UNIVERSITÄT
DUISBURG
ESSEN

Open-Minded

University Duisburg-Essen

Faculty of Mathematics

Fermat's Last Theorem for regular primes

Master thesis by

Jan Paul Diekmann

First reviewer:	Prof. Dr. Jan Kohlhaase
Second reviewer:	Prof. Dr. Johannes Sprang
Submission deadline:	December 05, 2023

Contents

Acknowledgements

First and foremost, I would like to thank Professor Kohlhaase for introducing me to the subject and for his constant support. In particular, I would like to thank him for his numerous corrections and suggestions for improving the general exposition of my thesis. However, the term “constant support” does not only refer to the project of writing this thesis, but it also refers to the two Algebraic Number Theory courses, which I attended in winter term 2021/22 and in summer term 2022. Without his detailed explanations, I would probably not have received the necessary background knowledge for this thesis. Furthermore, I would like to give my thanks to Professor Sprang for agreeing to take time to read and review my thesis.

Moreover, I would like to thank Professor Hein, Xiaoyu Zhang, as well as Hind Souly, Hasan Hasan, Gregor Kremers, Mike Farniok and Florian Leptien for their help with the preparation of difficult exams, seminar talks or certain problems of this thesis. Someone else to whom I am thankful is Dietrich Lüerßen. He helped me to improve the style and language of this document and also checked that most of its contents are easy to understand.

I would also like to thank all my friends and relatives for being with me, because their good wishes and encouragements made it a lot easier for me to keep my study of mathematics going.

Finally, I want to express my profound gratitude to my parents for providing me with unfailing support and ongoing encouragement throughout my entire study and during the process of researching and writing this thesis. This accomplishment would not have been possible without them. Thank you.

Jan Diekmann

Gelsenkirchen, December 2023

1 Introduction

Pierre de Fermat, one of the greatest mathematicians of the 17th century, stated the assertion that for any $n > 2$ the equation $x^n + y^n = z^n$ has no solutions x, y, z in positive integers. Moreover, Fermat claimed that he had found a remarkable proof, for which the margin was too small. This assertion was proved by Andrew Wiles and Richard Taylor in 1993/94. It is known as "Fermat's Last Theorem" (since it was proved as the last one of Fermat's results).

Analogously to [2, page 1], we introduce the main object of interest: A prime number p is said to be regular if it does not divide the class number of the field $\mathbb{Q}(\zeta_p)$. A consequence of this property is that whenever for a fractional ideal $\mathfrak{a}$ in $\mathbb{Q}(\zeta_p)$, $\mathfrak{a}^p$ is principal, then $\mathfrak{a}$ is itself principal. The concept of a regular prime was introduced by Kummer. He proved the following result in 1847:

Theorem 1. *For a regular prime $p \geq 3$, the equation $x^p + y^p = z^p$ does not have a solution in positive integers x, y, z.*

Before Kummer's proof of this assertion, Fermat's Last Theorem was only known for prime exponents 3 (Euler), 5 (Dirichlet and Lagrange, independently) and 7 (Lamé). Fermat himself had proved "Fermat's Last Theorem" for exponent 4. After Kummer, Fermat's Last Theorem was known for the 21 odd primes below 100 except 19, 37 and 67 (cf. [2, page 1]).

In the second section of this document, some preliminary information about cyclotomic fields is given. It can be found in [2] and [5], where most of the content is taken from [2]. Some of the results are about general cyclotomic fields $\mathbb{Q}(\zeta_n)$, $n \geq 3$, but most of them deal with the field $\mathbb{Q}(\zeta_p)$, where $p \geq 3$ is a fixed prime number.

