MATH 776
THE KRONECKER–WEBER THEOREM

ANDREW SNOWDEN

1. The local Kronecker–Weber theorem

We are now ready to prove the local theorem:

Theorem 1.1. *Any finite abelian extension of $\mathbf{Q}_p$ is contained in $\mathbf{Q}_p(\zeta_n)$ for some n.*

Let $K/\mathbf{Q}_p$ be a finite abeian extension with Galois group G. By the structure theorem for finite abelian groups, $G \cong \prod_{i=1}^n G_i$ where each G_i is cyclic of prime power order. Let K_i be the field correspond to the quotient $G \to G_i$. As K is the compositum of the K_i, it suffices to prove the theorem for each K_i. Thus, relabeling, we may as well assume that G itself is of prime power order, say $G = \mathbf{Z}/q^r\mathbf{Z}$ for some prime q.

Case 1: $q \neq p$**.** Since G is prime to p, the extension $K/\mathbf{Q}_p$ is tamely ramified. We can thus write $K = L(\pi^{1/e})$, where L/K is unramified, π is a uniformizer of L, and e is the ramification index of $K/\mathbf{Q}_p$; we know that L contains all eth roots of unity. We have a split short exact sequence

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Gal}(K/L) & \longrightarrow & G & \longrightarrow & \mathrm{Gal}(L/\mathbf{Q}_p) & \longrightarrow & 0 \\ & & \Vert & & & & \Vert & & \\ & & \mu_e & & & & \mathbf{Z}/f\mathbf{Z} & & \end{array}$$

and so $G \cong (\mathbf{Z}/f\mathbf{Z}) \ltimes \mu_e$. As we explained last time, the generator (Frobenius) of $\mathrm{Gal}(L/\mathbf{Q}_p)$ acts by $x \mapsto x^p$ on μ_e. Since G is abelian, this action must be trivial; that is, we must have $x = x^p$ for all eth roots of unity. It follows that $e \mid p-1$.

Since L/K is unramified, p is a uniformizer of L, and so we can write $\pi = up$ for a unit u of L. We have

$$K = L((pu)^{1/e}) \subset L((-u)^{1/e}, (-p)^{1/e}).$$

Since e is prime to p, the extension $L((-u)^{1/e})/L$ is unramified, and thus unramified over $\mathbf{Q}_p$, and so $L((-u)^{1/e}) \subset \mathbf{Q}_p(\zeta_m)$ for some m prime to p. On the other hand, we have

$$\mathbf{Q}_p((-p)^{1/e}) \subset \mathbf{Q}_p((-p)^{1/(p-1)}) = \mathbf{Q}_p(\zeta_p),$$

where the containment comes from the fact that e divides $p-1$, and the equality was proved last time. We thus see that $K \subset \mathbf{Q}_p(\zeta_{mp})$, which completes the proof.

Case 2: $q = p \neq 2$**.** We have $G \cong \mathbf{Z}/p^r\mathbf{Z}$. Let $L_1/\mathbf{Q}_p$ be the unique unramified extension of degree p^r, let $L_2/\mathbf{Q}_p$ be the unique subextension of $\mathbf{Q}_p(\zeta_{p^{r+1}})/\mathbf{Q}_p$ with Galois group $\mathbf{Z}/p^r\mathbf{Z}$,

Date: January 29, 2019.

and let $L = L_1 L_2$ be their compositum. Since $L_1/\mathbf{Q}_p$ is unramified and $L_2/\mathbf{Q}_p$ is totally ramified, the natural map

$$\mathrm{Gal}(L/\mathbf{Q}_p) \to \mathrm{Gal}(L_1/\mathbf{Q}_p) \times \mathrm{Gal}(L_2/\mathbf{Q}_p) \cong (\mathbf{Z}/p^r\mathbf{Z})^2$$

is an isomorphism. We claim that K is contained in L, which will prove the theorem. Suppose not. Consider the injective map

$$\mathrm{Gal}(KL/\mathbf{Q}_p) \to \mathrm{Gal}(L/\mathbf{Q}_p) \times \mathrm{Gal}(K/\mathbf{Q}_p) \cong (\mathbf{Z}/p^r\mathbf{Z})^3.$$

The image is a subgroup of $(\mathbf{Z}/p^r\mathbf{Z})^3$ that surjects onto $(\mathbf{Z}/p^r\mathbf{Z})^2$, but is strictly larger than this group. It follows that $\mathrm{Gal}(KL/\mathbf{Q}_p)$ has a quotient of the form $(\mathbf{Z}/p\mathbf{Z})^3$. This yields a Galois extension of $\mathbf{Q}_p$ with this group. Thus to complete the proof, it suffices to prove the following:

Proposition 1.2. *There is no Galois extension of $\mathbf{Q}_p$ with group $(\mathbf{Z}/p\mathbf{Z})^3$ (assuming $p \neq 2$).*

We do this in the following section.

