Kronecker-Weber via Ramification Theory

Sharad V. Kanetkar

In this note we prove the well known theorem of Kronecker-Weber using only ramification theory. The following steps are described in a series of exercises in [1, pp. 125-127].

Kronecker-Weber Theorem.

Theorem : Every finite abelian extension of $\mathbf{Q}$ (field of rational numbers) is contained in a cyclotomic field.
Proof : Let K be a finite abelian extension of $\mathbf{Q}$ with $G = \mathrm{Gal}(K/\mathbf{Q})$.

Step 1 : It is enough to assume that K is of degree p^m over $\mathbf{Q}$ for some prime p. For if G is expressed as a direct product of its Sylow subgroups :

$$G \cong S_{p_1} \times \cdots \times S_{p_r},$$

then fixed subfields k_i (of K) with groups S_{p_i} will generate K. If k_i belongs to a cyclotomic field F_i, for $i = 1, 2, \cdots, r$; then $K \subseteq F_1F_2 \cdots F_r \subseteq$ some cyclotomic field. Hence we assume $K = k_1$ and $[K : \mathbf{Q}] = p^m$.
Step 2 : It is enough to assume that p is the only prime ramified in K. Suppose $q \in \mathbf{Z}$ is a prime (other that p) which is ramified in K. Let $E(\cdot|\cdot)$ and $e(\cdot|\cdot)$ denote the inertia group and the ramification index respectively. Let U be a prime of K lying above q with $e(U \mid q) = e$. Now the higher ramification group $V_1(U \mid q)$ is a $q-$subgroup of a $p-$group G [1, page 121]. Hence $|V_1(U \mid q)| = 1$ and $|V_0/V_1| = e$. Since G is abelian $|V_0/V_1| \mid (q-1)$ [1, page 124, Ex. 26(c)]. This gives $e|(q-1)$. Now there is a (unique) subfield $K_1 \subseteq \mathbf{Q}(\zeta_q)$ (where $\mathbf{Q}(\zeta_m)$ denotes the m-th cyclotomic field, i.e. ζ_m is a primitive m-th root of unity) with $[K_1 : \mathbf{Q}] = e$. Since $e \mid p^m$ and $q \neq p$, q is tamely ramified in both K_1 and K. Now q is totally ramified in $\mathbf{Q}(\zeta_q)$ and hence in K_1. This gives that the ramification index of q in K_1 is also e. Let U_1 be a prime of L lying above U in K. Now, $\mathrm{Gal}(K/\mathbf{Q})$ and $\mathrm{Gal}(K_1/\mathbf{Q})$ are both p-groups and since $\mathrm{Gal}(L/\mathbf{Q})$ injects into $\mathrm{Gal}(K/\mathbf{Q}) \times \mathrm{Gal}(K_1/\mathbf{Q})$, it is also a p-group. This shows that $V_1(U_1 \mid q)$ is both a p-group and a q-group implying that it is trivial. Thus $E(U_1 \mid q)$ is cyclic. Let W be the (unique) prime of K_1 lying below U_1. Hence, by restriction, $E(U_1 \mid q)$ injects into $E(U \mid q) \times E(W \mid q)$. All these three groups are cyclic and the last two have

order e each. This shows that $E(U_1 \mid q)$ is of order e. Thus the ramification index of q in L is also e. Since $e(U_1 \mid q) = e(U \mid q) = e, e(U_1 \mid U) = 1$. Let L_1 be the inertia field of U_1, i.e., L_1 is the fixed field of $E(U_1 \mid q)$. Then for any field F containing $L_1, U_1 \cap F$ is totally ramified in L. Thus for $F = L_1K_1, (U_1 \cap F)$ is totally ramified in L. But $F \supset K_1$ and therefore $e(U_1 \mid (U_1 \cap F)) \mid e(U_1 \mid U)$. This implies $e(U_1 \mid U_1 \cap F) = 1$. Thus $U_1 \cap F$ is totally ramified as well as unramified in L implying $F = L$. Hence if L_1 belongs to a cyclotomic field then since $K_1 \subset \mathbf{Q}(\zeta_q)$, L will be a subfield of a cyclotomic field. But $K \subset L$ and hence K will be a subfield of some cyclotomic field proving the theorem. Thus it is enough to replace K by L_1. But it is easy to see that all unramified primes of K are unramified in L_1 and, in addition, q is also unramified in L_1 (but ramified in K). Thus continuing this process of reduction we can assume that there are no primes other that p which are ramified in K. This finishes the proof of step 2.

