The Kronecker-Weber Theorem

Lucas Culler

Introduction

The Kronecker-Weber theorem was one of the earliest results of class field theory. It says:

Theorem. *(Kronecker-Weber-Hilbert) Every abelian extension of the rational numbers $\mathbb{Q}$ is contained in a cyclotomic extension.*

Recall that an abelian extension is a finite field extension $K/\mathbb{Q}$ such that the galois group $\mathrm{Gal}(K/\mathbb{Q})$ is abelian, and a cyclotomic extension is an extension of the form $\mathbb{Q}(\zeta)$, where ζ is an n^{th} root of unity.
This paper consists of two proofs of the Kronecker-Weber theorem. The first is rather involved, but elementary, and uses Hilbert's theory of higher ramification groups. The second is a simple application of the main results of class field theory, which classifies abelian extension of an arbitrary number field.

An Elementary Proof

Now we will present an elementary proof of the Kronecker-Weber theoerem, in the spirit of Hilbert's original proof. The particular strategy used here is outlined in Marcus [1].

Minkowski's Theorem

We first prove a classical result due to Minkowski:

Theorem. *(Minkowski) Any finite extension of Q has nonzero discriminant. In particular, such extension is ramified at some prime $p \in \mathbb{Z}$.*

Proof. Let $K/\mathbb{Q}$ be a finite extension of degree n, and let $A = \mathcal{O}_K$ be its ring of integers. Consider the embedding:
s

$$A \longrightarrow \mathbb{R}^r \oplus \mathbb{C}^s$$

$$x \mapsto (\sigma_1(x), ..., \sigma_r(x), \tau_1(x), ..., \tau_s(x))$$

where the σ_i are the real embeddings of K and the τ_i are the complex embeddings, with one embedding chosen from each conjugate pair, so that n = r+2s. It is easily checked that this embeds A as a lattice Λ in $\mathbb{R}^n$, whose fundamental parallelogram has volume

$$\mathrm{Vol}(\mathbb{R}^n/\Lambda) = 2^{-s}\sqrt{\mathrm{disc}(K)}$$

Under this embedding, the norm of an element $x \in A$ is given by:

$$N(x) = |\sigma_1(x)| \cdots |\sigma_r(x)||\tau_1(x)|^2 + \ldots |\tau_s(x)|^2$$

which can easily be extended to a function on all of $\mathbb{R}^n$. Now consider the following convex region in $\mathbb{R}^n$:

$$C = \{x \in \mathbb{R}^n \mid \sum_{i=1}^{r} |x_{\sigma_i}| + 2\sum_{j=1}^{s} |x_{\tau_j}| < n\}$$

A page of integrals shows that the volume of this set is given by:

$$\text{Vol}(C) = \frac{2^r n^n}{n!} \left(\frac{\pi}{2}\right)^s$$

If $x \in C$, then $N(x) < 1$, because the geometric mean is bounded above by the arithmetic mean. Thus $x \cdot C \cap \Lambda = \{0\}$, since every nonzero element of A has norm at least 1. By Minkowski's convex body lemma, this implies:

$$\text{Vol}(C) \leq 2^n \text{Vol}(\mathbb{R}^n/\Lambda)$$

By definition of the norm and by the computations above, we see that:

$$\frac{2^r n^n}{n!} \left(\frac{\pi}{2}\right)^s \leq 2^n 2^{-s} \sqrt{\text{disc}(K)}$$

And therefore:

$$\text{disc}(K) \geq \left(\frac{\pi}{4}\right)^s \frac{n!}{n^n}$$

Since $\pi < 4$ and $n^n < n!$ if $n \neq 1$, we see that:

$$\text{disc}(K) > 1$$

This completes the proof, because the primes that ramify in the extension $K/\mathbb{Q}$ are precisely those that divide $\text{disc}(K)$.

□

Higher Ramification Groups

Next we show that it is enough to prove the Kronecker-Weber theorem in the case where all primes are wildly ramified. In this section, L/K is a finite extension of number fields, $A = \mathcal{O}_K$ and $B = \mathcal{O}_L$ are the rings of integers, P is a prime of A, and Q is a prime of B lying over P.

