Class Number One

Thomas Browning

November 2020

1 The Cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$

1.1 Galois Theory

Fix a prime p.

1.1.1 Odd Primes

If p is odd then for each $k \geq 0$, $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^{k+1}})/\mathbb{Q})$ is cyclic of order $(p-1)p^k$. By the Galois correspondence, there is a unique subfield $\mathbb{B}_k \subseteq \mathbb{Q}(\zeta_{p^{k+1}})$ such that $\mathrm{Gal}(\mathbb{B}_k/\mathbb{Q})$ is cyclic of order p^k. If $k \geq 1$ then by the Galois correspondence, there is a unique subfield of $\mathbb{B}_k$ whose Galois group over $\mathbb{Q}$ is cyclic of order p^{k-1}. This must be $\mathbb{B}_{k-1}$. Thus, $\mathbb{B}_{k-1}$ is contained in $\mathbb{B}_k$. We obtain a chain

$$\mathbb{Q} = \mathbb{B}_0 \subseteq \mathbb{B}_1 \subseteq \mathbb{B}_2 \subseteq \cdots$$

where $\mathrm{Gal}(\mathbb{B}_k/\mathbb{Q}) \cong \mathbb{Z}/p^k\mathbb{Z}$ and $\mathbb{B}_k \subseteq \mathbb{Q}(\zeta_{p^{k+1}})$.

1.1.2 Even Primes

If $p = 2$ then let

$$\mathbb{B}_k = \mathbb{Q}(\cos(\pi/2^{k+1})) = \mathbb{Q}(\zeta_{2^{k+2}} + \zeta_{2^{k+2}}^{-1}) \subseteq \mathbb{Q}(\zeta_{2^{k+2}})$$

for $k \geq 0$. Note that $\mathbb{B}_k$ is a subfield of $\mathbb{R}$, so it is a proper subfield of $\mathbb{Q}(\zeta_{2^{k+2}})$. Then the polynomial relation

$$\zeta_{2^{k+2}}^2 - (\zeta_{2^{k+2}} + \zeta_{2^{k+2}}^{-1})\zeta_{2^{k+2}} + 1 = 0.$$

shows that $[\mathbb{Q}(\zeta_{2^{k+2}}) : \mathbb{B}_k] = 2$, which forces $\mathbb{B}_k$ to be the fixed field of $\mathbb{Q}(\zeta_{2^{k+2}})$ under complex conjugation. There are two consequences of this. Firstly, $\mathbb{B}_{k-1}$ is contained in $\mathbb{B}_k$ for $k \geq 1$. Secondly,

$$\mathrm{Gal}(\mathbb{B}_k/\mathbb{Q}) \cong \frac{(\mathbb{Z}/2^{k+2}\mathbb{Z})^\times}{\{\pm 1\}} \cong \mathbb{Z}/2^k\mathbb{Z}.$$

We obtain a chain

$$\mathbb{Q} = \mathbb{B}_0 \subseteq \mathbb{B}_1 \subseteq \mathbb{B}_2 \subseteq \cdots$$

where $\mathrm{Gal}(\mathbb{B}_k/\mathbb{Q}) \cong \mathbb{Z}/2^k\mathbb{Z}$ and $\mathbb{B}_k \subseteq \mathbb{Q}(\zeta_{2^{k+2}})$. We summarize these results in the following theorem.

Theorem 1. *There is a chain*

$$\mathbb{Q} = \mathbb{B}_0 \subseteq \mathbb{B}_1 \subseteq \mathbb{B}_2 \subseteq \cdots$$

where $\mathrm{Gal}(\mathbb{B}_k/\mathbb{Q}) \cong \mathbb{Z}/p^k\mathbb{Z}$. *If* p *is odd then* $\mathbb{B}_k \subseteq \mathbb{Q}(\zeta_{p^{k+1}})$. *If* $p = 2$ *then* $\mathbb{B}_k \subseteq \mathbb{Q}(\zeta_{2^{k+2}})$.

