_1, \dots, x_n \in L$ such that $x_1 y^{g_1} + \cdots + x_n y^{g_n} = 0$ for all $y \in L$. (Hint: suppose the contrary, choose a counterexample with n as small as possible, then make an even smaller counterexample.)

2. Prove the additive analogue of Hilbert's Theorem 90: if L/K is a finite Galois extension with Galois group G, then $H^1(G, L) = 0$, where the abelian group is now the additive group of L. (Hint: by the normal basis theorem (see for example Lang, *Algebra*), there exists $\alpha \in L$ whose conjugates form a basis of L as a K-vector space.)

3. (Optional) If L/K is a finite Galois extension with Galois group G, then $H^1(G, \mathrm{GL}(n, L)) = 0$. (Hint: the hard part is proving that the thing that you get from independence of automorphisms is actually an *invertible* matrix. Show in fact that the matrices you can get satisfy no L-linear relations.)