First we recall the definition of tame and wild ramification:

Definition. *We say that Q/P is tamely ramified if the ramification index $e(Q/P)$ is relatively prime to the characteristic of the residue field $\mathcal{O}_K/P$. Otherwise, we say that Q/P is wildly ramified.*

This proof of the Kronecker-Weber theorem makes extensive use of the higher ramification groups, which we now define:

Definition. *The nth ramification group $E_n(Q/P)$ is defined as follows:*

$$E_n(Q/P) = \{\sigma \in \text{Gal}(L/K) \mid \sigma(x) \equiv x \pmod{Q^{n+1}} \, \forall \, x \in B\}$$

In particular, if $n = 0$ we recover the inertial group $E(Q/P)$. If the context is clear, the Q and P will often be omitted.

It is clear that each E_n is a normal subgroup of the decomposition group $D = D(Q/P)$, so in particular E_{n+1} is normal in E_n.
One of the most fundamental facts about higher decomposition groups is the following:

Proposition. *There is a natural injective homomorphism $\phi_n : E_n/E_{n+1} \to U^{(n)}/U^{(n+1)}$, where $U^{(0)} = \hat{B}^\times$ and $U^{(n)} = 1 + \hat{Q}^n \subset \hat{B}^\times$ for $n > 0$.*

Proof. For convenience, we will work in the completions $\hat{A}$ and $\hat{B}$ at P and Q, respectively. This is justified by the isomorphism $D(Q/P) \to \mathrm{Gal}(\hat{L}/\hat{K})$, which takes $E_n(Q/P)$ isomorphically onto $E_n(\hat{Q}/\hat{P})$.
Let π be any uniformizer for $\hat{B}$. For any $\sigma \in E_n(Q/P)$, we have:

$$\sigma(\pi) = \alpha\pi$$

for some $\alpha \in \hat{B}^\times$. Since $\sigma \in E_n$, we have (for $n > 0$):

$$\pi \equiv \sigma(\pi) \equiv \alpha\pi \pmod{Q^{n+1}}$$

Thus $\alpha \in U^(n)$. Now let $u \in B$ be any unit. We have

$$\sigma(u) = \beta u$$

for some $\beta \in \hat{B}^\times$. Then:

$$\beta \equiv \sigma(u)u^{-1} \equiv uu^{-1} \equiv 1 \pmod{Q^{n+1}}$$

So the map

$$\phi_n(\sigma) = \sigma(\pi)/\pi$$

is a well defined homomorphism from E_n/E_{n+1} to $U^{(n)}/U^{(n+1)}$, and does not depend on the choice of uniformizer π. It is injective, because if

$$\alpha \equiv 1 \pmod{Q^{n+1}}$$

then for any $x = u\pi^k \in \hat{B}$, we have:

$$\sigma(x) \equiv \sigma(u\pi^k) \equiv \sigma(u)\sigma(\pi^k) \equiv u\alpha^k\pi^k \equiv u\pi^k \equiv x \pmod{Q^{n+1}}$$

□

This fairly simple observation has several useful corollaries:

Corollary. *Q/P is tamely ramified if and only if all the higher decomposition groups are trivial.*

Proof. ($\Rightarrow$) Simply note that, for $n > 1$, $|U^{(n)}/U^{(n+1)}| = |B/Q|$, since it is isomorphic to $1 + Q^n/Q^{n+1} \subset (R/Q^{n+1})^\times$. Hence, if $e(P/Q)$ is prime to p, the injective homomorphism ϕ_n must be 0, hence $E_n = 0$ for all $n > 1$.
($\Leftarrow$) Similarly, since $|U^{(0)}/U^{(1)}| = |R/P^\times|$, the order of E/E_1 must be prime to p. Hence, if p divides $|E|$, at least one higher ramification group must be nonzero. □

Corollary. *$D(Q/P)$ is solvable for any P and Q*

Proof. D/E is isomorphic to a subgroup of $\mathrm{Gal}(R/Q/S/P)$, which is abelian, and by the proposition, E_i/E_{i+1} is isomorphic to a subgroup of an abelian group. Thus the ramification groups form a filtration of D, and each of the quotients are abelian, so D is solvable. □

