Kronecker-Weber via Stickelberger

par Franz LEMMERMEYER


Abstract. In this note we give a new proof of the theorem of Kronecker-Weber based on Kummer theory and Stickelberger’s theorem.

Introduction

The theorem of Kronecker-Weber states that every abelian extension of $\mathbb{Q}$ is cyclotomic, i.e., contained in some cyclotomic field. The most common proof found in textbooks is based on proofs given by Hilbert [2] and Speiser [7]; a routine argument shows that it is sufficient to consider cyclic extensions of prime power degree $p^m$ unramified outside $p$, and this special case is then proved by a somewhat technical calculation of differentials using higher ramification groups and an application of Minkowski’s theorem, according to which every extension of $\mathbb{Q}$ is ramified. In the proof below, this not very intuitive part is replaced by a straightforward argument using Kummer theory and Stickelberger’s theorem.

In this note, $\zeta_m$ denotes a primitive $m$-th root of unity, and “unramified” always means unramified at all finite primes. Moreover, we say that a normal extension $K/F$

- is of type $(p^a, p^b)$ if $\text{Gal}(K/F) \cong (\mathbb{Z}/p^a\mathbb{Z}) \times (\mathbb{Z}/p^b\mathbb{Z})$;
- has exponent $m$ if $\text{Gal}(K/F)$ has exponent $m$.

1. The Reduction

In this section we will show that it is sufficient to prove the following special case of the Kronecker-Weber theorem (it seems that the reduction to extensions of prime degree is due to Steinbacher [3]):

Proposition 1.1. The maximal abelian extension of exponent $p$ that is unramified outside $p$ is cyclic: it is the subfield of degree $p$ of $\mathbb{Q}(\zeta_{p^2})$.

The corresponding result for the prime $p = 2$ is easily proved.
Proposition 1.2. The maximal real abelian 2-extension of \( \mathbb{Q} \) with exponent 2 and unramified outside 2 is cyclic: it is the subfield \( \mathbb{Q}(\sqrt{2}) \) of \( \mathbb{Q}(\zeta_8) \).

Proof. The only quadratic extensions of \( \mathbb{Q} \) that are unramified outside 2 are \( \mathbb{Q}(i), \mathbb{Q}(\sqrt{-2}) \), and \( \mathbb{Q}(\sqrt{2}) \).

The following simple observation will be used repeatedly below:

Lemma 1.3. If the compositum of two cyclic \( p \)-extensions \( K, K' \) is cyclic, then \( K \subseteq K' \) or \( K' \subseteq K \).

Now we show that Prop. 1.1 implies the corresponding result for extensions of prime power degree:

Proposition 1.4. Let \( K/\mathbb{Q} \) be a cyclic extension of odd prime power degree \( p^m \) and unramified outside \( p \). Then \( K \) is cyclotomic.

Proof. Let \( K' \) be the subfield of degree \( p^m \) in \( \mathbb{Q}(\zeta_{p^m+1}) \). If \( K'K \) is not cyclic, then it contains a subfield of type \( (p,p) \) unramified outside \( p \), which contradicts Prop. 1.1. Thus \( K'K \) is cyclic, and Lemma 1.3 implies that \( K = K' \).

Next we prove the analog for \( p = 2 \):

Proposition 1.5. Let \( K/\mathbb{Q} \) be a cyclic extension of degree \( 2^m \) and unramified outside 2. Then \( K \) is cyclotomic.

Proof. If \( m = 1 \) we are done by Prop. 1.2. If \( m \geq 2 \), assume first that \( K \) is nonreal. Then \( K(i)/K \) is a quadratic extension, and its maximal real subfield \( M \) is cyclic of degree \( 2^m \) by Prop. 1.2. Since \( K/\mathbb{Q} \) is cyclotomic if and only if \( M \) is, we may assume that \( K \) is totally real.

Now let \( K' \) be the maximal real subfield of \( \mathbb{Q}(\zeta_{2^{2m+2}}) \). If \( K'K \) is not cyclic, then it contains three real quadratic fields unramified outside 2, which contradicts Prop. 1.2. Thus \( K'K \) is cyclic, and Lemma 1.3 implies that \( K = K' \).

Now the theorem of Kronecker-Weber follows: first observe that abelian groups are direct products of cyclic groups of prime power order; this shows that it is sufficient to consider cyclic extensions of prime power degree \( p^m \). If \( K/\mathbb{Q} \) is such an extension, and if \( q \neq p \) is ramified in \( K/\mathbb{Q} \), then there exists a cyclic cyclotomic extension \( L/\mathbb{Q} \) with the property that \( KL = FL \) for some cyclic extension \( F/\mathbb{Q} \) of prime power degree in which \( q \) is unramified. Since \( K \) is cyclotomic if and only if \( F \) is, we see that after finitely many steps we have reduced Kronecker-Weber to showing that cyclic extensions of degree \( p^m \) unramified outside \( p \) are cyclotomic. But this is the content of Prop. 1.4 and 1.5.