The goal of Section 3 is to give a precise elaboration of the proof of Theorem 1, which can be found in [2]. By means of contradiction, it is assumed that some fixed odd regular prime p and some positive integers x, y, z satisfy $x^p + y^p = z^p$. The proof is divided into the two cases of $p \nmid xyz$ and $p \mid xyz$, treated in Subsections 3.1 and 3.2, separately. The second of these cases turns out to be more complex than the first one, and in particular, it relies on the result that a unit of $\mathbb{Z}[\zeta_p]$ which is congruent to a rational integer mod p is a pth power of a unit in $\mathbb{Z}[\zeta_p]$. This fact is known as *Kummer's Lemma*. Here, it is taken from [5, Theorem 5.36, page 79]. This reference provides two proofs, of which we are going to treat the second one, [5, pages 80–81], which relies on class field theory.

Section 4 proves as much as possible of a theorem known as *Kummer's criterion*. It asserts that p divides the class number of $\mathbb{Q}(\zeta_p)$ if and only if it divides the numerator of the Bernoulli number B_j for $j = 2, 4, \ldots, p-3$, see [5, Remarks, page 6]. Therefore, Kummer's criterion is a simple answer to the question, whether a given prime $p \geq 3$ is regular or not, whereas determining the class number of $\mathbb{Q}(\zeta_p)$ is, in general, not an easy task. The main ideas for the proof of this theorem are taken from [5]. For some background information we occasionally refer to [1] or [4]. Generally, p is assumed to be a fixed odd prime. Also, we use the notations $h_p := h(\mathbb{Q}(\zeta_p))$ and $h_p^+ := h(\mathbb{Q}(\zeta_p + \zeta_p^{-1}))$, where h is the class number.

The first subsections of Section 4 treat important properties of characters of $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, the generalized Bernoulli numbers and p-adic L-functions, separately. After that, in Subsection 4.4, we prove that h_p^+ divides h_p. This fact allows us to define the *relative class number* of $\mathbb{Q}(\zeta_p)$ by $h_p^- := h_p/h_p^+$. It turns out that $p \mid h_p^-$ if and only if p divides the numerator of B_j for some $j = 2, 4, \ldots, p-3$. A consequence of this result is that there are infinitely many irregular primes (cf. Theorem 47).

Nevertheless, at this point, the proof of Kummer's criterion is not yet complete, since $p \mid h_p$ does not necessarily imply $p \mid h_p^-$. To fill this "gap" in the proof, we are going to prove the fact that $p \mid h_p^+$ implies $p \mid h_p^-$, see Subsections 4.5 and 4.6.

Notation and conventions

Unless otherwise stated, we fix some odd prime $p \geq 3$ and let ζ instead of ζ_p denote a primitive pth root of unity. Also in general, for any $n \in \mathbb{Z}_{>0}$, let μ_n be the group of nth roots of unity. Then we sometimes use $K := \mathbb{Q}(\zeta_p)$ and let $\mathfrak{o}_K$ be the ring of integers of K. We sometimes use the definitions $G := \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, $N := N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}$ and $\pi := 1 - \zeta_p$.

As in [5], we will abuse terminology and speak of the units of K if we really mean the elements of $\mathfrak{o}_K^\times$.

2 Basic properties of cyclotomic fields

We start with some basic facts about cyclotomic fields.

Lemma 2. (cf. [5, Theorem 2.6, page 11]) *Let $n \geq 3$ and let ζ_n be a primitive* nth *root of unity. $\mathbb{Z}[\zeta_n]$ is the ring of algebraic integers of $\mathbb{Q}(\zeta_n)$.*

Therefore, $\mathbb{Z}[\zeta_n]$ is a Dedekind domain (so we have unique factorization into prime ideals, etc.)

Proof. Omitted, see [5, page 11]. □

Lemma 3. (cf. [2, Lemma 1, page 1]) *In $\mathbb{Z}[\zeta]$, the numbers $1-\zeta$, $1-\zeta^2$, …, $1-\zeta^{p-1}$ are all associates and $1+\zeta$ is a unit. Also $p = u(1-\zeta)^{p-1}$ for some unit u and $(1-\zeta)$ is the only prime ideal in $\mathbb{Z}[\zeta]$ dividing (p).*

The following proof is taken from [2, page 1]. A few of its ideas are explained by results from [3] about ramification theory.