In the following sections, we will need the following stronger version of the proposition above:

Proposition. *Suppose D/E_1 is abelian. Then the image of the homomorphism $\phi_0 : E/E_1 \to (B/Q)^\times$ is contained in $(A/P)^\times$.*

Proof. Suppose the $\phi_0(\sigma) = \alpha$). Then we have:

$$\sigma(\pi) \equiv \alpha\pi \pmod{Q^{n+1}}$$

for any uniformizer π. Replacing π with $\tau^{-1}(\pi)$ for any $\tau \in D$, we see that:

$$\sigma(\tau^{-1}(\pi)) \equiv \alpha\tau^{-1}(\pi) \pmod{Q^{n+1}}$$

And thus

$$\sigma(\pi) \equiv \tau(\sigma(\tau^{-1}(\pi))) \equiv \tau(\alpha)\pi \pmod{Q^{n+1}}$$

Since any element of $\mathrm{Gal}(B/Q/A/P)$ is the restriction of an element of D, this shows that α is invariant under every element of $\mathrm{Gal}(B/Q/A/P)$. Hence $\alpha \in A/P$, as desired. □

Eliminating Tame Ramification

We now prove that it suffices to prove the Kronecker-Weber theorem in the case where no primes are tamely ramified.

Proposition. *Suppose a prime $p \in \mathbb{Z}$ is tamely ramified in an abelian extension $K/\mathbb{Q}$. Then there exists an extension $K'/\mathbb{Q}$ and a subfield $L \subset \mathbb{Q}(\zeta)$, for some nth root of unity ζ, such that:*

1. *Any prime that is unramified in K is also unramified in K'.*
2. *p is unramified in K'*
3. *$LK = LK'$*

Proof. Fix a prime P of K lying over p. Then $E_1 = E_1(P/p)$ is trivial, so E is isomorphic to a subgroup of $(\mathbb{F}_p)^\times$. Since $K/\mathbb{Q}$ is abelian, the ramification index e divides p-1.

Let ζ be a pth root of unity, and let $L \subset \mathbb{Q}(\zeta)$ be the unique subfield of order e. Since p is totally ramified in $\mathbb{Q}(\zeta)$, it is totally ramified in L also, and since p is prime to the order of $L/\mathbb{Q}$, p is tamely ramified in L. Let Q be the unique prime of L lying over p.

Now consider the composite LK. Let U be a prime of LK lying over Q, and let K' be its inertial field, that is, the fixed field of $E(U/P)$. We claim that K' is the extension described above.

Say $q \in \mathbb{Z}$ is unramified. Then q does not divide the discriminant of K, and since $q \neq p$, q does not divide the discriminant of L. Thus it does not divide the discriminant of KL, hence it is unramified in KL, hence it is unramified in K'. This shows that K' satisfies property 1 above.

Since any prime is unramified in its inertia field, property 2 is automatic. Thus it suffices to show that K' satisfies property 3.

First note that U is tamely ramified, since $E(U/p)$ injects into $\mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(L/Q)$, which has order prime to p. Thus $E(U/p)$ injects into the cyclic group $Z/p^{\times}$. Thus $E(U/p)$ is cyclic. But if we look at the image of $E(U/p)$ in $\mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(L/\mathbb{Q})$, we see that it is contained in $E(Q/p) \times \mathrm{Gal}(L/\mathbb{Q})$, which has exponent e. Thus $E(U/p)$ is a cyclic group of order at most e.

Since p is ramified in L with ramification index e, it must be ramified in $K'L$ with ramification index at least e. But p is unramified in K', so $[LK' : K] \geq e$. But $[LK : K] = e$, so $LK = LK'$, as desired. □

Thus we have reduced the Kronecker-Weber theorem to the case where all primes are wildly ramified. In fact, we can do better:

Proposition. *It suffices to prove the Kronecker-Weber theorem in the case where $[K : Q] = p^k$ for some prime $p \in \mathbb{Z}$, $\mathrm{Gal}(K/\mathbb{Q})$ is cyclic, and p is the only ramified prime.*