Case 3: $q = p = 2$**.** This is similar to Case 2 but somewhat more complicated. We leave it as an exercise.

2. Proof of Proposition 1.2

To prove the proposition, we need to establish some basic facts about the field $\mathbf{Q}_p(\zeta_p)$, which we denote by F. We let $\pi = 1 - \zeta_p$, which is a uniformizer of F, and we let $G = \mathrm{Gal}(F/\mathbf{Q}_p)$. The cyclotomic character $\chi \colon G \to (\mathbf{Z}/p\mathbf{Z})^\times$ is an isomorphism.

Lemma 2.1. *For $g \in G$ we have ${}^g\pi = \chi(g)\pi \pmod{\pi^2}$.*

Proof. We have ${}^g\pi = 1 - \zeta_p^{\chi(g)}$, and so

$$\frac{{}^g\pi}{\pi} = \frac{1 - \zeta_p^{\chi(g)}}{1 - \zeta_p} = 1 + \zeta_p + \cdots + \zeta_p^{\chi(g)-1}.$$

Since each term on the right is a p-power root of unity, and thus congruent to 1 modulo π, the entire right side is congruent to $\chi(g)$ modulo π. The result follows. □

Lemma 2.2. *Let x be a principal unit of F. Then there exists an integer n such that $\zeta_p^n x$ is congruent to 1 modulo π^2.*

Proof. If x is congruent to 1 modulo π^2, take $n = 0$. Otherwise, write $x = 1 + m\pi + O(\pi^2)$ for some integer m; note that this is possible since the residue field of F is $\mathbf{F}_p$, and so every element is represented by an integer. Since $\zeta_p = 1 - \pi$, we have $\zeta_p^n = 1 - n\pi + O(\pi^2)$. Thus, taking $n = -m$, we have

$$\zeta_p^{-m} x = (1 - m\pi + O(\pi^2))(1 + m\pi + O(\pi^2)) = 1 + O(\pi^2),$$

which completes the proof. □

Lemma 2.3. *We have $U_1(F)^p = U_{p+1}(F)$.*

Proof. Let $x \in U_1(F)$. By Lemma 2.2, write $x = \zeta_p^n(1 + y)$ where $v(y) \geq 2$. By the binomial theorem, $x^p = 1 + pyz + y^p$, where z is a $\mathbf{Z}$-linear combination of powers of y. Since $F/\mathbf{Q}_p$ is totally ramified of degree $p - 1$, we have $v(p) = p - 1$, and so $v(py) \geq p + 1$. Of course, $v(y^p) \geq 2p \geq p + 1$ as well. Thus $x^p \in U_{p+1}(F)$.

Conversely, suppose that $x \in U_{p+1}(F)$, and write $x = 1 + y$ with $v(y) \geq p + 1$. Consider the series $\sum_{n \geq 0} \binom{1/p}{n} y^n$. We have

$$\binom{1/p}{n} = \frac{(1/p)(1/p - 1) \cdots (1/p - n + 1)}{n!}.$$

The numerator has n copies of p^{-1} in it, while the denominator has approximately (and at most) $n/(p-1)$ copies of p in it. Since p has valuation $p - 1$, we find

$$v\left(\binom{1/p}{n}\right) \geq -(p-1)\left(n + \frac{n}{p-1}\right) = -pn.$$

Since $v(y^n) \geq (p+1)n$, the terms in the series have valuation tending to infinty, and so the series converges. It converses to an element of $U_1(F)$ that is a pth root of x. ☐

Lemma 2.4. *Let $x \in U_1(F)$ be such that ${}^g x/x^{\chi(g)}$ is a pth power for all $g \in G$. Then we can write $x = \zeta_p^a (1+\pi)^b u$ where $a, b \in \mathbf{Z}$ and $u \in U_1(F)^p$.*

Proof. Since ${}^g x/x^{\chi(g)}$ is a pth power and a principal unit, it is a pth power of a principal unit, i.e., it belongs to $U_1(F)^p$, which is $U_{p+1}(F)$ by Lemma 2.3. Thus ${}^g x$ is congruent to $x^{\chi(g)}$ modulo π^{p+1}. Per Lemma 2.2, let $a \in \mathbf{Z}$ be such that $\zeta_p^{-a} x = 1 + O(\pi^2)$, and write $\zeta_p^{-a} = 1 + c\pi^n + O(\pi^{n+1})$ for integers c and n with $n \geq 2$. Then (using Lemma 2.1),

$${}^g x = \zeta_p^{a\chi(g)}(1 + c\chi(g)^n \pi^n + O(\pi^{n+1})), \qquad x^{\chi(g)} = \zeta_p^{a\chi(g)}(1 + c\chi(g)\pi^n + O(\pi^{n+1})).$$