Proof. Let $K = \mathbb{Q}(\zeta)$, $N = N_{K/\mathbb{Q}}$ and $G = \mathrm{Gal}(K/\mathbb{Q})$. By Lemma 2,

$\mathbb{Z}[\zeta]$ is the ring of algebraic integers of $\mathbb{Q}(\zeta)$, so we write $\mathfrak{o}_K := \mathbb{Z}[\zeta]$. For any $i \in \{1, \ldots, p-1\}$, let $j \in \{1, \ldots, p-1\}$ such that $ij \equiv 1 \bmod p$. Then we obtain

$$\frac{1-\zeta}{1-\zeta^j} = \frac{1-\zeta^{ij}}{1-\zeta^j} = \sum_{l=0}^{i-1} (\zeta^j)^l \in \mathbb{Z}[\zeta] \qquad \text{and} \qquad \frac{1-\zeta^j}{1-\zeta} = \sum_{l=0}^{j-1} \zeta^l \in \mathbb{Z}[\zeta],$$

so the elements $1-\zeta$, $1-\zeta^2$, ..., $1-\zeta^{p-1}$ are all associates and the elements $(1-\zeta^j)/(1-\zeta)$ are all units in $\mathfrak{o}_K$. In particular,

$$1+\zeta = ((1+\zeta)/(1-\zeta))(1-\zeta) = (1-\zeta^2)/(1-\zeta) \in \mathfrak{o}_K^\times.$$

Then consider the following equation:

$$1 + X + \cdots + X^{p-1} = \prod_{j=1}^{p-1} (X - \zeta^j)$$

Setting $X = 1$ in this equation yields

$$p = \prod_{j=1}^{p-1} (1-\zeta^j) = \prod_{j=1}^{p-1} \frac{1-\zeta^j}{1-\zeta}(1-\zeta) = u(1-\zeta)^{p-1},$$

where we let $u = \prod_{j=1}^{p-1}((1-\zeta^j)/(1-\zeta)) \in \mathfrak{o}_K^\times$. Furthermore, it follows that

$$N(1-\zeta) = \prod_{\sigma \in G} \sigma(1-\zeta) = \prod_{j=1}^{p-1} (1-\zeta^j) = p.$$

If $\mathfrak{N}$ denotes the ideal norm then $\mathfrak{N}((1-\zeta)) = (N(1-\zeta)) = (p)$. Since $\mathfrak{N}$ is multiplicative and $(p) \subseteq \mathbb{Z}$ is a prime ideal it follows that so is $(1-\zeta) \subseteq \mathfrak{o}_K$. This completes the proof of Lemma 3. □

The following lemma and its proof are taken from [3, proof of Theorem

3.29 (ii), step 1, pages 86–87].

Lemma 4. *For a number field K with ring of integers $\mathfrak{o}_K$, we consider the group homomorphism*

$$\lambda : K \to \mathbb{R},\ x \mapsto (\log(|x|_v))_{v|\infty},$$

where v runs through all archimedean places of K. Then $\ker(\lambda|_{\mathfrak{o}_K^\times}) = \mu(K)$, *where $\mu(K)$ is the set of roots of unity in K.*