Step 3 : **Case(i)** $p = 2,\ [K : \mathbf{Q}] = 2^m$.
In this case 2 is totally ramified in K since otherwise no prime will be ramified in the fixed field of $E(U \mid 2)$ and this will imply, by [1,page 137, Cor.3], that $E(U \mid 2) = G$. Thus 2 is totally ramified in K. Thus $e(U \mid 2) = 2^m$. If $m = 1$ then $[K : \mathbf{Q}] = 2$ and $K = \mathbf{Q}[\sqrt{d}]$ for some square-free integer d. But the $\mathrm{Disc}(K/\mathbf{Q}) = d$ *or* $4d$. Since 2 is the only ramified prime of K, 2 is the only possible divisor of d. Hence

$$K = \mathbf{Q}[\sqrt{2}] \text{ or } \mathbf{Q}[\sqrt{-2}] \text{ or } \mathbf{Q}[\sqrt{1}].$$

All these fields are subfields of $\mathbf{Q}[\zeta_8]$. Hence the theorem is proved in this case. If $m > 1$ then consider $L = \mathbf{Q}(\zeta_{2^{m+2}}) \cap \mathbf{R}$, where $\mathbf{R}$ is the field of real numbers. Then $[L : \mathbf{Q}] = 2^m$ and $L \subset \mathbf{R}$. Hence L contains a unique quadratic subfield, namely $\mathbf{Q}[\sqrt{2}]$. Hence $\mathrm{Gal}(L/\mathbf{Q})$ contains unique subgroup of index 2. Thus L is a cyclic extension. Now consider the field LK. Let μ be the extension of σ (where $< \sigma >= \mathrm{Gal}(L \mid \mathbf{Q})$ to LK. Let F be the fixed field of μ. Since μ restricted to L generates $\mathrm{Gal}(L/\mathbf{Q}), F \cap L = \mathbf{Q}$. If $[F : \mathbf{Q}] > 2$ then $F \cap \mathbf{R} \neq \mathbf{Q}$ and it will contain $\mathbf{Q}[\sqrt{2}] \subset L$ but $F \cap L = \mathbf{Q}$. Hence $[F : \mathbf{Q}] \leq 2$. If $[F : \mathbf{Q}] = 2$ then $F = \mathbf{Q}[\sqrt{-2}]$ or $\mathbf{Q}[i]$ and both are contained in $\mathbf{Q}[\zeta_8]$. Thus $K \subseteq LK = FL \subseteq \mathbf{Q}(\zeta_{2^{m+2}})$ and the theorem is proved. If $F = \mathbf{Q}$ then $< \mu >= \mathrm{Gal}(LK/\mathbf{Q})$ and since

$$\mathrm{Gal}(LK/\mathbf{Q}) \hookrightarrow \mathrm{Gal}(L/\mathbf{Q}) \times \mathrm{Gal}(K/\mathbf{Q}),$$

order of any element of $\mathrm{Gal}(LK/\mathbf{Q}) \leq \mathrm{lcm}\ (|\ \mathrm{Gal}\ (L/\mathbf{Q})\ |, |\ \mathrm{Gal}\ (K/\mathbf{Q})\ |)$ $= 2^m$. Thus $2^m \leq [LK : \mathbf{Q}] \leq 2^m$. Hence $L = LK$ implying $K \subseteq L \subseteq \mathbf{Q}[\zeta_{2^{m+2}}]$. Thus the theorem is proved in this case also.

Case(ii) p is odd and $[K : \mathbf{Q}] = p^m$.
Consider the case $m = 1$. Hence K is of degree p over $\mathbf{Q}$ and p is the only ramified prime in K. Thus if U is the prime of K lying above p then $e(U \mid p) = p$.
Claim : $\mathrm{diff}(R/Z) = U^{2(p-2)}$, where R is the ring of integers of K.
Proof : Let $\pi \in U - U^2$ then π satisfies a monic irreducible polynomial over $\mathbf{Z}$, say,

$$f(x) = x^p + a_{p-1}x^{p-1} + \cdots + a_0.$$

Let ϑ_U be the valuation corresponding to the DVR R_U. Then $\vartheta_U(\pi) = 1$ and since $U^p = pR$, $\vartheta_U(p) = p$. Now the coefficients a_i are symmetric polynomials in $\sigma\pi$, $\sigma \in \mathrm{Gal}(K/\mathbf{Q})$ and $\vartheta_U(\sigma\pi) = 1$, $\forall\sigma \in \mathrm{Gal}(K/\mathbf{Q})$. Hence $\vartheta_U(a_i) \geq 1$ and hence $p \mid a_i$. But $a_0 = \pm\prod(\sigma\pi)$ and hence $\vartheta_U(a_0) = p$. Now in the expression

