A SIMPLE PROOF OF KRONECKER-WEBER THEOREM

NIZAMEDDIN H. ORDULU

1. Introduction

The main theorem that we are going to prove in this paper is the following:

Theorem 1.1. ***Kronecker-Weber Theorem*** *Let $K/\mathbb{Q}$ be an abelian Galois extension. There exists an n such that $K \subset \mathbb{Q}(\zeta_n)$.*

Theorem 1.1 is equivalent to the following equality

$$\mathbb{Q}^{ab} = \prod_{n=1}^{\infty} \mathbb{Q}(\zeta_n)$$

where $\mathbb{Q}^{ab}$ denotes the maximal abelian extension (the field that contains all the abelian extensions of $\mathbb{Q}$.) So basically theorem 1.1 says that the maximal abelian extension of $\mathbb{Q}$ is the compositum of the cyclotomic extensions of $\mathbb{Q}$. Therefore it gives a classification of abelian extensions of $\mathbb{Q}$. In general the abelian extensions of a number field can be classified by means of class field theory. In this paper we present a proof of theorem 1.1 without appealing to class field theory. A remarkable aspect of this work is that it makes use of the local-global principle. In other words we obtain theorem 1.1 from the following theorem:

Theorem 1.2. ***Local Kronecker-Weber Theorem*** *Let $K/\mathbb{Q}_p$ be an abelian Galois extension. There exists an n such that $K \subset \mathbb{Q}_p(\zeta_n)$*

2. Notations and Fundamental Theorems

Throughout this paper p will denote a rational prime, $\mathbb{Q}_p$ the completion of rational numbers with respect to p-adic valuation, $K_\mathfrak{p}$ the completion of a number field K with respect to one of its prime ideals $\mathfrak{p}$ and ζ_n a primitive nth root of unity.

We start with basic facts and well known theorems from algebraic number theory. We give some of the proofs.

Definition 2.1. Let K and L be finite extensions of $\mathbb{Q}$ (or $\mathbb{Q}_p$.) The smallest field containing K and L is called the compositum of K and L and denoted as KL.

Theorem 2.2. *Let K and L be finite Galois extensions of $\mathbb{Q}$.$Gal(KL/\mathbb{Q})$ is isomorphic to the subgroup $\{(\phi,\psi)|\phi|_{K\cap L}=\psi|_{K\cap L}\}$ of $Gal(K/\mathbb{Q})\times Gal(L/\mathbb{Q})$. Similar argument holds for $\mathbb{Q}_p$.*

Proof Let $G=Gal(KL/\mathbb{Q})$ and $H=\{(\phi,\psi)|\phi|_{K\cap L}=\psi|_{K\cap L}\}$. Clearly the map $\Lambda: G\to H$, $\sigma\to(\sigma|_K,\sigma|_L)$ defines an injective homomorphism between G and H. We show that this homomorphism is indeed an isomorphism by showing that $|G|=|H|$. Let $M=K\cap L$ and let $[M:\mathbb{Q}]=m$, $[KL:K]=k$ and $[KL:L]=l$. Viewing $A=Gal(KL/K)$ and $B=Gal(KL/L)$ as subgroups of $Gal(KL/M)$ one can easily show that $A\cap B=\{id|_{KL}\}$ and the fixed field of AB is M. It follows that $[KL:M]=kl$. So $[K:M]=l$ and $[L:M]=k$. Combining with $[M:\mathbb{Q}]=m$ and simple counting shows that $|H|=klm$. But $|G|=[KL:\mathbb{Q}]=[KL:M][M:\mathbb{Q}]=klm$ so we are done.

Theorem 2.3. *Let $L/\mathbb{Q}$ be an abelian Galois extension and let*

$$Gal(L/\mathbb{Q})\cong\prod_{i=1}^{m}G_i.$$

Then

$$L=\prod_{i=1}^{m}L^{G_i}.$$

Similar argument holds for $\mathbb{Q}_p$.

Proof It suffices to prove for $m=2$. Let $L/\mathbb{Q}=G_1\times G_2$. Then $L^{G_1}\cap L^{G_2}=\mathbb{Q}$. By theorem 2.2 $Gal(L^{G_1}L^{G_2})=G_1\times G_2$. From this the theorem follows.

