The Kronecker-Weber Theorem

November 30, 2007

Let us begin with the local statement.

Theorem 1 *Let $K/\mathbf{Q}_p$ be an abelian extension. Then K is contained in a cyclotomic extension of $\mathbf{Q}_p$.*

Proof: We give the proof only for odd primes.

Lemma 2 *Suppose $K/\mathbf{Q}_p$ is totally ramified of degree p, with p odd. Then $G_2 = \{1\}$, and $\nu_K(\mathcal{D}_{K/\mathbf{Q}_p}) = 2(p-1)$.*

Proof: Suppose i is the smallest integer such that $G_i = \{1\}$. Then $\nu_K(\mathcal{D}_{K/\mathbf{Q}_p}) = (p-1)i$, and since

$$\nu_K(\mathcal{D}_{K/\mathbf{Q}_p}) \leq e - 1 + \nu_K(e) = e - 1 + \nu_K(p) = 2e - 1,$$

we conclude that

$$\begin{aligned} (p-1)i &\leq 2p - 1 = 2p - 2 + 1 \\ i &\leq 2 + \frac{1}{p-1} \end{aligned}$$

Since p is odd and i is at least 2, we conclude that $i = 2$ and $\nu_K(\mathcal{D}_{K/\mathbf{Q}_p}) = 2(p-1)$. □

Lemma 3 *Suppose $K/\mathbf{Q}_p$ is totally ramified of degree p^2, with p odd. Then G_1/G_2 and G_{p+1}/G_{p+2} are cyclic of order p, and $\nu_K(\mathcal{D}_{K/\mathbf{Q}_p}) = 3p^2 - p - 2$.*

Proof: Recall that for any $i > 0$ we have an injective homomorphism

$$\theta_i\colon G_i/G_{i+1} \to \mathsf{m}^{\mathsf{i}}/\mathsf{m}^{\mathsf{i+1}},$$

where i is the maximal ideal of the ring of integeres of K. Since the residue field is the prime field, we see that each quotient is cyclic. Suppose that j is the smallest integer such that $G_j = \{1\}$ and that i is the smallest integer such that $G \neq G_i$. Recall that i and j are congruent modulo p, so that we can write $j = i + pk$, where i is at least 2 and k is at least 1. The formula for the value of the different now gives:

$$\begin{aligned} \nu_E(\mathcal{D}_{K/\mathbf{Q}_p}) &= (p^2 - p)i + (p-1)(i + pk) \\ &= p^2(k+i) - pk - i. \end{aligned}$$

On the other hand, the upper bound for the different is $e - 1 + \nu_K E(p^2) = 3p^2 - 1$, so we get

$$\begin{aligned} p^2(k+i) - pk - i &\leq 3p^2 - 1 \\ (p^2 - p)(k+i) + pi - i &\leq 3p^2 - 3p + 3p - 3 + 2 \\ (p^2 - p)(k+i) &\leq 3p^2 - 3p + (p-1)(3-i) + 2 \\ &\leq 3p^2 - 3p + (p-1) + 2 \\ (k+i) &\leq 3 + \frac{1}{p} + \frac{2}{p^2 - p} \end{aligned}$$

Since p is at least three, we see that $k + i$ is bounded by $3\ \frac{2}{3}$, and so must be 3. Thus, $i = 2$, $k = 1$, and $\nu_E(\mathcal{D}_{K/\mathbf{Q}_p}) = 3p^2 - p - 2$. □

Lemma 4 *Any totally ramified Galois extension K of degree p^2 over $\mathbf{Q}_p$ is cyclic (p is odd).*

Proof: It suffices to show that the Galois group of $K/\mathbf{Q}_p$ has a unique subroup of order p. Let H be such a subgroup and let K' be its fixed field; then $\nu_K(\mathcal{D}_{K/\mathbf{Q}_p}) = p\nu_{K'}(\mathcal{D}_{K'/\mathbf{Q}_p}) = 2p^2 - 2p$. By the multiplicativity of the different in extensions and the previous lemma, we deduce that

$$\begin{aligned} \nu_K(\mathcal{D}_{K/K'}) &= \nu_K(\mathcal{D}_{K/\mathbf{Q}_p} - \nu_K(\mathcal{D}_{K'/\mathbf{Q}_p}) \\ &= (3p^2 - p - 2) - (2p^2 - 2p) \\ &= p^2 + p - 2 \\ &= (p-1)(p+2). \end{aligned}$$