Proof. Clearly, $\mu(K) \subseteq \ker(\lambda|_{\mathfrak{o}_K^\times})$, since for any $\zeta \in \mu(K)$ there is some $0 \neq r \in \mathbb{Z}$ such that for all $\sigma \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$, $\sigma(\zeta^r) = \sigma(1) = 1$. That means we obtain $|\zeta|_v^r = |\zeta^r|_v = 1$ for all $v|\infty$ and therefore $|\zeta|_v = 1$ for all $v|\infty$. Hence we get $\zeta \in \ker(\lambda|_{\mathfrak{o}_K^\times})$. To show the reverse inclusion, let $n = [K : \mathbb{Q}]$ and $x \in \ker(\lambda|_{\mathfrak{o}_K^\times})$. For all $\sigma \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$, we have $|\sigma(x)| = 1$. Thus the coefficients of the minimal polynomial of x over $\mathbb{Q}$ are integers bounded by $[-n, n]$. Since $x \in \ker(\lambda|_{\mathfrak{o}_K^\times})$ was arbitrary, this implies that the set of minimal polynomials over $\mathbb{Q}$ of elements of $\ker(\lambda|_{\mathfrak{o}_K^\times})$ is finite. Hence the set of roots of all these polynomials is finite. From this, it follows that $\ker(\lambda|_{\mathfrak{o}_K^\times})$ is a finite subgroup of $K^\times$, hence is cyclic. Thus $\ker(\lambda|_{\mathfrak{o}_K^\times}) \subseteq \mu(K)$. This completes the proof. □

Corollary 5. *For any $u \in \mathbb{Z}[\zeta]^\times$, $u/\overline{u}$ is a root of unity, where $\overline{u}$ denotes the complex conjugation of u.*

Proof. The complex conjugation is the $\mathbb{Q}$-automorphism of $\mathbb{Q}(\zeta)$ defined by $\zeta \mapsto \zeta^{-1}$. Let $u \in \mathbb{Z}[\zeta]^\times$ be arbitrary. Since $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is abelian, $\sigma(\overline{u}) = \overline{\sigma(u)}$ for all $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. Thus $|\sigma(u/\overline{u})|^2 = (\sigma(u)/\overline{\sigma(u)})(\overline{\sigma(u)}/\sigma(u)) = 1$ for all $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, so by applying Lemma 4 to $K = \mathbb{Q}(\zeta)$ and $\mathfrak{o}_K = \mathbb{Z}[\zeta]$, $u/\overline{u}$ is a root of unity. □

Lemma 6. *Let W denote the group of roots of unity in $\mathbb{Q}(\zeta_p)$. Then $W = \mu_{2p}$, where μ_{2p} is the group of $(2p)$th roots of unity.*

Proof. Since $-\zeta_p \in \mathbb{Q}(\zeta_p)$ is a $(2p)$th root of unity, we have $\mu_{2p} \subseteq W$.
To show the reverse inclusion, note that W is finite cyclic (cf. [3] Theorem 3.29 (i), page 86). It follows that $W = \mu_m$ for some natural number m. Since $\mu_{2p} \subseteq \mu_m$, $2p|m$. Thus there are $a, b \in \mathbb{Z}_{>0}$ with $m = 2^b p^a n$, $(n, 2) = 1 = (n, p)$. Now $\mathbb{Q}(\zeta_m)$ is a subfield of $\mathbb{Q}(\zeta_p)$, hence $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] \leq p - 1$. But then $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \varphi(m) = 2^{b-1} p^{a-1}(p-1)\varphi(n) \leq p - 1$, so $a = b = 1$ and, since $(n, 2) = 1$, also $n = 1$. That means $m = 2p$, so $\mu_m \subseteq \mu_{2p}$. Altogether, $W = \mu_m = \mu_{2p}$, as claimed. □

At this point, we change our notation of primitive pth roots of unity back to ζ.

Definition 7. (cf. [5, page 38]) *Let K be a number field. A subfield of K is called totally real if all of its embeddings into $\mathbb{C}$ have image in $\mathbb{R}$ and totally imaginary if none of its complex embeddings have image in $\mathbb{R}$. Moreover, for any field $K \subseteq \mathbb{C}$, the maximal totally real subfield of K is denoted by K^+.*

Lemma 8. *The maximal totally real subfield of $\mathbb{Q}(\zeta)$ is $\mathbb{Q}(\zeta)^+ = \mathbb{Q}(\zeta + \zeta^{-1})$. In particular, $\mathbb{Q}(\zeta + \zeta^{-1})$ is the set of all $x \in \mathbb{Q}(\zeta)$ with $\overline{x} = x$.*