Theorem 2.4. *Let L/K be a finite Galois extension. (L and K can be number fields or local fields) Let $\mathfrak{p}$ be a prime ideal of K. Then $\mathfrak{p}$ factorizes in L as*

$$\mathfrak{p}=\mathfrak{b}_1^e\mathfrak{b}_2^e...\mathfrak{b}_g^e$$

The number e is called the ramification index. The degree of the extension of the residue fields $\mathcal{O}_L$ mod $\mathfrak{b}_1$ / $\mathcal{O}_K$ mod $\mathfrak{p}$ is denoted by f. If the degree of L/K is n then

$$n=efg.$$

(If K and L are local $g=1$) $\mathfrak{p}$ is said to be totally ramified in L if $e=n$ and unramified if $e=1$. (If K and L are local fields then we say L/K is unramified or totally ramified if $e=1$ or $e=n$ respectively. A number field extension is said to be unramified if all prime ideals are unramified.)

Proof See any introductory Algebraic Number theory book or [S2] p. 101.

Definition 2.5. Let L/K be a Galois extension, $\mathfrak{p}$ a prime of K, $\mathfrak{b}$ a prime lying above $\mathfrak{p}$. The decomposition group $D_{\mathfrak{b}}$ of $\mathfrak{b}$ is given by $D_{\mathfrak{b}} = \{\sigma \in Gal(L/K) | \sigma(\mathfrak{b}) = \mathfrak{b}\}$.(If L and K are local then $D_{\mathfrak{b}}$ is the whole Galois group.) The ramification group $I_{\mathfrak{b}}$ is defined as follows:

$$I_{\mathfrak{b}} = \{\sigma \in D_{\mathfrak{b}} \mid \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{b}} \text{ for all } \alpha \in \mathcal{O}_L\}$$

$\mathfrak{p}$ is unramified in $L^{I_{\mathfrak{b}}}$ and $L^{I_{\mathfrak{b}}}$ is the largest such field among the intermediate fields of L/K.

Theorem 2.6. *Let L/K be a Galois extension of number fields. If $\mathfrak{p}$ is a prime of K and $L_{\mathfrak{b}}/K_{\mathfrak{p}}$ is the localization of L/K with respect to $\mathfrak{p}$, then $Gal(L_{\mathfrak{b}}/K_{\mathfrak{p}}) \cong D_{\mathfrak{b}}$ and the inertia groups of $\mathfrak{b}$ in both extensions are isomorphic.*

Proof There exist injections $i_1 : K \hookrightarrow K_{\mathfrak{p}}$ and $i_2 : L \hookrightarrow L_{\mathfrak{b}}$. Certainly any element of $Gal(L_{\mathfrak{b}}/K_{\mathfrak{p}})$ induces an automorphism of $i_2(L)/i_1(K)$. Furthermore since $i_1(K)$ is dense in $K_{\mathfrak{p}}$ and $i_2(L)$ is dense in $L_{\mathfrak{b}}$ the restriction $\Sigma : Gal(L_{\mathfrak{b}}/K_{\mathfrak{p}}) \to Gal(i_2(L)/i_1(K))$ is injective. Furthermore since any automorphism of $L_{\mathfrak{b}}/K_{\mathfrak{p}}$ preserves $\mathfrak{b}$-adic absolute value the image of Σ must be in $D_{\mathfrak{b}}$. Conversely if $\sigma \in D_{\mathfrak{b}}$ then one can extend σ uniquely to an automorphism of $L_{\mathfrak{b}}/K_{\mathfrak{p}}$.

Theorem 2.7. *Let K and L be finite Galois extensions of $\mathbb{Q}_p$ and suppose that L/K is Galois. Then there is a surjective homomorphism between the inertia groups I_L and I_K of L and K.*

Proof Let $M/\mathbb{Q}_p$ be the maximal unramified subextension of $L/\mathbb{Q}_p$. Then the maximal unramified subextension of $K/\mathbb{Q}_p$ is $M \cap K/\mathbb{Q}_p$. Since the restriction homomorphism $Gal(M/\mathbb{Q}_p) \to Gal(M \cap K/\mathbb{Q}_p)$ is surjective, the theorem follows.