On th other hand, if j is the smallest integer such that $H_j = \{1\}$, the equation $\nu_K(\mathcal{D}_{K/K'}) = (p-1)j$ shows that $j = p+2$. We conclude that H is contained in the subgroup G_{p+1}, and hence coincides with it. □

Having proved some limits on the type of extensions which can occur, our next task if to construct some interesting cyclotomic extensions.

Lemma 5 *For any positive integer a, there is an integer m such that $E^u_a := \mathbf{Q}_p(\zeta_m)$ is unramified and cyclic of degree p^a.*

Proof: We know that the finite field $\mathbf{F}_p$ admits an extension of degree p^a, and that this extension is automatically separable, cyclic, and cyclotomic, obtained by adjoining an mth root of unity for some m relatively prime to p. Then $\mathbf{Q}_p(\zeta_m)$ is unramified and has the same properties. □

Lemma 6 *For any positive integer a, there is a (unique) subfield E^w_a of $\mathbf{Q}_p(\zeta_{p^{a+1}})$ which is totally ramified, cyclic, and of degree p^a over $\mathbf{Q}_p$.*

Proof: We know that $\mathbf{Q}(\zeta_{p^{a+1}})$ is totally ramified over $\mathbf{Q}_p$, and Galois with group $(\mathbf{Z}/p^{a+1}\mathbf{Z})^*$. Furthermore, the canonical exact sequence of abelian groups

$$1 \to U \to (\mathbf{Z}/p^{a+1}\mathbf{Z})^* \to \mathbf{F}_p^* \to 1$$

splits uniquely, since the order $p-1$ of the quotient is relatively prime to the order p^a of the kernel. Then the fixed field E^w_a of the image of the splitting $\mathbf{F}_p^* \subseteq G(\mathbf{Q}(\zeta_{p^{a+1}}))$ is totally ramified and Galois, with group H. Since p is odd, the group H is cyclic. □

Lemma 7 *The compositum $E_a := E^w_a E^u_a$ is Galois over $\mathbf{Q}_p$, with group $\mathbf{Z}/p^a\mathbf{Z} \times \mathbf{Z}/p^a\mathbf{Z}$.*

Proof: Observe that $E^w_a \cap E^u_a$ is totally ramified and unramified over $\mathbf{Q}_p$, hence trivial. It follows that the Galois group of the compositum is the product of the two Galois groups. □

Now we can prove Theorem 1 for cyclic p-extensions.

Lemma 8 *Let K be a Galois extension of $\mathbf{Q}_p$ which is cyclic of order p^a. Then K is contained in the field E_a.*

Proof: Let $E := E_a$. We have a diagram of abelian extensions:

$$\begin{tikzcd}
 & KE & \\
K \arrow[ur] & & E \arrow[ul] \\
 & K \cap E \arrow[ul] \arrow[ur] & \\
 & \mathbf{Q}_p \arrow[u] &
\end{tikzcd}$$

Thus

$$Gal(KE/\mathbf{Q}_p) \cong Gal(K/\mathbf{Q}_p) \times_{\mathrm{Gal}(K\cap E/\mathbf{Q}_p)} Gal(E/\mathbf{Q}_p).$$

The $K \cap E/\mathbf{Q}_p$ is cyclic of degree p^b, with $b \leq a$, and the natural surjection $Gal(K/\mathbf{Q}_p) \to Gal(K \cap E/\mathbf{Q}_p)$ can be identified with the projection $\mathbf{Z}/p^a\mathbf{Z} \to \mathbf{Z}/p^b\mathbf{Z}$. Let

$$M := Gal(K/\mathbf{Q}_p) \times Gal(E/\mathbf{Q}_p) \cong (\mathbf{Z}/p^a\mathbf{Z})^3.$$