1.2 Ramification Theory

It is known that the extension $\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}$ is totally ramified at the prime p and unramified at every other prime. From this we can deduce the ramification of the extensions $\mathbb{B}_k/\mathbb{Q}$.

Lemma 2. *The extension $\mathbb{B}_k/\mathbb{Q}$ is totally ramified at the prime p and unramified at every other prime.*

Combining Lemma 2 with the following proposition will allow us to deduce that the class number of $\mathbb{B}_k$ is indivisible by p. The proof of the following proposition is adapted from the proof of Theorem 10.4 in Washington's *Introduction to Cyclotomic Fields*.

Proposition 3. *Let K be a number field. Assume that $K/\mathbb{Q}$ is Galois and that $\mathrm{Gal}(K/\mathbb{Q})$ is a p-group. Also assume that at most one prime of $\mathbb{Q}$ ramifies in $K/\mathbb{Q}$. Then the class number of K is indivisible by p.*

Proof. By class field theory, there exists a number field H (the p-Hilbert class field of K) such that:

(a) H is Galois over $\mathbb{Q}$,

(b) K is contained in H,

(c) The extension H/K is unramified,

(d) The degree $[H : K]$ equals the power of p dividing the class number of K.

Let $G = \mathrm{Gal}(H/\mathbb{Q})$. Let $\mathfrak{q}$ be the prime of $\mathbb{Q}$ that ramifies in $K/\mathbb{Q}$. If no such prime exists then let $\mathfrak{q}$ be any prime of $\mathbb{Q}$. Let $\mathfrak{r}$ be a prime of H lying over $\mathfrak{q}$. Let $I_{\mathfrak{r}/\mathfrak{q}} \leq G$ be the inertia subgroup.

Now assume that the class number of K is divisible by p. Then (d) implies that the extension H/K is nontrivial. Then (c) implies that $\mathfrak{q}$ is not totally ramified in $H/\mathbb{Q}$. In particular, $I_{\mathfrak{r}/\mathfrak{q}} \lneq G$. By the theory of p-groups, $I_{\mathfrak{r}/\mathfrak{q}}$ is contained in a proper normal subgroup N of G. Then the fixed field F of N is a nontrivial Galois extension of $\mathbb{Q}$. Let $\mathfrak{r}_0$ be the prime of F lying under $\mathfrak{r}$. Since $I_{\mathfrak{r}/\mathfrak{q}}$ is contained in N, we know that $e_{\mathfrak{r}_0/\mathfrak{q}} = 1$. Since $F/\mathbb{Q}$ is Galois, $\mathfrak{q}$ is unramified in $F/\mathbb{Q}$. Since all other primes of $\mathbb{Q}$ are unramified in $H/\mathbb{Q}$, $F/\mathbb{Q}$ is unramified. This is a contradiction since $\mathbb{Q}$ has no nontrivial unramified extensions. □

Theorem 4. *The class number of $\mathbb{B}_k$ is indivisible by p.*

Proof. By Theorem 1 and Lemma 2, $\mathbb{B}_k$ satisfies the conditions of Proposition 3. □

1.3 Ideal Class Groups

Let L/K be an extension of number fields.

- Let $\mathcal{F}_K$ and $\mathcal{F}_L$ denote the groups of fractional ideals of K and L.
- Let $\mathcal{P}_K$ and $\mathcal{P}_L$ denote the groups of principal fractional ideals of K and L.
- Let Cl_K and Cl_L denote the ideal class groups of K and L.

1.3.1 The Upward Map

There is a homomorphism $\mathcal{J}_{L/K} \colon \mathcal{F}_K \to \mathcal{F}_L$ defined by $\mathcal{J}_{L/K}(I) = I\mathcal{O}_L$. Then $\mathcal{J}_{L/K}(\alpha\mathcal{O}_K) = \alpha O_L$, which shows that $\mathcal{J}_{L/K}(\mathcal{P}_K) \subseteq \mathcal{P}_L$. In particular, $\mathcal{J}_{L/K} \colon \mathcal{F}_K \to \mathcal{F}_L$ induces a map $J_{L/K} \colon Cl_K \to Cl_L$.