Proof. Since any abelian group is a direct sum of cyclic group of prime power order, any abelian extension is a composite of cyclic extensions of prime power degree. The proposition above allows us to assume that p is the only ramified prime in each of these cyclic extensions. □

Reduction to the Crucial Case

We now reduce further to the case where $[K : Q]$ is a prime p and $\mathrm{disc}(K)$ is a power of p. In particular, we show that the Kronecker-Weber theorem is implied by the following two results:

Proposition (1). *Let p be an odd prime. Then there is a unique extension $K/\mathbb{Q}$ of order p such that* $\mathrm{disc}(K)$ *is a power of p.*

Proposition (2). *The only quadratic extensions of $\mathbb{Q}$ with discriminant a power of 2 are $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$, or $\mathbb{Q}(\sqrt{-2})$.*

Note that the second statement is obvious, since the discriminant of $K = \mathbb{Q}(\sqrt{d})$, where d is a squarefree integer, is given by:

$$\mathrm{disc}(K) = \begin{cases} d & d \equiv 1 (\mathrm{mod}\, 4) \\ 4d & d \equiv 2, 3 (\mathrm{mod}\, 4) \end{cases}$$

The first statement is more difficult, so we postpone its proof to the following section. For now, we shall use it, along with the reductions achieved in the previous section, to deduce the Kronecker-Weber theorem:

Theorem. *Assuming proposition 1, any cyclic extension $K/\mathbb{Q}$ of degree p^n whose discriminant is a power of p is contained in $\mathbb{Q}(\zeta)$, where ζ is a p^{n+1}st root of unity if p is odd and a 2^{n+2}nd root of unity if $p = 2$. By the results of the previous section, therefore, any abelian extension of $\mathbb{Q}$ is contained in a cyclotomic extension.*

Proof. We define an extension L of $\mathbb{Q}$ as follows: if p is odd, let L be the unique subfield of $\mathbb{Q}(\zeta)$ of order p^n; otherwise, let L be $\mathbb{Q}(\zeta) \cap \mathbb{R}$. KL is again an extension whose order is a power of p. We will show that KL is contained in $\mathbb{Q}(\zeta)$.

In both cases, $\mathrm{Gal}(L/\mathbb{Q})$ is cyclic. Let τ be a generator, and let $\tilde{\tau}$ be any automorphism of KL extending τ. Let F be the fixed field of $\tilde{\tau}$. Since the fixed field of τ is $\mathbb{Q}$, $L \cap F = \mathbb{Q}$. There is an injection $\mathrm{Gal}(LK/Q) \to \mathrm{Gal}(L/\mathbb{Q}) \times \mathrm{Gal}(K/\mathbb{Q})$, which has exponent p^n, so $\tilde{\tau}$ has order at most p^n. On the other hand, it extended τ, which had order p^n, so $\tilde{\tau}$ has order exactly p^n. Thus

$[KL : F] = p^n$. We will show that $[FL : F] = p^n$, hence $KL = FL$, and that $FL \subset \mathbb{Q}(\zeta)$, hence $K \subset \mathbb{Q}(\zeta)$

For the case $p = 2$, consider the automorphism of F given by complex conjugation. Its fixed field is a subfield of $\mathbb{R}$ of degree 2^k, and thus contains a quadratic subfield. By Proposition 2, this must be $\mathbb{Q}(\sqrt{2})$. Similarly, L must contain $\mathbb{Q}(\sqrt{2})$, but this is a contradiction, since we had proved that $L \cap F = \mathbb{Q}$. Thus the fixed field of complex conjugation, acting on F, must be $\mathbb{Q}$. But then the fundamental theorem of Galois theory shows that F is a quadratic extension, since complex conjugation has order 2. Hence $F = \mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-2})$, so $FL = \mathbb{Q}(\zeta)$ and $[FL : F] = 2^n$, as desired.

For the case where p is odd, note that if $F \neq \mathbb{Q}$, then both L and F contain the unique cyclic extension of degree p with discriminant a power of p. This is a contradiction, since F was defined to be the fixed field of an automorphism that generates $\mathrm{Gal}(L/\mathbb{Q})$, which by Galois theory implies that $L \cap F = \mathbb{Q}$. Thus $F = \mathbb{Q}$, and $FL = L \subset \mathbb{Q}(\zeta)$, so $[FL : F] = [L : \mathbb{Q}] = p^n$, as desired.