Proof. On the one hand, $f(X) := X^2 - (\zeta + \zeta^{-1})X + 1 \in \mathbb{Q}(\zeta + \zeta^{-1})[X]$ satisfies $f(\zeta) = 0$, so $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})] \leq 2$. On the other hand, $\zeta \notin \mathbb{R}$ and $\mathbb{Q}(\zeta + \zeta^{-1}) \subseteq \mathbb{R}$ for any embedding $\mathbb{Q}(\zeta) \hookrightarrow \mathbb{C}$, so $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})] \geq 2$. Thus $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})] = 2$ and f is the minimal polynomial of ζ over $\mathbb{Q}(\zeta + \zeta^{-1})$. We have

$$\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta + \zeta^{-1})) = \{(\zeta \mapsto \zeta^i) | i = \pm 1\} \cong \{\pm 1\}.$$

Since this is a normal subgroup of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, the extension $\mathbb{Q}(\zeta+\zeta^{-1})/\mathbb{Q}$ is normal, hence Galois, and satisfies

$$\begin{aligned}\mathrm{Gal}(\mathbb{Q}(\zeta+\zeta^{-1})/\mathbb{Q}) &\cong \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})/\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta+\zeta^{-1})) \\ = \{(\zeta \mapsto \zeta^i) | 1 \leq i \leq p-1\}/\{(\zeta \mapsto \zeta^i) | i = \pm 1\} &\cong (\mathbb{Z}/p\mathbb{Z})^\times/\{\pm 1\}.\end{aligned}$$

That is, the elements of $\mathrm{Gal}(\mathbb{Q}(\zeta+\zeta^{-1})/\mathbb{Q})$ are given by the restrictions of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ to $\mathbb{Q}(\zeta+\zeta^{-1})$. In particular, for each $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta+\zeta^{-1})/\mathbb{Q})$, there is an $i \in \{1,\ldots,p-1\}$ such that $\sigma(\zeta+\zeta^{-1}) = \zeta^i + \zeta^{-i} \in \mathbb{R}$. Thus $\mathbb{Q}(\zeta+\zeta^{-1})$ is a totally real subfield of $\mathbb{Q}(\zeta)$. Since $\mathbb{Q}(\zeta)$ itself is not totally real, $\mathbb{Q}(\zeta+\zeta^{-1})$ is a maximal totally real subfield of $\mathbb{Q}(\zeta)$. Note that maximal totally real subfields are unique because totally real subfields are stable under compositum.

To prove the second assertion, note that we obviously have $\mathbb{Q}(\zeta+\zeta^{-1}) \subseteq \mathbb{Q}(\zeta) \cap \mathbb{R}$. To prove the reverse inclusion, let $x \in \mathbb{Q}(\zeta)$ with $\overline{x} = x$ be arbitrary. Write $x = \sum_{j=0}^{p-2} a_j \zeta^j$ for suitable $a_j \in \mathbb{Q}$. Since $x = \overline{x} = \sum_{j=0}^{p-2} a_j \zeta^{-j}$, we get

$$x = \frac{1}{2}(\sum_{j=0}^{p-2} a_j \zeta^j + \sum_{j=0}^{p-2} a_j \zeta^{-j}).$$

Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ be arbitrary and let $i \in \{1,\ldots,p-1\}$ such that $\sigma(\zeta) = \zeta^i$. Then we obtain

$$\sigma(x) = \sigma(\frac{1}{2}(\sum_{j=0}^{p-2} a_j \zeta^j + \sum_{j=0}^{p-2} a_j \zeta^{-j})) = \frac{1}{2}(\sum_{j=0}^{p-2} a_j \zeta^{ij} + \sum_{j=0}^{p-2} a_j \zeta^{-ij}) \in \mathbb{R},$$

so $x \in \mathbb{Q}(\zeta)^+ = \mathbb{Q}(\zeta+\zeta^{-1})$. Therefore, $\mathbb{Q}(\zeta+\zeta^{-1})$ is in fact the set of all all $x \in \mathbb{Q}(\zeta)$ with $\overline{x} = x$.

