Math 254B, UC Berkeley, Spring 2002 (Kedlaya)
The Local Kronecker-Weber Theorem

Reference. Washington, *Introduction to Cyclotomic Fields*, Chapter 14.

We now prove the local Kronecker-Weber theorem, modulo some steps which will be left as exercises. As shown previously, this will imply the original Kronecker-Weber theorem.

Theorem 1 (Local Kronecker-Weber). *If $K/\mathbb{Q}_p$ is a finite abelian extension, then $K \subseteq \mathbb{Q}_p(\zeta_n)$ for some positive integer n.*

Since $\mathrm{Gal}(K/\mathbb{Q}_p)$ decomposes into a product of cyclic groups of prime power order, by the structure theorem for finite abelian groups, we may write K as the compositum of extensions of $\mathbb{Q}_p$ whose Galois groups are cyclic of prime power order. In other words, it suffices to prove local Kronecker-Weber under the assumption that $\mathrm{Gal}(K/\mathbb{Q}_p) \cong \mathbb{Z}/q^r\mathbb{Z}$ for some prime q and some $r \in \mathbb{N}$.

First recall the following facts from last semester.

Lemma 2. *Let L/K be an unramified extension of finite extensions of $\mathbb{Q}_p$. Then $L = K(\zeta_{q-1})$, where q is the cardinality of the residue field of L.*

Lemma 3. *Let L/K be a totally and tamely ramified extension of finite extensions of $\mathbb{Q}_p$ of degree e. (Recall that tamely ramified means that p does not divide e.) Then there exists a generator π of the maximal ideal of the valuation ring of K such that $L = K(\pi^{1/e})$.*

Lemma 4. *The fields $\mathbb{Q}_p((-p)^{1/(p-1)})$ and $\mathbb{Q}_p(\zeta_p)$ are equal.*

We now proceed to the proof of the local Kronecker-Weber theorem.

Case 1: $q \neq p$.

Let L be the maximal unramified subextension of K. By Lemma 2, $L = \mathbb{Q}_p(\zeta_n)$ for some n. Let $e = [K : L]$. Since e is a power of q, e is not divisible by p, so K is totally and tamely ramified over L. Thus by Lemma 3, there exists $\pi \in L$ generating the maximal ideal of $\mathfrak{o}_L$ such that $K = L(\pi^{1/e})$. Since $L/\mathbb{Q}_p$ is unramified, p also generates the maximal ideal of $\mathfrak{o}_L$, so we can write $\pi = -pu$ for some unit $u \in \mathfrak{o}_L^*$. Now $L(u^{1/e})/L$ is unramified since e is prime to p and u is a unit. In particular, $L(u^{1/e})/\mathbb{Q}_p$ is unramified, hence abelian. Then $K(u^{1/e})/\mathbb{Q}_p$ is the compositum of the two abelian extensions $K/\mathbb{Q}_p$ and $L(u^{1/e})/\mathbb{Q}_p$, so it's also abelian. Hence any subextension is abelian, in particular $\mathbb{Q}_p((-p)^{1/e})/\mathbb{Q}_p$.

For $\mathbb{Q}_p((-p)^{1/e})/\mathbb{Q}_p$ to be Galois, it must contain the e-th roots of unity (since it must contain all of the e-th roots of $-p$, and we can divide one by another to get an e-th root of unity). But $\mathbb{Q}_p((-p)^{1/e})/\mathbb{Q}_p$ is totally ramified, whereas $\mathbb{Q}_p(\zeta_e)/\mathbb{Q}_p$ is unramified. This is a contradiction unless $\mathbb{Q}_p(\zeta_e)$ is actually equal to $\mathbb{Q}_p$, which only happens if $e|p-1$ (since the residue field $\mathbb{F}_p$ of $\mathbb{Q}_p$ contains only $(p-1)$-st roots of unity).