□

The Crucial Case

Now we have proved the Kronecker-Weber theorem, modulo proposition 1 of the previous section. We now recall the statement and provide the missing proof. Note that we depart from Marcus in the proof of this fact; instead we are following the approach used by Hilbert in his Zahlbericht. [2]

Proposition (1). *There is a unique extension $K/\mathbb{Q}$ of degree p with discriminant a power of p; in particular, it is the unique subfield of $\mathbb{Q}(\zeta)$ of degree p over $\mathbb{Q}$, where ζ is a p^2th root of unity.*

Proof. Let K be the unique subfield of the p^2th cyclotomic field of order p. Then K is ramified only at the prime p, which shows existence of an extension with the desired properties.

Now suppose that K' is another such extension. We want to show that $K = K'$. To do this, first take the composite $K'L$ with the pth cyclotomic field $L = \mathbb{Q}(\zeta)$. Since L contains the pth roots of unity, the standard results of Kummer theory apply, so $K'L = L(\sqrt[p]{\alpha})$ for some $\alpha \in L$. For example, if $K = K'$, then α could be ζ, or a number of the form $\zeta^k \beta^p$ for some $k \in \mathbb{Z}$ not divisible by p and some $\beta \in L$.

Let $\lambda = 1 - \zeta$. Then $N(\lambda) = p$, so λ generates the unique prime ideal of L lying over p. We will now show that α can be chosen to be an algebraic integer satisfying

$$\alpha \equiv 1 (\mathrm{mod}\, \lambda^p)$$

First we can choose α to be prime to p. To see this, we use the fact that $K'L$ is abelian. Consider a generator τ for $\mathrm{Gal}(L/\mathbb{Q})$, and extend it to an automorphism $\tau \in \mathrm{Gal}(K'L/\mathbb{Q})$. Also consider a generator σ for $\mathrm{Gal}(K'L/L)$. Since σ and τ commute, we have:

$$\sigma(\tau(\sqrt[p]{\alpha})) = \tau(\sigma(\sqrt[p]{\alpha})) = \tau(\zeta \sqrt[p]{\alpha}) = \zeta^l \tau(\sqrt[p]{\alpha})$$

for some primitive root l modulo p. This shows that $\sqrt[p]{\alpha}$ is an eigenvector of σ with eigenvalue ζ^l. Hence

$$\tau(\alpha) = \tau(\sqrt[p]{\alpha})^p = \left(c \sqrt[p]{\alpha^l}\right)^p = c^p \alpha^l$$

Now it is clear that α can be chosen to be prime to p. Simply replace α by $\frac{\tau(\alpha)}{\alpha}$. Since the ideal generated by λ is invariant under τ, any factor of λ dividing α cancels out, leaving something prime

to p. Note that once α is prime to p, we can also force α to be congruent to 1 mod λ by raising α to a suitable power, since the multiplicative group of a finite field is cyclic. Also, using the fact that

$$\zeta^a \equiv 1 - a\lambda(\mathrm{mod}\lambda^2)$$

we can force α to be congruent to 1 mod λ^2 by multiplying by a suitable power of ζ. Finally, we use induction to obtain the desired congruence. Say we have already shown that

$$\alpha \equiv 1 + a\lambda^e(\mathrm{mod}\lambda^{e+1})$$

Now we use again the fact that $K'L$ is abelian. we have the congruence

$$\sigma(\alpha) \equiv c^p\alpha^l(\mathrm{mod}\lambda^{e+1})$$

which, given our assumption, implies that

$$c \equiv c^p \equiv 1(\mathrm{mod}\lambda)$$

and therefore

$$c^p \equiv 1(\mathrm{mod}p)$$

As a consequence we have

$$1 + a(l\lambda)^e \equiv \sigma(\alpha) \equiv \alpha^l \equiv 1 + al(\lambda^e)(\mathrm{mod}\lambda^e)$$