This completes the proof. □

Lemma 9. (cf. [2, page 3]) *There is an isomorphism of rings*

$$(\mathbb{Z}/(p))[X]/(X-1)^{p-1} \cong \mathbb{Z}[\zeta]/(p).$$

In $\mathbb{Z}[\zeta]/(p)$, the powers $1, \zeta, \zeta^2, \ldots, \zeta^{p-2}$ are a basis over $\mathbb{Z}/(p)$.

Proof. Let $\phi : \mathbb{Z}[X] \to \mathbb{Z}[\zeta]$, $f(X) \mapsto f(\zeta)$, be the canonical ring homomorphism. It is surjective. The kernel of ϕ is the ideal generated by $\Phi_p(X) := X^{p-1} + \cdots + X + 1$, so we have an isomorphism $\overline{\phi} : \mathbb{Z}[X]/(\Phi_p(X)) \xrightarrow{\sim} \mathbb{Z}[\zeta]$, $\overline{f} \mapsto f(\zeta)$. Let $\pi : \mathbb{Z}[\zeta] \to \mathbb{Z}[\zeta]/(p)$ be the canonical projection. It induces a ring isomorphism $\mathbb{Z}[X]/(p, \Phi_p(X)) \cong \mathbb{Z}[\zeta]/(p)$.
There are canonical ring isomorphisms

$$\mathbb{Z}[X]/(p, \Phi_p(X)) \cong (\mathbb{Z}/(p))[X]/(\Phi_p(X))$$

and

$$(\mathbb{Z}/(p))[X]/(\Phi_p(X)) = (\mathbb{Z}/(p))[X]/(X-1)^{p-1}.$$

The latter one comes from the following equation valid in $(\mathbb{Z}/(p))[X]$:

$$\Phi_p(X) = X^{p-1} + \cdots + X + 1 = \frac{X^p - 1}{X - 1} = \frac{(X-1)^p}{X-1} = (X-1)^{p-1}.$$

Altogether, we obtain an isomorphism $(\mathbb{Z}/(p))[X]/(X-1)^{p-1} \cong \mathbb{Z}[\zeta]/(p)$ sending $f(X) + (p, (X-1)^{p-1})$ to $f(\zeta) + p\mathbb{Z}[\zeta]$. Since $1, X, \ldots, X^{p-2}$ is a basis of $(\mathbb{Z}/(p))[X]/(X-1)^{p-1}$ over $\mathbb{Z}/(p)$, the powers $1, \zeta, \ldots, \zeta^{p-2}$ are a basis in $\mathbb{Z}[\zeta]/(p)$ over $\mathbb{Z}/(p)$. □

Lemma 10. (cf. [5, Proposition 1.5, page 3]) *Let ε be a unit of $\mathbb{Z}[\zeta]$. Then there exist $\varepsilon_1 \in \mathbb{Q}(\zeta + \zeta^{-1})$ and $r \in \mathbb{Z}$ such that $\varepsilon = \zeta^r \varepsilon_1$.*

Proof. The main ideas are taken from [5, page 4]. From Corollary 5, we know that $\varepsilon/\overline{\varepsilon}$ is a root of unity in $\mathbb{Q}(\zeta)$, so $\varepsilon/\overline{\varepsilon} = \pm\zeta^a$ for some $a \in \mathbb{Z}$, by

Lemma 6.