Theorem 2.8. *The inertia group of the extension $\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p$ is isomorphic to $(\mathbb{Z}/p^e\mathbb{Z})^*$ where p^e is the exact power of p dividing n.*

Proof By theorem 2.6 the inertia group of is isomorphic to the inertia group of $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ corresponding to p. Now let $n = p^e m$. Then

$$Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/p^e\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*$$

It is not hard to check that the fixed field of the subgroup isomorphic to $(\mathbb{Z}/m\mathbb{Z})^*$ is $\mathbb{Q}(\zeta_{p^e})$. Furthermore $\mathbb{Q}(\zeta_{p^e})/\mathbb{Q}$ is totally ramified with inertia group $(\mathbb{Z}/p^e\mathbb{Z})^*$. Since $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ is unramified at p no further ramification occurs.

Theorem 2.9. *(*Hensel's Lemma*) Let L be a local field, $\mathfrak{b}$ be its maximal ideal, l be the residue field, $f \in \mathcal{O}_L[x]$ be a monic polynomial, $\tilde{f}$ be its restriction to l, and $\alpha \in l$ be such that $\tilde{f}(\alpha) = 0$ and $\tilde{f}'(\alpha) \neq 0$. Then there exists a root β of f in $\mathcal{O}_L$ such that $\beta = \alpha$ (mod $\mathfrak{b}$).*

Proof Let $\beta_0 \in \mathcal{O}_L$ be such that $\beta_0 = \alpha\ (mod\ \mathfrak{b})$. Define $\beta_m = \beta_{m-1} - \frac{f(\beta_{m-1})}{f'(\beta_{m-1})}$. It is an easy exercise to show that the sequence $\{\beta_m\}$ converges and the limit is a root of f. For a proof see [F-V] p. 36.

Theorem 2.10. *If $K/\mathbb{Q}$ is unramified then $K = \mathbb{Q}$*

Proof By a theorem of Minkowski

$$\sqrt{|d_K|} \geq (\frac{\pi}{4})^s \frac{n^n}{n!}$$

where s is half the number of complex embeddings of K and $n = [K : \mathbb{Q}]$. Using this one can show that if $n > 1$ then $|d_K| > 1$ therefore there exists primes that are ramified. So if all primes are unramified, $n = 1$.

Theorem 2.11. *Let $K/\mathbb{Q}$ be a Galois extension. The Galois group is generated by the inertia groups I_p where p runs through all rational primes.*

Proof Let L be the fixed field of the group generated by I_ps. Then $L/\mathbb{Q}$ is unramified so $L = \mathbb{Q}$. The theorem follows.

3. Deriving the Global Theorem from the Local Case

Theorem 3.1. *The local Kronecker-Weber theorem implies the Global Kronecker-Weber theorem.*

Proof Assume that the local Kronecker-Weber theorem holds for all rational primes. Let $K/\mathbb{Q}$ be an abelian extension and p a rational prime that ramifies in K. Let $\mathfrak{b}$ be a prime lying above p. Consider the localization $K_{\mathfrak{b}}/\mathbb{Q}_p$. The Galois group is the decomposition group of $\mathfrak{b}$ and hence the extension is abelian. By the local Kronecker-Weber theorem $L_{\mathfrak{b}} \subset \mathbb{Q}_p(\zeta_{n_p})$ for some n_p. Let p^{e_p} be the exact power of p dividing n_p. Let

$$n = \prod_{p\ ramifies} p^{e_p}.$$

Claim 3.2. $K \subset \mathbb{Q}(\zeta_n)$

proof of the claim Let $L = K(\zeta_n)$. By the proof of theorem 2.7 we know that $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is unramified outside n so the primes that ramify in L are the same as that of K. Let p be a prime that ramifies in L. Then by theorem 2.6 I_p can be computed locally. The localization of L is L_p=$K_{\mathfrak{b}}(\zeta_n) \subset \mathbb{Q}_p(\zeta_{n_p}, \zeta_n) = \mathbb{Q}_p(\zeta_m)$ where m is the least common multiple of n_p and n. Now by theorem 2.8 the inertia groups of $\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p$ and $\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p$ are both isomorphic to

$(\mathbb{Z}/p^e\mathbb{Z})^*$. Since $\mathbb{Q}_p(\zeta_n) \subset L_p \subset \mathbb{Q}_p(\zeta_m)$ by theorem 2.7, the inertia group of L_p is $(\mathbb{Z}/p^{e_p}\mathbb{Z})^*$. Therefore $|I_p| = \phi(p^{e_p})$. By theorem 2.11,

$$|Gal(L/\mathbb{Q})| \leq \prod_{p\, ramifies} |I_p| \leq \phi(n).$$

It follows that $[L : Q] \leq \phi(n)$, but L already contains $\mathbb{Q}(\zeta_n)$ and $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$. Therefore $L = \mathbb{Q}(\zeta_n)$ from which it follows that $K \subset \mathbb{Q}(\zeta_n)$.