Now $K \subseteq L((-p)^{1/e}, u^{1/e})$ as noted above. But on one hand, $L(u^{1/e})$ is unramified over L, so $L(u^{1/e}) = L(\zeta_m)$ for some m; on the other hand, because $e|(p-1)$, we have $\mathbb{Q}_p((-p)^{1/e}) \subseteq \mathbb{Q}_p((-p)^{1/(p-1)}) = \mathbb{Q}_p(\zeta_p)$ by Lemma 4. Putting it all together,

$$K \subseteq L((-p)^{1/e}, u^{1/e}) \subseteq \mathbb{Q}_p(\zeta_n, \zeta_p, \zeta_m) \subseteq \mathbb{Q}_p(\zeta_{mnp}).$$

Case 2: $q = p \neq 2$.

Before proceeding, recall a lemma from Kummer theory (previous handout).

Lemma 5. *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*

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

Suppose $\mathrm{Gal}(K/\mathbb{Q}_p) \cong \mathbb{Z}/p^r\mathbb{Z}$. We can use roots of unity to construct two other extensions of $\mathbb{Q}_p$ with this Galois group. Namely, $\mathbb{Q}_p(\zeta_{p^{p^r}-1})/\mathbb{Q}_p$ is unramified of degree p^r, and automatically has cyclic Galois group; meanwhile, the index $p-1$ subfield of $\mathbb{Q}_p(\zeta_{p^{r+1}})$ is ramified with Galois group $\mathbb{Z}/p^r\mathbb{Z}$. By assumption, K is not contained in the compositum of these two fields, so $\mathrm{Gal}(K(\zeta_{p^{p^r}-1}, \zeta_{p^{r+1}})/\mathbb{Q}_p) \cong (\mathbb{Z}/p^r\mathbb{Z})^2 \times \mathbb{Z}/p^s\mathbb{Z}$ for some $s > 0$. This group admits $(\mathbb{Z}/p\mathbb{Z})^3$ as a quotient, so we have an extension of $\mathbb{Q}_p$ with Galois group $(\mathbb{Z}/p\mathbb{Z})^3$. It thus suffices to prove the following lemma.

Lemma 6. *For $p \neq 2$, there is no extension of $\mathbb{Q}_p$ with Galois group $(\mathbb{Z}/p\mathbb{Z})^3$.*

Proof. For convenience, put $\pi = \zeta_p - 1$. Then π is a uniformizer of $\mathbb{Q}_p(\zeta_p)$.

If $\mathrm{Gal}(K/\mathbb{Q}_p) \cong (\mathbb{Z}/p\mathbb{Z})^3$, then $\mathrm{Gal}(K(\zeta_p)/\mathbb{Q}_p(\zeta_p)) \cong (\mathbb{Z}/p\mathbb{Z})^3$ as well, and $K(\zeta_p)$ is abelian over $\mathbb{Q}_p$ with Galois group $(\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/p\mathbb{Z})^3$. We can apply Kummer theory to $K(\zeta_p)/\mathbb{Q}_p(\zeta_p)$; it gives us a subgroup $B \subseteq \mathbb{Q}_p(\zeta_p)^*/(\mathbb{Q}_p(\zeta_p)^*)^p$ isomorphic to $(\mathbb{Z}/p\mathbb{Z})^3$ such that $K(\zeta_p) = \mathbb{Q}_p(\zeta_p, B^{1/p})$. Let $\omega : \mathrm{Gal}(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p) \to (\mathbb{Z}/p\mathbb{Z})^*$ be the canonical map; by the previous lemma,

$$b^g/b^{\omega(g)} \in (\mathbb{Q}_p(\zeta_p)^*)^p \qquad \forall b \in B, g \in \mathrm{Gal}(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p),$$

since $\mathbb{Q}_p(\zeta_p, b^{1/p}) \subseteq K(\zeta_p)$ is also abelian over $\mathbb{Q}_p$.