Since this argument can be found in all the proofs based on the Hilbert-Speiser approach (see e.g. Greenberg [11] or Marcus [6]), we need not repeat the details here.
2. Proof of Proposition \[1.1\]

Let \( K/Q \) be a cyclic extension of prime degree \( p \) and unramified outside \( p \). We will now use Kummer theory to show that it is cyclotomic. For the rest of this article, set \( F = Q(\zeta_p) \) and define \( \sigma_a \in G = \text{Gal}(F/Q) \) by \( \sigma_a(\zeta_p) = \zeta_p^a \) for \( 1 \leq a < p \).

**Lemma 2.1.** The Kummer extension \( L = F(\sqrt[p]{\mu}) \) is abelian over \( Q \) if and only if for every \( \sigma_a \in G \) there is a \( \xi \in F^\times \) such that \( \sigma_a(\mu) = \xi^p \mu^a \).

For the simple proof, see e.g. Hilbert [3, Satz 147] or Washington [9, Lemma 14.7].

Let \( K/Q \) be a cyclic extension of prime degree \( p \) and unramified outside \( p \). Put \( F = Q(\zeta_p) \) and \( L = KF \); then \( L = F(\sqrt[p]{\mu}) \) for some nonzero \( \mu \in \mathcal{O}_F \), and \( L/F \) is unramified outside \( p \).

**Lemma 2.2.** Let \( q \) be a prime ideal in \( F \) with \( (\mu) = q^a \mathfrak{a}, \ q \nmid r \) and \( L/Q \) is abelian, then \( q \) splits completely in \( F/Q \).

**Proof.** Let \( \sigma \) be an element of the decomposition group \( Z(q|q) \) of \( q \). Since \( L/Q \) is abelian, we must have \( \sigma_a(\mu) = \xi^p \mu^a \). Now \( \sigma_a(q) = q \) implies \( q^a \parallel \xi^p \mu^a \), and this implies \( r \equiv ar \mod p \); but \( p \nmid r \) show that this is possible only if \( a = 1 \). Thus \( \sigma_a = 1 \), and \( q \) splits completely in \( F/Q \). \( \square \)

In particular, we find that \( (1 - \zeta) \nmid \mu \). Since \( L/F \) is unramified outside \( p \), prime ideals \( p \nmid p \) must satisfy \( p^{bp} \parallel \mu \) for some integer \( b \). This shows that \( (\mu) = a^p \) is the \( p \)-th power of some ideal \( a \). From \( (\mu) = a^p \) and the fact that \( L/Q \) is abelian we deduce that \( \sigma_a(a^p) = a^{pa} \xi^p \), where \( \sigma_a(\zeta_p) = \zeta_p^a \). Thus \( \sigma_a(c) = c^a \) for the ideal class \( c = [a] \) and for every \( a \) with \( 1 \leq a < p \). Now we invoke Stickelberger’s Theorem (cf. [4] or [5, Chap. 11]) to show that \( a \) is principal:

**Theorem 2.3.** Let \( F = Q(\zeta_p) \); then the Stickelberger element

\[
\theta = \sum_{a=1}^{p-1} a^{-1} \sigma_a^{-1} \in \mathbb{Z}[\text{Gal}(F/Q)]
\]

annihilates the ideal class group \( \text{Cl}(F) \).

From this theorem we find that \( 1 = \xi^p = \prod_{a=1}^{p-1} \sigma_a^{-1}(c)^a = \xi^{p-1} = c^{-1} \), hence \( c = 1 \) as claimed. In particular \( a = (a) \) is principal. This shows that \( \mu = \alpha^p \eta \) for some unit \( \eta \), hence \( L = F(\sqrt{\eta}) \). Now write \( \eta = \zeta^t \varepsilon \) for some unit \( \varepsilon \) in the maximal real subfield of \( F \). Since \( \varepsilon \) is fixed by complex conjugation \( \sigma_1 \) and since \( L/F \) is abelian, we see that \( \zeta^{-t} \varepsilon = \sigma_1(\mu) = \xi^p \mu^{-1} \), hence \( \zeta^{-t} \varepsilon = \xi^p \zeta^{-t} \varepsilon^{-1} \). Thus \( \varepsilon \) is a \( p \)-th power, and we find \( \mu = \zeta^t \). But this implies that \( L = Q(\zeta_p^t) \), and Prop. \[1.1\] is proved.

Since every cyclotomic extension is ramified, we get the following special case of Minkowski’s theorem as a corollary:
Corollary 2.4. Every solvable extension of $\mathbb{Q}$ is ramified.

Acknowledgement

It is my pleasure to thank the unknown referee for the careful reading of the manuscript.

References