□

Now let $L/\mathbb{Q}_p$ be an abelian Galois extension. For the proof of the local Kronecker-Weber theorem we handle the following three cases seperately:

- The extension is unramified i.e. the maximal ideal of $\mathbb{Q}_p$ remains prime in L.
- The extension is tamely ramified i.e. the ramification degree e is not divisible by p.
- The extension is wildly ramified i.e. the ramification degree e is divisible by p.

4. The Unramified Case

We prove a stronger theorem from which the unramified case of the local Kronecker-Weber theorem follows.

Theorem 4.1. *Let L/K be an unramified, finite Galois extension where K and L are finite extensions of $\mathbb{Q}_p$.$L = K(\zeta_n)$ for some n with $p \nmid n$.*

Proof Assume that L/K is such an extension. Since $e = 1$ the inertia group is trivial and therefore the Galois group of L/K is isomorphic to the Galois group of the extension of the residue fields. Let α generate the extension of residue fields l/k. Since α is an element of a finite field with characteristic p, it is a root of unity with order coprime to p. Let n be the order of α. Now apply theorem 2.9 with $f = x^n - 1$ to obtain a root $\beta \in \mathcal{O}_L$ of $x^n - 1$ such that $\beta = \alpha \ (mod\ \mathfrak{b})$. Then $[K(\beta) : K] \geq [k(\alpha) : k]$ but the latter has degree equal to $[l : k] = [L : K]$ therefore $L = K(\beta) = K(\zeta_n)$.

□

Now taking $K = \mathbb{Q}_p$ gives us the desired result.

5. The Tamely Ramified Case

We begin with two auxilary lemmata.

Lemma 5.1. *Let K and L be finite extensions of $\mathbb{Q}_p$ and $\wp_K$ the maximal ideal of $\mathcal{O}_K$. Suppose L/K is totally ramified of degree e with $p \nmid e$. Then there exists $\pi \in \wp_K \backslash \wp_K^2$ and a root α of $x^e - \pi = 0$ such that $L = K(\alpha)$.*

proof Let $|.|$ denote the absolute value on $\mathbb{C}_p$. Let $\pi_0 \in \wp_K \backslash \wp_K^2$ and let $\beta \in L$ be a uniformizing parameter so that $|\beta^e| = |\pi_0|$. Then $\beta^e = \pi_0 u$ for some $u \in U_L$ (= the units of $\mathcal{O}_L$) Now since $f = 1$ the extension of the residue fields is trivial, hence there exists $u_0 \in U_K$ such that $u = u_0$ $(mod\ \wp_L)$. Therefore $u = u_0 + x$ with $x \in \wp_L$. Let $\pi = \pi_0 u_0$. Then $\beta^e = \pi_0(u_0 + x) = \pi + \pi_0 x$ so $|\beta^e - \pi| < |\pi_0| = |\pi|$. Let $\alpha_1, \alpha_2, ..., \alpha_e$ be the roots of $f(X) = X^e - \pi$. We claim that $L = K(\alpha_i)$ for some i.

Since $|\alpha_i|^e = |\pi|$, $|\alpha_i| = |\alpha_j|$ for all i, j. We have

$$|\alpha_i - \alpha_j| \leq Max\{|\alpha_i|, |\alpha_j|\} = |\alpha_1|.$$

But

$$\prod_{i \neq 1} |\alpha_i - \alpha_1| = |f'(\alpha_1)| = |e\alpha_1^{e-1}| = |\alpha_1|^{e-1}.$$

So $|\alpha_i - \alpha_1| = |\alpha_1|, \forall i \neq 1$. Since

$$\prod_i |\beta - \alpha_i| = |f(\beta)| < |\pi| = \prod_i |\alpha_i|,$$

we must have $|\beta - \alpha_i| < |\alpha_1|$ for some i. Without loss of generality assume that $i = 1$. Now let M be the Galois closure of the extension $K(\alpha_1, \beta)/K(\beta)$. Let $\sigma \in Gal(M/K(\beta))$. We have

$$|\beta - \sigma(\alpha_1)| = |\sigma(\beta - \alpha_1)| = |\beta - \alpha_1| < |\alpha_1| = |\alpha_i - \alpha_1|$$

for $i \neq 1$. But

$$|\alpha_1 - \sigma(\alpha_1)| \leq Max\{|\alpha_1 - \beta|, |\beta - \sigma(\alpha_1)|\} < |\alpha_i - \alpha_1|.$$