Then we have an exact sequence:

$$0 \to Gal(KE/\mathbf{Q}_p) \to M \to \mathbf{Z}/p^b\mathbf{Z} \to 0$$

where the map on the right is given by the difference of the two maps $Gal(K/\mathbf{Q}_p) \to Gal(K \cap E/\mathbf{Q}_p)$, $Gal(E/\mathbf{Q}_p) \to Gal(K \cap E/\mathbf{Q}_p)$. Let $\overline{M} := M \otimes \mathbf{Z}/p^b\mathbf{Z}$. Then the map $\pi\colon M \to \mathbf{Z}/p^b\mathbf{Z}$ factors through a surjection of free $\mathbf{Z}/p^b\mathbf{Z}$-modules: $\overline{\pi}\colon \overline{M} \to \mathbf{Z}/p^b\mathbf{Z}$. This surjection admits a splitting, so that

$\overline{M}$ admits a basis $\overline{e}_1, \overline{e}_2, \overline{e}_3$ such that $\overline{\pi}(\overline{e}_1) = \overline{\pi}(\overline{e}_2) = 0$ and $\overline{\pi}(\overline{e}_3) = 1$. Then if $e_i \in M$ lifts $\overline{e}_i$, (e_1, e_2, e_3) is a basis for M and $\pi(e_1) = \pi(e_2) = 0$, $\pi(e_e) = 1$. This implies that the kernel of π is isomorphic to $\mathbf{Z}/p^a\mathbf{Z} \times \mathbf{Z}/p^a\mathbf{Z} \times \mathbf{Z}/p^{a-b}\mathbf{Z}$. If K is not contained in E, then $a < b$ and the Galois group $G(EK/\mathbf{Q}_p)$ admits a quotient isomorphic to $G' := (\mathbf{Z}/p\mathbf{Z})^3$. This tells us that $\mathbf{Q}_p$ admits a field extension K' which is Galois with this G' as Galois group. The maximal unramifed extension K'_u of K is cyclic over $\mathbf{Q}_p$, and corresponds to a quotient G'_u of G', and hence is either trivial or of order p. In any case it is a direct factor of G' (not uniquely). The fixed field K'' of a splitting of $G'_u \to G'$ is totally ramified over $\mathbf{Q}_p$ and Galois with group $(\mathbf{Z}/p\mathbf{Z})^c$, with $c = 2$ or 3. This would contradict the previous lemma. □

Let us next discuss the tame case. Here we do not need to assume that p is odd.

Lemma 9 *Let $K/\mathbf{Q}_p$ be a tamely ramified and abelian extension. Then its ramification degree e divides $p-1$, and K is contained in $K^u(\zeta_p)$, where K^u is the unramified part of K.*

Proof: We have an exact sequence

$$1 \to G_0 \to G \to G/G_0 \to 1$$

where G/G_0 is (identified with) the Galois group of the residual extension of $K/\mathbf{Q}_p$. We also have the tame character $\tau \colon G_0 \to k_B^*$. Recall that if $h \in G_0$ and $g \in G$, $\tau(ghg^{-1}) = g(\tau(h))$. Since G is abelian, it follows that $\tau(h) = g(\tau(h))$. Since G maps surjectively to the Galois group of the residual extension, it follows that $\tau(h) \in \mathbf{F}_p^*$. Since the ramification is tame, τ is injective, and the order e of G_0 divides the order of $\mathbf{F}_p^*$, viz. $p-1$.