1.3.2 The Downward Map

There is a homomorphism $\mathcal{N}_{L/K} \colon \mathcal{F}_L \to \mathcal{F}_K$ defined by $\mathcal{N}_{L/K}(\mathfrak{q}) = \mathfrak{p}^{f(\mathfrak{q}/\mathfrak{p})}$ and extending multiplicatively. It is a fact of algebraic number theory that $\mathcal{N}_{L/K}(\alpha\mathcal{O}_L) = N_K^L(\alpha)\mathcal{O}_K$, which shows that $\mathcal{N}_{L/K}(\mathcal{P}_L) \subseteq \mathcal{P}_K$. In particular, $\mathcal{N}_{L/K} \colon \mathcal{F}_L \to \mathcal{F}_K$ induces a map $N_{L/K} \colon Cl_L \to Cl_K$.

1.3.3 Compatibility I

Lemma 5. *The composition $N_{L/K} \circ J_{L/K} \colon Cl_K \to Cl_K$ is the $[L:K]$th power map.*

Proof. Let $\mathfrak{p}$ be a prime of K and let $\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_g^{e_g}$. Then

$$\begin{aligned}
\mathcal{N}_{L/K}(\mathcal{J}_{L/K}(\mathfrak{p})) &= \mathcal{N}_{L/K}(\mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_g^{e_g}) \\
&= \mathcal{N}_{L/K}(\mathfrak{q}_1)^{e_1} \cdots \mathcal{N}_{L/K}(\mathfrak{q}_g)^{e_g} \\
&= (\mathfrak{p}^{f_1})^{e_1} \cdots (\mathfrak{p}^{f_g})^{e_g} \\
&= \mathfrak{p}^{e_1 f_1 + \cdots + e_g f_g} \\
&= \mathfrak{p}^{[L:K]}.
\end{aligned}$$

The result follows from extending multiplicatively and passing to the quotient. □

Proposition 6. *If $|Cl_K|$ is coprime to $[L:K]$ then $J_{L/K} \colon Cl_K \to Cl_L$ is injective and $N_{L/K} \colon Cl_L \to Cl_K$ is surjective.*

Proof. Lemma 5 states that $N_{L/K} \circ J_{L/K} \colon Cl_K \to Cl_K$ is the $[L:K]$th power map. If $[L:K]$ is coprime to $|Cl_K|$ then this is an isomorphism. In particular, $J_{L/K}$ is injective and $N_{L/K}$ is surjective. □

By Theorem 1 and Theorem 4, the extensions $\mathbb{B}_k/\mathbb{B}_{k-1}$ satisfy the conditions of Proposition 6. We obtain inclusions and surjections

$$Cl_{\mathbb{Q}} = Cl_{\mathbb{B}_0} \underset{\twoheadleftarrow}{\hookrightarrow} Cl_{\mathbb{B}_1} \underset{\twoheadleftarrow}{\hookrightarrow} Cl_{\mathbb{B}_2} \underset{\twoheadleftarrow}{\hookrightarrow} \cdots .$$

1.3.4 Compatibility II

Lemma 7. *If L/K is Galois then the composition $J_{L/K} \circ N_{L/K} \colon Cl_L \to Cl_L$ is given by*

$$c \mapsto \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(c).$$

Proof. Let $\mathfrak{q}$ be a prime of L, let $\mathfrak{p}$ be the prime of K lying under $\mathfrak{q}$, and let $\mathfrak{q}_1, \ldots, \mathfrak{q}_g$ be the primes of L lying over $\mathfrak{p}$. Since $\mathrm{Gal}(L/K)$ acts transitively on the primes of L lying over $\mathfrak{p}$, we have

$$\prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\mathfrak{q}) = \mathfrak{q}_1^{n/g} \cdots \mathfrak{q}_g^{n/g} = (\mathfrak{q}_1^e \cdots \mathfrak{q}_g^e)^f = \mathcal{J}_{L/K}(\mathfrak{p}^f) = \mathcal{J}_{L/K}(\mathcal{N}_{L/K}(\mathfrak{q})).$$