$$f'(\pi) = p\pi^{p-1} + (p-1)a_{p-1}\pi^{p-2} + \cdots + a_1,$$

all terms have valuations distinct *mod* p. Therefore

$$\begin{aligned} \vartheta_U(f'(\pi)) &= \min\{\vartheta_U(p\pi^{p-1}), \vartheta_U((p-1)a_{p-1}\pi^{p-2} \cdots \vartheta_U(a_1)\}. \\ \text{Hence, } 2p-1 &\geq \vartheta_U(f'(\pi)) \geq p. \end{aligned}$$

But by Hilbert's formula [1, page 124, Exc. 27],

$$\vartheta_U(f'(\pi)) = \vartheta_U(\mathrm{diff}(R/Z)) = \sum_{i=0}^{\infty}(\mid V_i \mid -1)$$

Since $\mid V_i \mid$ is a power of p, $(p-1) \mid \vartheta_U(f'(\pi))$. Hence $\vartheta_U(f'(\pi)) = 2p-2$. And $\mathrm{diff}(R/\mathbf{Z}) = U^{2p-2}$ (because no other prime is ramified in k). Thus the claim is proved.
Now let $m = 2$.
Claim : G is cyclic.
Proof : Consider the inertia field corresponding to the prime p. In this field p is unramified. Hence no prime is ramified in this inertia field. Hence it must be equal to $\mathbf{Q}$. Thus K is totally ramified with $e(U/p) = p^2$. Since V_1 is Sylow$-p$ subgroup of $\mathrm{Gal}(K/\mathbf{Q}), \mid V_1 \mid = p^2 = \mid V_0 \mid$. Let $V_r = V_r(U/p)$ be the least r for which $\mid V_r \mid < p^2$. But $V_{r-1}/V_r \hookrightarrow R/U \cong \mathbf{Z}/p\mathbf{Z}$ and hence $\mid V_r \mid = p$. Let H be any subgroup of G having order p. Let K_H be the fixed field of H. Then $[K_H : K] = p$ and $\mathrm{diff}(R_H/\mathbf{Q}]) = U^{2p-2}$. Hence from the transitivity of different,

$$\mathrm{diff}R/\mathbf{Z}) = \mathrm{diff}(R/R_H).U^{(2p-2)p}, \quad [1, \text{ page 96, Ex.38}].$$

Hence $\text{diff}(R/R_H)$ is independent of H as long as $[H : \mathbf{Q}] = p$. Now by Hilbert's formula the power of U dividing $\text{diff}(R/R_H)$ is given by

$$\alpha = \sum_{i=0}^{\infty} \mid V_i \cap H \mid -1.$$

Hence α is strictly maximized when $H = V_r$. Since α is independent of H, V_r is the only subgroup of order p in G. Thus G is cyclic, proving the claim. Thus in case $m = 1$, k is unique, otherwise KK_1 will be of degree p^2 containing two distinct subfields of degree p. Hence K is the unique subfield of $\mathbf{Q}[\zeta_{p^2}]$. Thus the theorem is true for the case $m = 1$.

Now let $m > 1$. Let L denote the unique subfield of $Q[\zeta_{p^{m+1}}]$ of degree p^m over $\mathbf{Q}$. Then $\text{Gal}(L/\mathbf{Q})$ is cyclic of order p^m. Then LK is cyclic by the claim. But

$$\text{Gal}(LK/\mathbf{Q}) \hookrightarrow \text{Gal}(L/\mathbf{Q}) \times \text{Gal}(k/\mathbf{Q}),$$

hence,

$$\begin{aligned} \mid \text{Gal}(LK/\mathbf{Q}) \mid &\leq lcm(\mid \text{Gal}(L/\mathbf{Q}) \mid, \mid \text{Gal}(K/\mathbf{Q}) \mid) \\ &= p^m. \end{aligned}$$

Therefore $L \subseteq LK \subseteq L$ and hence $K \subseteq L \subseteq \mathbf{Q}(\zeta_{p^{m+1}})$, and the theorem is proved in this case also.

REFERENCE

1. D. A. Marcus, *Number Fields*, Springer Verlag, 1977.

Sharad V. Kanetkar
Bhaskaracharya Pratishthana
56/14, Erandavane, Damle Path
Off Law College Road
Pune-411 004
e-mail : bhaskara_p@vsnl.com