Now consider the following diagram of field extensions.

$$\begin{tikzcd}
 & K(\zeta_p) & & \\
K \arrow[ur] & & K^u(\zeta_p) \arrow[ul] & \\
 & K^u \arrow[ul] \arrow[ur] & & \mathbf{Q}(\zeta_p) \arrow[ul] \\
 & & \mathbf{Q}_p \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

In this diagram, $K^u/\mathbf{Q}_p$ is unramified and $\mathbf{Q}(\zeta_p)/\mathbf{Q}_p$ is totally ramified, so $K^u \cap \mathbf{Q}(\zeta_p) = \mathbf{Q}_p$ and $K^u(\zeta_p)/K^u$ is Galois with group $\mathbf{F}_p^*$. The extension $K(\zeta_p)/K^u$ is totally and tamely ramified, and hence its Galois group is cyclic, say of order n. Since it is cyclic, it has a unique subgroup of index d for each divisor d of n. Hence for each such d there is a unique extension K_d of K^u contained in $K(\zeta_p)$; in particular $K^u = K_e$. Similarly, $K^u(\zeta_p)/K^u$ is cyclic of degree $p-1$, so for each divisor d of $p-1$ there is a unique extension K'_d of K^u contained in $K^u(\zeta_p)$. Since e divides $p-1$, $K = K_e = K'_e$ is contained in $K^u(\zeta_p)$. □

Remark 10 The last part of the argument above applies more generally. It is worth stating the conclusion, which is sometimes called Abhyankar's lemma. Let K/K_0 be a Galois extension of local fields which is tamely ramified, with ramification degree e. Let E/K_0 be Galois, totally and tamely ramified, with degree divisible by e. Then K is contained in K^uE. This applies to numberfields as well.

Proof of Theorem 1 Let $K/\mathbf{Q}_p$ be an abelian extension. The Galois group $G(K/\mathbf{Q}_p)$ is the product of cyclic groups of prime power order, and so K

is the compositum of field extensions each of which is Galois and abelian of prime power order. It suffices to prove that each of these is contained in a cyclotomic extension. Thus we may assume that K is cyclic of order ℓ^a for some prime ℓ. Lemma 8 then asserts that K is contained in a cyclotomic extension if $\ell = p$. If not, $K/\mathbf{Q}_p$ is tame, and hence contained in $K^u(\zeta_p)$. But we have already noted that unramified extensions of $\mathbf{Q}_p$ are contained in cyclotomic fields. This completes the proof. $\square$

Now let us discuss the global case. A crucial ingredient is the fact that $\mathbf{Q}$ has no nontrivial unramified extensions. This can be expressed group-theoretically as follows.

Theorem 11 *Let $K/\mathbf{Q}$ be a finite Galois extension of $\mathbf{Q}$. Then the Galois group $G(K/\mathbf{Q})$ is generated by the set of elements which belong to some inertia group at some prime of K.*

Proof: Indeed, if H is the subgroup of $G(K/\mathbf{Q})$ generated by all such elements, then the fixed field K^H is unramified over $\mathbf{Q}$, hence is equal to $\mathbf{Q}$. $\square$

For example, if we write a positive integer m as a product of prime powers: $m = \prod p^{r_p}$, we obtain an isomorphism of rings $\mathbf{Z}/m\mathbf{Z} \cong \prod_p \mathbf{Z}/p^{r_p}\mathbf{Z}$ and hence an isomorphism of groups $(\mathbf{Z}/m\mathbf{Z})^* \cong \prod_p (\mathbf{Z}/p^{r_p}\mathbf{Z})^*$. This isomorphism corresponds to compositum of fields $\mathbf{Q}(\zeta_m) \cong \otimes \mathbf{Q}(\zeta_{p^{r_p}})$. In fact, under these isomorphisms, the factor $(\mathbf{Z}/p^{r_p})^*$ corresponds exactly to the inertia subgroup $I_p \subseteq G(\mathbf{Q}(\zeta_m)/\mathbf{Q})$ at (any prime lying over) p. Note that in this case, the inertial subgroups are actually disjoint, and the map $\prod I_p \to G(\mathbf{Q}(\zeta_m)/\mathbf{Q})$ is an isomorphism.