The result follows from extending multiplicatively and passing to the quotient. □

Let σ generate $\mathrm{Gal}(\mathbb{B}_k/\mathbb{Q})$. Then σ gives a permutation of $Cl_{\mathbb{B}_k}$. Since $\sigma^{p^k} = 1$, we know that each cycle of this permutation has order a power of p. We can use Lemma 7 to say more.

Theorem 8. *If $Cl_{\mathbb{B}_{k-1}}$ is trivial then every nonidentity cycle of σ on $Cl_{\mathbb{B}_k}$ has order p^k.*

Proof. Let $c \in Cl_{\mathbb{B}_k}$ and suppose that $\sigma^{p^{k-1}}(c) = c$. By Lemma 7 and our assumption that $Cl_{\mathbb{B}_{k-1}}$ is trivial,

$$c^p = (c)\left(\sigma^{p^{k-1}}(c)\right)\left(\sigma^{2\cdot p^{k-1}}(c)\right) \cdots \left(\sigma^{(p-1)p^{k-1}}(c)\right) = J_{\mathbb{B}_k/\mathbb{B}_{k-1}}(N_{\mathbb{B}_k/\mathbb{B}_{k-1}}(c)) = J_{\mathbb{B}_k/\mathbb{B}_{k-1}}(1) = 1.$$

By Theorem 4, $c = 1$. Thus, if $c \neq 1$ then $\sigma^{p^{k-1}}(c) \neq c$. □

Theorem 8 can also be stated in terms of fixed-point-free automorphism groups. An action of a group G on a group H is said to be fixed-point-free if $g \cdot h = h$ implies that $g = 1$ or $h = 1$.

Corollary 9. *If $Cl_{\mathbb{B}_{k-1}}$ is trivial then the action of $\mathrm{Gal}(\mathbb{B}_k/\mathbb{Q})$ on $Cl_{\mathbb{B}_k}$ is fixed-point-free.*

1.4 The Hilbert Class Field

It is natural to consider the semidirect product $G = Cl_{\mathbb{B}_k} \rtimes \mathrm{Gal}(\mathbb{B}_k/\mathbb{Q})$. Corollary 9 can be rephrased as saying that if $Cl_{\mathbb{B}_{k-1}}$ is trivial then G is a "Frobenius group". Since $\mathrm{Gal}(\mathbb{B}_k/\mathbb{Q})$ is a quotient of G, one might wonder if G is a secretly isomorphic $\mathrm{Gal}(H/\mathbb{Q})$ for some number field H containing $\mathbb{B}_k$.

By class field theory, there exists a number field H (the Hilbert class field of $\mathbb{B}_k$) such that:

(a) H is Galois over $\mathbb{Q}$,

(b) $\mathbb{B}_k$ is contained in H,

(c) The extension $H/\mathbb{B}_k$ is unramified,

(d) The Galois group $\mathrm{Gal}(H/\mathbb{B}_k)$ is isomorphic to $Cl_{\mathbb{B}_k}$.

(e) The action of $\mathrm{Gal}(\mathbb{B}_k/\mathbb{Q})$ on $\mathrm{Gal}(H/\mathbb{B}_k)$ agrees with the action of $\mathrm{Gal}(\mathbb{B}_k/\mathbb{Q})$ on $Cl_{\mathbb{B}_k}$.