Since these are congruent modulo π^{p+1} for all g, either $n \geq p+1$ or else $n \equiv 1 \pmod{p-1}$, which implies $n = p$ (since $n \geq 2$); thus $n \geq p$ in all cases. We thus see that $\zeta_p^{-a} x$ is 1 modulo π^p, and can thus be written at $1 + b\pi^p + O(\pi^{p+1})$ for some integer b (in fact, $b = c$ if $n = p$, and $b = 0$ if $n > p$). Note that $1 + b\pi^p$ is congruent to $(1 + \pi^p)^b$ modulo π^{p+1}. Thus, working modulo π^{p+1}, or, equivalently, $U_1(F)^p$, we have $x = \zeta_p^a (1+\pi)^n$, which completes the proof. ☐

Proof of Proposition 1.2. Suppose that $E/\mathbf{Q}_p$ is Galois with group $(\mathbf{Z}/p\mathbf{Z})^3$. We apply Kummer theory to the extension $E(\zeta_p)/F$. This tells us that $E(\zeta_p) = F(B^{1/p})$ for some canonical subgroup $B \subset F^\times/(F^\times)^p$ isomorphic to $(\mathbf{Z}/p\mathbf{Z})^3$. Since $F(x^{1/p})$ is abelian over $\mathbf{Q}_p$ for all $x \in B$ (being a subfield of $E(\zeta_p)$), Proposition 3.5 of the previous note tells us that $x^g/x^{\chi(g)} \in F^p$ for all $g \in G$.

Let $x \in F^\times$ be a lift of some element $\overline{x}$ of B, and write $x = u\pi^m$ where u is a unit of F. The element ${}^g x/x^{\chi(g)}$ has valuation $v(x)(1 - \chi(g))$ modulo p; but it is also a pth power, and thus its valuation is 0 mod p. We conclude that $v(x)$ is a multiple of p, since we can choose g so that $\chi(g) \neq 1$ modulo p. Since we can modify x by pth powers, we may as well assume that it has valuation 0, i.e., that it is a unit. In fact, since every element of the residue field is a pth power, we can assume that it is a principal unit. But now, by Lemma 2.4, we see that x can be written in the form $\zeta_p^a (1 + \pi^p)^b$ modulo pth powers.

The above analysis shows that B belongs to the subgroup of $F^\times/(F^\times)^p$ generated by ζ_p and $1 + \pi^p$. Thus, as an $\mathbf{F}_p$-vector space, $\dim(B) \leq 2$. This is a contradiction. ☐

3. The global Kronecker–Weber theorem

Finally, we can prove the global theorem:

Theorem 3.1. *Any finite abelian extension of $\mathbf{Q}$ is contained in $\mathbf{Q}(\zeta_n)$ for some n.*

Let $K/\mathbf{Q}$ be given finite abelian extension. Let $p_1, \ldots, p_r$ be the finitely many rational primes at which K ramifies, and for each i choose a prime $\mathfrak{p}_i$ of K over p_i. By local Kronecker–Weber, each $K_{\mathfrak{p}_i}$ is contained in some $\mathbf{Q}_{p_i}(\zeta_{n_i})$. Let p^{e_i} be the largest power of p dividing n_i, and put $m = p_1^{e_1} \cdots p_r^{e_r}$. We will show that K is contained in $\mathbf{Q}(\zeta_m)$.

Let $L = K(\zeta_m)$ and let $I_p \subset \mathrm{Gal}(L/\mathbf{Q})$ be the inertia group at p. Let $\mathfrak{q}_i$ be a prime of L over $\mathfrak{p}_i$. Then $\mathbf{Q}_{p_i}(\zeta_m) \subset L_{\mathfrak{q}_i} \subset \mathbf{Q}_{p_i}(\zeta_{\mathrm{lcm}(m,n_i)})$; since p^{n_i} is the largest power of p dividing m and n_i, we see that $I_{p_i} \cong (\mathbf{Z}/p^{e_i}\mathbf{Z})^\times$. Let $I \subset \mathrm{Gal}(L/\mathbf{Q})$ be the subgroup generated by the I_{p_i}'s. Then

$$|I| \le \prod_{i=1}^{r} |I_{p_i}| = \prod_{i=1}^{r} \varphi(p_i^{e_i}) = \varphi(m) = [\mathbf{Q}(\zeta_m) : \mathbf{Q}].$$

The fixed field L^I is everywhere unramified; thus, by Minkowski's theorem, it is $\mathbf{Q}$. Hence $I = \mathrm{Gal}(L/\mathbf{Q})$, and so $[L : \mathbf{Q}] = |I| \le [\mathbf{Q}(\zeta_m) : \mathbf{Q}]$. Since $\mathbf{Q}(\zeta_m) \subset L$, we must have $L = \mathbf{Q}(\zeta_m)$, and so $K \subset \mathbf{Q}(\zeta_m)$.

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