and therefore

$$l^e \equiv l(\mathrm{mod}\lambda)$$

but l was supposed to be a primitive root modulo λ and e was greater than 1. The inductive step works as long as e is less than p, so we have shown

$$\alpha \equiv 1 + a\lambda^p(\mathrm{mod}\lambda^{p+1})$$

or in other words

$$\alpha \equiv 1(\mathrm{mod}\lambda^p)$$

as desired. That $K = K'$ follows immediately from this. To see why, consider the number

$$\xi = \frac{1 - \sqrt[p]{\alpha}}{\lambda}$$

This is an algebraic integer, because $1 - \alpha$ is divisible by λ. Its minimal polynomial is given by:

$$f(x) = \left(x - \frac{1}{\lambda}\right)^p - \frac{\alpha}{\lambda^p}$$

Thus the discriminant of $KK'L$ over KL must contain the ideal generated by

$$\pm N\left(f'(\xi)\right) = \pm N\left(p(\xi - \frac{1}{\lambda})^{p-1}\right) = \epsilon\alpha^{p-1}$$

for some unit ϵ. In particular, the discriminant is prime to p. But then p is unramified in the extension $KK'L/KL$. Hence p is unramified in the inertial field $T/\mathbb{Q}$. But p was the only ramified prime in K, K', and L, hence no prime other than p can be ramified in T. But this is a contradiction, since there are no unramified extensions of $\mathbb{Q}$.

□

This lemma completes the proof of the Kronecker-Weber theorem. I think it is somewhat interesting that none of the "elementary" proofs of the Kronecker-Weber theorem I was able to find in modern literature make use of the argument above, despite how truly elementary it is.

Class Field Theory

The proof of the Kronecker-Weber theorem presented above is very similar to Hilbert's orginal proof, which he gave in 1895, finishing the work of Kronecker (1853) and Weber (1886). Some decades later, class field theory emerged, which gave a classification of the abelian extensions of an arbitrary number field. We now turn to a summary of the main results of class field theory. Once these results have been stated, we will use them to reprove the Kronecker-Weber theorem.

Adèles and Idèles

Let K be a number field, and let $R = \mathcal{O}_K$ be its ring of integers. We define the adèles of K to be the restricted direct product

$$\mathbb{A}_K = \prod_P \hat{K}_P$$

where $\hat{K}_P$ denotes the completion of K at the (possibly inifinite) prime $P \subset R$. By restricted direct product we mean that an element of $\mathbb{A}_K$ is a tuple (a_P) such that $a_P \in \hat{K}_P$ for all P and $a_P \in \hat{R}_P$ for all but finitely many P. We give $\mathbb{A}_K$ the restricted direct product topology, meaning that we take as a basis the set of all products $\prod_P U_P$, where $U_P \subset \hat{K}_P$ is an open subset and $U_P \subset \hat{R}_P$ for all but finitely many P. Note that under this topology, $\mathbb{A}_K$ becomes a locally compact topological group.

Note that K embeds in $\mathbb{A}_K$ as a discrete additive subgroup, because the standard product formula

$$\prod_P |a|_P = 1,$$

which holds for all $a \in K^\times$, implies that $|a|_P$ cannot be simultaneously small for all primes P. Thus there is a neighborhood of 0 that contains no nonzero elements of K.

The group of units of $\mathbb{A}_K$ is denoted $\mathbb{I}_K$ and is called the group of idèles. Thus an idèle is an adèle such that all but finitely many of its coordinates are units in $\hat{R}_P$. Note that $\mathbb{I}_K$ is also a locally compact topological group. Perversely, however, it is not given the subspace topology inherited from its inclusion into $\mathbb{A}_K$. Rather, it is given the restricted product topology with respect to the open sets $U_P = \hat{R}_P^\times$. One reason for this is that otherwise the inversion map would not be continuous. To see this, note that in the adeles, a neighborhood basis for 1 is given by all sets of the form

$$\prod_{P \in S} V_P \times \prod_{P \notin S} W_P$$

where S is a finite set, V_P is an open subset of $\hat{K}_P$ containing 1, and W_P is the set of nonzero elements of $\hat{R}_P$. Each of these sets contains a sequence that tends to zero in $\mathbb{A}_K$, so any neighborhood of 1 must contain such a sequence. However, the inverse image of any of the basic open sets under inversion contains no such sequence, so inversion cannot be continuous.