There is a short exact sequence of groups

$$1 \longrightarrow \mathrm{Gal}(H/\mathbb{B}_k) \longrightarrow \mathrm{Gal}(H/\mathbb{Q}) \xrightarrow{\pi} \mathrm{Gal}(\mathbb{B}_k/\mathbb{Q}) \longrightarrow 1$$

where $\mathrm{Gal}(H/\mathbb{B}_k) \cong Cl_{\mathbb{B}_k}$ and $\mathrm{Gal}(\mathbb{B}_k/\mathbb{Q}) \cong \mathbb{Z}/p^k\mathbb{Z}$. By Theorem 4, $\mathrm{Gal}(H/\mathbb{B}_k) \cong Cl_{\mathbb{B}_k}$ has order indivisible by p. Then p^k is the largest power of p dividing $\mathrm{Gal}(H/\mathbb{Q})$.

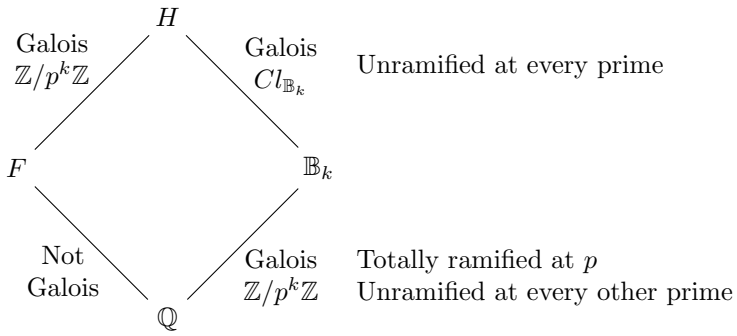
Lemma 10. *The above short exact sequence splits (in the semidirect product sense).*

Proof. As before, let σ generate $\mathrm{Gal}(\mathbb{B}_k/\mathbb{Q})$. Then $\sigma = \pi(\tau)$ for some $\tau \in \mathrm{Gal}(H/\mathbb{Q})$. In particular, τ has order divisible by p^k. Since p^k is the largest power of p dividing $\mathrm{Gal}(H/\mathbb{Q})$, τ has order $p^k m$ where $p \nmid m$. Then τ^m has order p^k. Furthermore, $\pi(\tau^m) = \sigma^m$ is a generator of $\mathrm{Gal}(\mathbb{B}_k/\mathbb{Q})$ since $p \nmid m$. Then $\sigma^m \mapsto \tau^m$ defines a right-inverse to π. □

Lemma 10 gives an isomorphism

$$\mathrm{Gal}(H/\mathbb{Q}) \cong \mathrm{Gal}(H/\mathbb{B}_k) \rtimes \mathrm{Gal}(\mathbb{B}_k/\mathbb{Q}) \cong Cl_{\mathbb{B}_k} \rtimes \mathrm{Gal}(\mathbb{B}_k/\mathbb{Q}) \cong G,$$

where the middle isomorphism implicitly uses (e). Let F denote the fixed field of a Sylow p-subgroup of $\mathrm{Gal}(H/\mathbb{Q})$. Then we have the diagram of fields



Note that $F/\mathbb{Q}$ is unramified at every prime other than p, but must be ramified at p since $F/\mathbb{Q}$ has no unramified extensions. Moreover, the ramification indices of p must be powers of p. However, $[F : \mathbb{Q}]$ is not divisible by p, so at least one prime of F lying over p is inert.

1.5 The Conjecture

I must confess that I've buried the lede. The following conjecture is wide open, but likely to be true.

Conjecture 11. *$\mathbb{B}_k$ has class number 1 for all $k \geq 0$ (and all primes p).*

It is important to keep in mind that we currently don't even know whether there are infinitely many number fields of class number 1. It is interesting to contrast Conjecture 11 with the conjecture that infinitely many real quadratic number fields have class number 1. One thing that makes the latter conjecture hard is that the real quadratic number fields of class number 1 are distributed unpredictably, so we don't know which specific real quadratic number fields to look at. In the case of Conjecture 11, however, we know exactly which number fields to look at, but we still can't prove it!