It follows that $\sigma(\alpha_1) \neq \alpha_i$ for $i \neq 1$. So $\sigma(\alpha_1) = \alpha_1$. Since σ was arbitrary we have $\alpha_1 \in K(\beta)$ thus $K(\alpha_1) \subset K(\beta) \subset L$. But $f(X)$ is irreducible over K by Eisenstein criterion so $[K(\alpha_1) : K] = e = [L : K]$. Therefore $L = K(\alpha_1)$.

□

Lemma 5.2. $\mathbb{Q}_p((-p)^{1/(p-1)}) = \mathbb{Q}_p(\zeta_p)$

Proof It is easy to prove that the maximal ideal of $\mathbb{Q}_p(\zeta_p)$ is given by $(1-\zeta_p)$. Now consider the polynomial

$$\begin{aligned} g(X) &= \frac{(X+1)^p - 1}{X} \\ &= X^{p-1} + pX^{p-2} + \cdots + p \end{aligned}$$

Then

$$0 = g(\zeta_p - 1) \equiv (\zeta_p - 1)^{p-1} + p \ (mod\ (\zeta_p - 1)^p),$$

so

$$u = \frac{(\zeta_p - 1)^{p-1}}{-p} \equiv 1 \ (mod\ \zeta_p - 1).$$

Let $f(X) = X^{p-1} - u$ then $f(1) \equiv 0\ (mod\ \zeta_p - 1)$ and $(\zeta_p - 1) \nmid f'(1)$. It follows from theorem 2.9 that there exists $u_1 \in \mathbb{Q}_p(\zeta_p)$ such that $u_1^{p-1} = u$. But then we have

$$(-p)^{1/(p-1)} = \frac{\zeta_p - 1}{u_1} \in \mathbb{Q}_p(\zeta_p)$$

On the other hand $X^{p-1} + p$ is irreducible over $\mathbb{Q}_p$ by Eisenstein's criterion so $\mathbb{Q}_p((-p)^{1/(p-1)})$ and $\mathbb{Q}_p(\zeta_p)$ have the same degree over $\mathbb{Q}_p$. Therefore $\mathbb{Q}_p((-p)^{1/(p-1)}) = \mathbb{Q}_p(\zeta_p)$.

□

Now let $L/\mathbb{Q}_p$ be a tamely ramified abelian extension. Let $K/\mathbb{Q}_p$ be the maximal unramified subextension. Then $K \subset \mathbb{Q}_p(\zeta_n)$ for some n by the previous section. L/K is totally ramified with degree $p \nmid e$. By lemma 5.1 $L = K(\pi^{1/e})$ for some π of order 1 in K. Since $K/\mathbb{Q}_p$ is unramified, p is of order 1 in K, so $\pi = -up$ for some unit $u \in K$. Since u is a unit and $p \nmid e$ the discriminant of $f(X) = X^e - u$ is not divisible by p, hence $K(u^{1/e})/K$ is unramified. By theorem 4.1

$$K(u^{1/e}) \subset K(\zeta_M) \subset \mathbb{Q}_p(\zeta_{Mn})$$

for some M. Let T be the compositum of the fields $\mathbb{Q}_p(\zeta_{Mn})$ and L. By theorem 2.2, $T/\mathbb{Q}_p$ is abelian. Since $u^{1/e}, \pi^{1/e} \in T \Rightarrow (-p)^{1/e} \in T$. It follows that $\mathbb{Q}_p((-p)^{1/e})/\mathbb{Q}_p$ is Galois since it is a subextension of the abelian extension $T/\mathbb{Q}_p$. Therefore $\zeta_e \in \mathbb{Q}_p((-p)^{1/e})$. Since $\mathbb{Q}_p((-p)^{1/e})$ is totally ramified, so is the subextension $\mathbb{Q}_p(\zeta_e)/\mathbb{Q}_p$. But $p \nmid e$, so the latter extension is trivial and $\zeta_e \in \mathbb{Q}_p$. Therefore $e \mid (p-1)$. Now by lemma 5.2,

$$\mathbb{Q}_p((-p)^{1/e}) \subset \mathbb{Q}_p(\zeta_p).$$

Therefore

$$L = K(\pi^{1/e}) = K(u^{1/e}, (-p)^{1/e}) \subset \mathbb{Q}_p(\zeta_{Mnp}).$$

This finishes the tamely ramified case.