Recall the structure of $\mathbb{Q}_p(\zeta_p)^*$. The maximal ideal of $\mathbb{Z}_p[\zeta_p]$ is generated by π, while each unit of $\mathbb{Z}_p[\zeta_p]$ is congruent to a $p-1$-st root of unity modulo π. Thus

$$\mathbb{Q}_p(\zeta_p)^* = \pi^{\mathbb{Z}} \times (\zeta_{p-1})^{\mathbb{Z}} \times U_1,$$

where U_1 denotes the set of units of $\mathbb{Z}_p[\zeta_p]$ congruent to 1 modulo π, and correspondingly

$$(\mathbb{Q}_p(\zeta_p)^*)^p = \pi^{p\mathbb{Z}} \times (\zeta_{p-1})^{p\mathbb{Z}} \times U_1^p.$$

Now choose a representative $a \in L^*$ of some nonzero element of B; without loss of generality, we may assume $a = \pi^m u$ for some $m \in \mathbb{Z}$ and $u \in U_1$. Then

$$\frac{a^g}{a^{\omega(g)}} = \frac{(\zeta_p^{\omega(g)} - 1)^m}{\pi^{m\omega(g)}} \frac{u^g}{u^{\omega(g)}};$$

but $v_\pi(\pi) = v_\pi(\zeta_p^{\omega(g)} - 1) = 1$. Thus the valuation of the right hand side is $m(1 - \omega(g))$, which can only be a multiple of p for all g if $m \equiv 0 \pmod p$. (Notice we just used that p is odd!) That is, we could have taken $m = 0$ and $a = u \in U_1$.

As for $u^g/u^{\omega(g)}$, note that U_1^p is precisely the set of units congruent to 1 modulo π^{p+1} (see exercises). Since $\zeta_p = 1+\pi+O(\pi^2)$, we can write $u = \zeta_p^b(1+c\pi^d+O(\pi^{d+1}))$, with $c \in \mathbb{Z}$ and $d \geq 2$. Since $\pi^g/\pi \equiv \omega(g) \pmod{\pi}$, we get

$$u^g = \zeta_p^{b\omega(g)}(1+c\omega(g)^d\pi^d + O(\pi^{d+1})), \quad u^{\omega(g)} = \zeta_p^{b\omega(g)}(1+c\omega(g)\pi^d + O(\pi^{d+1})).$$

But these two have to be congruent modulo π^{p+1}. Thus either $d \geq p+1$ or $d \equiv 1 \pmod{p-1}$, the latter only occurring for $d = p$.

What this means is that the set of possible u is generated by ζ_p and by $1+\pi^p$. But these only generate a subgroup of U_1/U_1^p isomorphic to $(\mathbb{Z}/p\mathbb{Z})^2$, whereas $B \cong (\mathbb{Z}/p\mathbb{Z})^3$. Contradiction. $\square$

Case 3: $p = q = 2$. This case is similar to the previous case, but a bit messier, because $\mathbb{Q}_2$ does admit an extension with Galois group $(\mathbb{Z}/2\mathbb{Z})^3$. We defer this case to the exercises.

Exercises.

1. Prove that (in the notation of Lemma 6) U_1^p is the set of units congruent to 1 modulo π^{p+1}. (Hint: in one direction, write $u \in U_1$ as a power of ζ_p times a unit congruent to 1 modulo π^2. In the other direction, use the binomial series for $(1+x)^{1/p}$.)

2. Prove that for any $r > 0$, there is an extension of $\mathbb{Q}_2$ with Galois group $\mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/2^r\mathbb{Z})^2$ contained in $\mathbb{Q}_2(\zeta_n)$ for some $n > 0$.

3. Suppose that $K/\mathbb{Q}_2$ is a $\mathbb{Z}/2^r\mathbb{Z}$-extension not contained in $\mathbb{Q}_2(\zeta_n)$ for any $n > 0$. Prove that there exists an extension of $\mathbb{Q}_2$ with Galois group $(\mathbb{Z}/2\mathbb{Z})^4$ or $(\mathbb{Z}/4\mathbb{Z})^3$.

4. Prove that there is no extension of $\mathbb{Q}_2$ with Galois group $(\mathbb{Z}/2\mathbb{Z})^4$. (Hint: use Kummer theory.)

5. Prove that there is no extension of $\mathbb{Q}_2$ with Galois group $(\mathbb{Z}/4\mathbb{Z})^3$. (Hint: reduce to showing that there exists no extension of $\mathbb{Q}_2$ containing $\mathbb{Q}_2(\sqrt{-1})$ with Galois group $\mathbb{Z}/4\mathbb{Z}$.)