1.6 Explicit Computation

We will now use the notation $\mathbb{B}_{p,k}$. We will prove Conjecture 11 for $\mathbb{B}_{2,1}$, $\mathbb{B}_{3,1}$, and $\mathbb{B}_{2,2}$. In each of these cases, the field in question is the maximal real subfield of a cyclotomic field:

$$\begin{aligned}\mathbb{B}_{2,1} &= \mathbb{Q}(\zeta_8 + \zeta_8^{-1}),\\ \mathbb{B}_{3,1} &= \mathbb{Q}(\zeta_9 + \zeta_9^{-1}),\\ \mathbb{B}_{2,2} &= \mathbb{Q}(\zeta_{16} + \zeta_{16}^{-1}).\end{aligned}$$

In general, the maximal real subfield of $\mathbb{Q}(\zeta_n)$ is $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$, and its ring of integers is $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$.

- The minimal polynomial of $\zeta_8 + \zeta_8^{-1}$ is $x^2 - 2$. Its discriminant is 8.
- The minimal polynomial of $\zeta_9 + \zeta_9^{-1}$ is $x^3 - 3x + 1$. Its discriminant is 81.
- The minimal polynomial of $\zeta_{16} + \zeta_{16}^{-1}$ is $x^4 - 4x^2 + 2$. Its discriminant is 2048.

We can now compute the Minkowski bounds, using the fact that $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ has no complex embeddings.

- The Minkowski bound for $\mathbb{B}_{2,1}$ is $\sqrt{2}$, so $Cl_{\mathbb{B}_{2,1}}$ is automatically trivial.
- The Minkowski bound for $\mathbb{B}_{3,1}$ is 2. Thus, $Cl_{\mathbb{B}_{3,1}}$ is generated by the primes of $\mathbb{B}_{3,1}$ lying over 2. The polynomial $x^3 - 3x + 1$ is irreducible modulo 2, which shows that (2) is the only prime of $\mathbb{B}_{3,1}$ lying over 2.
- The Minkowski bound for $\mathbb{B}_{2,2}$ is $3\sqrt{2}$. Thus, $Cl_{\mathbb{B}_{2,2}}$ is generated by the primes lying over 2 and 3. The polynomial $x^4 - 4x^2 + 2$ is irreducible modulo 3, which shows that (3) is the only prime of $\mathbb{B}_{2,2}$ lying over 3. As for 2, note that $\alpha = \zeta_{16} + \zeta_{16}^{-1} = \sqrt{2 + \sqrt{2}}$. Then

  $$2 = ((\alpha^2 - 2)^2 - \alpha^2)^2 = (\alpha^2 - \alpha - 2)^2(\alpha^2 + \alpha - 2)^2.$$

  In fact, the ideals $(\alpha^2 - \alpha - 2)$ and $(\alpha^2 + \alpha - 2)$ are equal since

  $$(\alpha^2 - \alpha - 2)(-2\alpha^2 - 2\alpha + 3) = -2\alpha^4 + 9\alpha^2 + \alpha - 6 = \alpha^2 + \alpha - 2$$

  and

  $$(\alpha^2 + \alpha - 2)(-2\alpha^2 + 2\alpha + 3) = -2\alpha^4 + 9\alpha^2 - \alpha - 6 = \alpha^2 - \alpha - 2$$

  where

  $$(-2\alpha^2 - 2\alpha + 3)(-2\alpha^2 + 2\alpha + 3) = 4\alpha^4 - 16\alpha^2 + 9 = 1.$$

  This shows that $(\alpha^2 - \alpha - 2) = (\alpha^2 + \alpha - 2)$ is the only prime of $\mathbb{B}_{2,2}$ lying over 2.

This proves Conjecture 11 for $\mathbb{B}_{2,1}$, $\mathbb{B}_{3,1}$, and $\mathbb{B}_{2,2}$.