6. The Wildly Ramified Case

This part of the proof requires knowledge of Kummer theory. We briefly sketch the proof for details see [W] p. 321. Assume that p is an odd prime. First of all note that we may assume by structure theorem for abelian groups and theorem 2.3, that the extension $L/\mathbb{Q}_p$ is cyclic, totally ramified of degree p^m for some m. Now let $K_u/\mathbb{Q}_p$ be an unramified cyclic extension of degree p^m and let $K_r/\mathbb{Q}_p$ be a totally ramified extension of degree p^m. (K_u can be obtained by taking the extension $F/\mathbb{F}_p$ of degree p^m and lifting the minimal polynomial of its primitive element to $\mathbb{Z}_p[X]$. The root of this polynomial will generate an unramified extension of degree p^m. K_r can be taken to be the fixed field of the subgroup isomorphic to $(\mathbb{Z}/p\mathbb{Z})^*$ in the extension $\mathbb{Q}_p(\zeta_{p^m})/\mathbb{Q}_p$.) By the unramified case of the thorem we know that $K_u \subset \mathbb{Q}_p(\zeta_n)$ for some n. Since $K_r \cap K_u = \mathbb{Q}_p$, by theorem 2.2,

$$Gal(K_rK_u/\mathbb{Q}_p) \cong (\mathbb{Z}/p^m\mathbb{Z})^2.$$

If $L \not\subseteq K_rK_u$ then

$$Gal(K(\zeta_n, \zeta_{p^{m+1}})/\mathbb{Q}_p) \cong (\mathbb{Z}/p^m\mathbb{Z})^2 \times \mathbb{Z}/p^{m'}\mathbb{Z}$$

for some $m' > 0$. This group has $(\mathbb{Z}/p\mathbb{Z})^3$ as a quotient, so there is a field N such that

$$Gal(N/\mathbb{Q}_p) \cong (\mathbb{Z}/p\mathbb{Z})^3.$$

Following lemma shows that this is impossible.

Lemma 6.1. *Let p be an odd prime. There is no extension $N/\mathbb{Q}_p$ such that*

$$Gal(N/\mathbb{Q}_p) \cong (\mathbb{Z}/p\mathbb{Z})^3.$$

Before proving the above lemma we quote the following lemma without proof. Interested reader can find the proof in [W] p. 327.

Lemma 6.2. *Let F be a field of characteristic $\neq p$, let $M = F(\zeta_p)$, and let $L = M(a^{1/p})$ for some $a \in M$. Define the character $\omega : Gal(M/F) \to \mathbb{F}_p^\times$ by $\sigma(\zeta_p) = \zeta_p^{\omega(\sigma)}$. Then*

$$L/F \text{ is abelian} \Rightarrow \sigma(a) = a^{\omega(\sigma)} \ (mod\ (M^\times)^p)$$

for all $\sigma \in Gal(M/F)$.

Proof of 6.1 Assume that there exists such an N, then $N(\zeta_p)/\mathbb{Q}_p$ is abelian and $Gal(N(\zeta_p)/\mathbb{Q}_p(\zeta_p)) \cong (\mathbb{Z}/p\mathbb{Z})^3$. This is a Kummer extension so there is a corresponding subgroup $B \subset \mathbb{Q}_p(\zeta_p)^\times/(\mathbb{Q}_p(\zeta_p)^\times)^p$ with $B \cong (\mathbb{Z}/p\mathbb{Z})^3$ and $\mathbb{Q}_p(\zeta_p)(B^{1/p}) = N(\zeta_p)$. Let $a \in B$ and $L = \mathbb{Q}_p(\zeta_p, a^{1/p}) \subset N(\zeta_p)$. Since $L/\mathbb{Q}_p$ is abelian, by lemma 6.2,

$$\sigma(a) = a^{\omega(\sigma)}(mod(\mathbb{Q}_p(\zeta_p)^\times)^p),\ \sigma \in Gal(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p).$$