In the topology described above, a neighborhood basis for 1 is given by all sets of the form:

$$\prod_{P \in S} V_P \times \prod_{P \notin S} U_P$$

where S is any finite set containing the infinite primes, V_P is an open subset of $\hat{K}_P$ containing 1, and U_P is the group of units of $\hat{R}_P$. Keeping in mind the counterexample above, it is clear that this new topology gives the idèles the structure of a locally compact topological group.

The construction of the adèles and idèles may seem pointlessly formal, but it is important to keep in mind that these tools were developed only after the main results of class field theory had been proven several times over. Thus they are an historically inaccurate starting point for any treatment of class field theory, and are not strictly necessary to communicate the ideas of the subject. On the other hand, they provide a convenenient language in which to state the classification of abelian extensions, and that is all that will be attempted in this exposition.

The Idèle Class Group

As in the case of the adèles, $K^\times$ embeds in $\mathbb{I}_K$ as a discrete subgroup. The image of the inclusion is called the group of principal idèles. In analogy with the usual class group, we define the idèle class group to be the quotient of the idèles by the principal idèles:

$$C_K = \mathbb{I}_K / K^\times$$

Since the principal idèles are a discrete subgroup, the idèle class group inherits the structure of a locally compact group.

It is worth noting that the usual class group can be recovered from the idèle class group. In particular, there is a surjective homomorphism

$$\begin{aligned} \mathbb{I}_K &\longrightarrow \mathrm{Div}(K) \\ \alpha &\mapsto \prod_{p \nmid \infty} P^{v_P(\alpha)} \end{aligned}$$

which descends to a surjective homomorphism

$$C_K \to Cl_K$$

where Cl_K is the usual class group of K.

One of the original constructions preceding the development of class field theory was the discovery of the Hilbert class field: a maximal unramified abelian extension H_K/K such that every real place of K remains real in H_K. As it turns out, $\mathrm{Gal}(H_K/K)$ is isomorphic to Cl_K. Indeed, under the correspondence indicated above, the Hilbert class field corresponds to Cl_K. In some sense, finite quotients of the idèle class group can be thought of as generalized class groups. The main idea of class field theory is that each of these generalized class groups is the galois group of an abelian

extension of K, and furthermore, that every abelian extension arises in this way. These statements will be expanded and made more precise in the following sections.

The Norm Map

Recall that for a finite field extension L/K, we have the norm map

$$N_K^L : L \to K$$
$$\alpha \mapsto \det(l_\alpha)$$

where $l_\alpha : L \to L$ is the linear transformation given by multiplication on the left by α.

Now let L and K be number fields. We define a map, also called the norm map,

$$\mathcal{N} : \mathbb{A}_L \to \mathbb{A}_K$$

by simply taking the product of all the local norm maps:

$$\mathcal{N}\left(\prod_Q \alpha_Q\right) = \prod_P \prod_{Q|P} N_{\hat{K}_P}^{\hat{L}_Q}(\alpha_P)$$

where Q runs over all primes of L and P runs over all primes of K. Since the norm of a unit is a unit, and all but finitely many coordinates of α are units for all α in $\mathbb{I}_L$, the map $\mathcal{N}$ takes $\mathbb{I}_L$ to $\mathbb{I}_\mathbb{K}$. Furthermore, when we restrict $\mathcal{N}$ to the principal idèles, we obtain the usual norm map N_K^L. In particular, the norm map descends to a map

$$\mathcal{N} : C_L \to C_K$$

Given any finite extension L/K, we can form the corresponding norm subgroup:

$$\mathcal{N}_L = \mathcal{N}(C_L) \subset C_K$$

This is a closed subgroup of finite index in C_K, although this is not trivial to prove. One can ask to what extent the norm subgroup determines the extension L/K. The answer is that it is determined by the maximal abelian subextension L^{ab}/K, as we shall see below.