Theorem 12 *Let $K/\mathbf{Q}$ be an abelian extension. Then K is contained in a cyclotomic field.*

Proof: The Galois group G of $K/\mathbf{Q}$ is abelian and finite, hence the product of finite cyclic groups of prime power order. Then K is the compositum of cyclic extensions of prime power order, and it suffices to treat each of these separately. So suppose that $K/\mathbf{Q}$ is cyclic of order a power of ℓ. Let p be a prime at which K ramifies. The local version of the theorem tells us that there is an m such that $K \subseteq \mathbf{Q}_p(\zeta_m)$. This certainly implies that $K(\zeta_m)/\mathbf{Q}(\zeta_m)$ is unramifed over the prime lying over p. Since only finitely many primes of

K are ramified, we can find a single m so that $K(\zeta_m)/\mathbf{Q}(\zeta_m)$ is everywhere unramified. This means that the inertia groups I_p of the extension $K(\zeta_m)/\mathbf{Q}$ have trivial intersection with the Galois group of the extension $K(\zeta_m)/\mathbf{Q}(\zeta_m)$, and hence map injectively to the Galois group of the extension $\mathbf{Q}(\zeta_m)/\mathbf{Q}$. Consider the commutative diagram:

$$\begin{tikzcd}
\prod_p I_p(K(\zeta_m)/\mathbf{Q}) \arrow[r] \arrow[d] & \prod I_p(\mathbf{Q}(\zeta_m)/\mathbf{Q}) \arrow[d] \\
G(K(\zeta_m)/\mathbf{Q}) \arrow[r] & G(\mathbf{Q}(\zeta_m)/\mathbf{Q})
\end{tikzcd}$$

As we have seen, the arrow on the top is injective, and the arrow on the right is an isomorphism. Theorem 11 (and the fact the Galois group is abelian) implies that the map on the left is surjective. But then it must be an isomorphism, and so must be the map on the bottom. This implies that $K \subseteq \mathbf{Q}(\zeta_m)$. □

Stritly speaking, our proof has a gap, since we did not prove the local theorem when $p = 2$. The following finesse of this tricky was explained to me by H. Lenstra.

Suppose again that K is cyclic of order a power of a prime ℓ. If ℓ is odd, K is at most tamely ramified at 2, and since the extension is abelian, the image of the tame character lies in $\mathbf{F}_2^* = \{1\}$. Hence K is unramified at 2.

show that K is in fact unramified at 2. Thus the proof goes through in this case. Now suppose that $\ell = 2$. Suppose that K ramifies at some odd prime p. Then K is again at most tamely ramified, and the argument in Lemma 9 shows that $K \subseteq K^u(\zeta_p)$, where K^u is the subfield of K unramified over p. It suffces to prove that K^u is contained in a cyclotomic field. Repeating this argument at all the odd primes, we are reduced to the case in which K is unramified everywhere except possibly at 2.

Lemma 13 *2cyc.l Suppose that $K/\mathbf{Q}$ is an abelian extension of degree a power of 2, is real, and is unramified outside of 2. Then $K/\mathbf{Q}$ is cyclic.*

Proof: It suffices to show that K has a unique subfield which is quadratic over $\mathbf{Q}$. But such a subfield must be $\mathbf{Q}(\sqrt{m})$ for some square free m, and because it is unramified away from 2, $m = \pm 2$ or $m = -1$. Since K is real, necessarily $m = 2$. □

Lemma 14 *Suppose that $K/\mathbf{Q}$ is an abelian extension of degree a power of 2, unramified outside of 2. Then K is contained in a cyclotomic extension.*

Proof: Consider the field $K(i)$. This is still unramified outside of 2 and abelian of degree a power of 2. Let K' be the invariants under complex conjugation; then K' is real, of degree a power of 2, and unramified outside of 2, hence cyclic, by the previous lemma. Suppose its degree is 2^m. Let F be the real part of $\mathbf{Q}(\zeta_{2^{m+2}})$. This is also abelian of degree 2^m, real, and unramified outside of 2. Since the lemma applies also to show that the compositum of K' and F is cyclic, we can conclude that $K' \subseteq F$. Hence $K \subseteq K'(i) \subset F(i)$, which is still a cyclotomic field.