Let v be the valuation on $\mathbb{Q}_p(\zeta_p)$ such that $v(\zeta_p - 1) = 1$. Then

$$v(a) = v(\sigma(a)) = \omega(\sigma)v(a)\ (mod\ p),\ for\ al\ \sigma.$$

Now if $\sigma \neq id$ the above equality gives $v(a) = 0\ (mod\ p)$.It is easy to verify that

$$\mathbb{Q}_p(\zeta_p)^\times = (\zeta_p - 1)^{\mathbb{Z}} \times W_{p-1} \times U_1$$

where W_{p-1} are the roots of unity in $\mathbb{Q}_p$ and $U_1 = \{u = 1\ (mod\ \zeta_p - 1)\}$. Since $p \mid v(a)$ and W_{p-1}'s elements are already pth powers, a is equivalent to an element in U_1. So assume $a \in U_1$. We can also assume $B \subset U_1/U_1^p$, and $Gal(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p)$ acts via ω. We claim that $U_1^p = \{u = 1\ (mod\ \pi^{p+1})\}$. Let $\pi = 1 - \zeta_p$. Now if $u \in U_1$ then $u = 1 + \pi x$. By looking at the binomial expansion one can show that $u^p = 1\ (mod\ \pi^{p+1})$. Conversely if $u_2 = 1\ (mod\ \pi^{p+1})$ then the binomial series for $(1 + u_2 - 1)^{1/p}$ converges. This proves the claim.

Let $u \in B$. Let $u = 1 + b\pi + \cdots$. Since $\zeta_p = 1 + \pi$ we have $\zeta_p^b = 1 + b\pi + \cdots$. Thus $u = \zeta_p^b u_1$ with $u_1 = 1\ (mod\ \pi^2)$. Since

$$\sigma(u) = u^{\omega\sigma}\ (mod\ U_1^p)$$

substituting $u = u_1\zeta_p^b$ yields $\sigma(u_1) = u_1^{\omega\sigma}\ (mod\ U_1^p)$. Write

$$u_1 = 1 + c\pi^d + \cdots$$

with $c \in \mathbb{Z}, p \nmid c$, and $d \geq 2$. Note that

$$\frac{\sigma(\pi)}{\pi} = \frac{\zeta_p^{\omega(\sigma)} - 1}{\zeta_p - 1} = \zeta_p^{\omega\sigma - 1} + \cdots + 1 = \omega(\sigma)\ (mod \pi).$$

So $(\sigma(\pi))/\pi = \omega(\sigma)\ (mod\ \pi)$.We have

$$\sigma(u_1) = 1 + c\omega(\sigma)^d\pi^d + \cdots$$

but

$$u_1^{\omega(\sigma)} = 1 + c\omega(\sigma)\pi^d + \cdots$$

Since $\sigma(u_1) = u_1^{\omega\sigma}\ (mod\ U_1^p)$ and $U_1^p = \{u = 1\ (mod\ \pi^{p+1})\}$, we have $\sigma(u_1) = u_1^{\omega(\sigma)}\ (mod\ \pi^{p+1})$. This means that either $d \geq p + 1$ or $d = 1\ (mod\ p - 1)$. The former means that $u_1 \in U_1^p$ and the latter means that $d = p$. Clearly $1 + \pi^p$ generates modulo U_1^p the subgroup of $u_1 = 1\ (mod\ \pi^p)$. We therefore obtained

$$B \subset \langle \zeta_p, 1 + \pi^p \rangle$$

where $\langle x, y \rangle$ denotes the group generated by x and y. Since $B \cong (\mathbb{Z}/p\mathbb{Z})^3$, we have a contradiction.

$\square$

For $p = 2$ one has to make a more careful analysis so we shall omit it here. For the proof of this case see [W] p. 329.

References

[S1] William Stein, *A Brief Introduction to Classical and Adelic Algebraic Number Theory*, Course Notes (2004).

[S2] William Stein, *Introduction to Algebraic Number Theory*, Course Notes (2005)

[G] Fernando Q. Gouvea, *p-adic numbers*, (1997).

[W] Lawrence C. Washington, *Introduction to Cyclotomic Fields*, (1997)

[F-V] I. B. Fesenko, S. V. Vostokov *Local Fields and their extensions*, (2002)

E-mail address: `nizam@mit.edu`