Abelian Extensions and the Kronecker-Weber Theorem

We can now state the main theorem on abelian extensions. This is not the only result of class field theory - for example, there is also Artin reciprocity – but it directly generalizes the Kronecker-Weber theorem, so it is the only result from class field theory that we shall be interested in.

Theorem. *If L/K is any finite extension of number fields, then we have the following:*

1. *The norm subgroup $\mathcal{N}_L$ is a closed subgroup of finite index in C_K.*
2. *There is a natural isomorphism $\mathrm{Gal}(L/K)^{ab} \to C_K/\mathcal{N}_L$.*
3. *The map $L \mapsto \mathcal{N}_L$ is a 1-1 correspondence between the finite abelian extensions L/K and closed subgroups of finite index in C_K.*

This theorem evidently generalizes the Kronecker-Weber theorem to an arbitrary number field. Conversely, if we calculate the idèle class group of $\mathbb{Q}$, and compute the norm subgroups corresponding to the cyclotomic fields, then we should be able to deduce the Kronecker-Weber theorem.

Proposition. *The idèle class group of $\mathbb{Q}$ is isomorphic to $\hat{Z}^\times \oplus \mathbb{R}_+^\times$.*

Proof. Let $\alpha = (\alpha_p) \in \mathbb{I}_\mathbb{Q}$ be an idèle. Consider the rational number

$$\beta = \prod_{p \neq \infty} p^{-v_p(\alpha)}$$

Then $\alpha\beta$ is an idèle with the property that each of its finite coordinates is a unit in $\mathbb{Q}_p$. Multiplying by ± 1, we can assume that its infinite coordinate is positive. Noting that any idèle class can be written uniquely in this way, and checking a few details, we see that

$$C_\mathbb{Q} \simeq \prod_{p \neq \infty} \mathbb{Z}_p^\times \oplus \mathbb{R}_\times^+$$

By the chinese remainder theorem,

$$\hat{Z}^\times \simeq \prod_{p \neq \infty} \mathbb{Z}_p^\times$$

so we obtain the desired conclusion.

□

We can now easily prove the Kronecker-Weber theorem.

Theorem. *(Kronecker-Weber-Hilbert) Every abelian extension of $\mathbb{Q}$ is contained in a cyclotomic extension.*

Proof. Let $x = (t, u_2, u_3, u_5, \dots)$ be any element of C_K. We will show that if not all u_p are equal to 1, then there is a cyclotomic extension L/K such that $x \notin \mathcal{N}_L$.
Say $u_p \neq 1$. Then $u_p = n + p^k x$ for some integer n, relatively prime to p, and some $x \in \mathbb{Z}_p \setminus p\mathbb{Z}_p$. Let $K/\mathbb{Q}$ be a a subextension of a cyclotomic extension such that p is totally ramified with ramification index p^{k+1}. Let $\hat{K}$ be its completion at the unique prime lying over p, and let π be a uniformizer for the ring of integers of $\hat{K}$.
If $u \in \hat{K}$ is a unit, then $u = m + \pi y$ for some integer m, relatively prime to p, and some $y \in R$. Then

$$N(u) = m^{p^{k+1}} + p^{k+1} Tr(\pi y) + \text{terms higher order in p}$$

Thus $N(u) \neq u_p$, since either they are distinct mod p or u_p is farther from 1 in the p-adic metric. Thus u_p is not a norm of any element of $\hat{K}$, hence x is not a norm of any element of $\mathbb{I}_K$.

Thus the norm subgroups of $\mathbb{I}_Q$ coming from cyclotomic extensions completely exhaust $\prod_{p \neq \infty} \mathbb{Z}_p^\times$. In other words, the intersection of the norm subgroups of all cyclotomic extensions is $\mathbb{R}_+^\times$. But $\mathbb{R}_+^\times$ is contained in the norm subgroup of any abelian extension. Since the bijection between abelian extensions and norm subgroups reverses containment, this shows that any abelian extension of $\mathbb{Q}$ is contained in a cyclotomic extension.

□

References

[1] Marcus, Number Fields

[2] Lemmermeyer, "Kronecker-Weber via Stickelberger"

[3] http://modular.fas.harvard.edu/papers/ant/html/node86.html