Suppose first that $\varepsilon/\overline{\varepsilon} = -\zeta^a$. We choose $b_0, b_1, \dots, b_{p-2} \in \mathbb{Z}$ such that $\varepsilon = b_0 + b_1\zeta + \cdots + b_{p-2}\zeta^{p-2}$. Note that $1, \zeta, \dots, \zeta^{p-2}$ generate $\mathbb{Z}[\zeta]$ as a $\mathbb{Z}$-module, since $\zeta^{p-1} = -\sum_{i=0}^{p-2} \zeta^i$. We claim that $\varepsilon \equiv b_0 + b_1 + \cdots + b_{p-2} \bmod (1-\zeta)$. To see this, note that for $i = 1, 2, \dots, p-1$, $(\zeta^i - 1)$ is associated to $(1-\zeta)$, see Lemma 3. This implies that

$$\varepsilon = \sum_{i=0}^{p-2} b_i\zeta^i = \sum_{i=0}^{p-2} b_i + \sum_{i=0}^{p-2}(\zeta^i - 1)b_i \equiv \sum_{i=0}^{p-2} b_i \bmod (1-\zeta).$$

Similarly, $\overline{\varepsilon} \equiv \sum_{i=0}^{p-2} b_i \bmod (1-\zeta)$, so altogether we obtain $\overline{\varepsilon} \equiv \varepsilon = -\zeta^a\overline{\varepsilon} = (1-\zeta^a)\overline{\varepsilon} - \overline{\varepsilon} \equiv -\overline{\varepsilon} \bmod (1-\zeta)$ and then $2\overline{\varepsilon} \equiv 0 \bmod (1-\zeta)$. But $2 \notin (1-\zeta)$, since otherwise we would get $1+\zeta = 2-(1-\zeta) \in (1-\zeta)$, contrary to the fact that $1+\zeta \in \mathbb{Z}[\zeta]^\times$, and that $(1-\zeta)$ is a prime ideal in $\mathbb{Z}[\zeta]$ (see Lemma 3). Thus $\overline{\varepsilon} \in (1-\zeta)$, again since $(1-\zeta)$ is a prime ideal in $\mathbb{Z}[\zeta]$. But this is a contradiction to $\overline{\varepsilon} \in \mathbb{Z}[\zeta]^\times$, and therefore the assumption $\varepsilon/\overline{\varepsilon} = -\zeta^a$ is not true. So it remains the case $\varepsilon/\overline{\varepsilon} = \zeta^a$. Choose $r \in \mathbb{Z}$ with $2r \equiv a \bmod p$ and set $\varepsilon_1 = \zeta^{-r}\varepsilon$. Then $\varepsilon = \varepsilon_1\zeta^r$ and $\overline{\varepsilon_1} = \zeta^r\overline{\varepsilon} = \zeta^r\zeta^{-a}\varepsilon = \zeta^{-r}\varepsilon = \varepsilon_1$. This completes the proof of Lemma 10. □

Lemma 11. (cf. [5, Proposition 2.16, page 16]) $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$ *is the ring of integers of* $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$.

Proof. Omitted, see [5, pages 16–17]. □

3 Proof of Fermat's Last Theorem for regular primes $p \geq 3$

Unless stated otherwise, this proof uses the ideas of [2]. We assume there are a regular prime $p \geq 3$ and some positive integers x, y, z with $x^p + y^p = z^p$.

Without loss of generality, let x, y, z be relatively prime. As already said, the proof is divided into two cases, based on whether the proposed solution (x, y, z) in pairwise relatively prime integers has p not dividing x, y or z or p dividing (exactly) one of them.

3.1 Case I: $p \nmid xyz$

In $\mathbb{Z}[\zeta]$, factor Fermat's equation as

$$z^p = x^p + y^p = \prod_{j=0}^{p-1}(x + \zeta^j y). \tag{1}$$

Let us show the factors on the right generate relatively prime ideals. For $0 \le j < j' \le p - 1$, a common ideal factor $\mathfrak{d}$ of $(x + \zeta^j y)$ and $(x + \zeta^{j'} y)$ must be a factor of the difference

$$x + \zeta^j y - x - \zeta^{j'} y = \zeta^j y(1 - \zeta^{j'-j}) = vy(1 - \zeta),$$

for some unit v. The last equality follows from Lemma 3, since it implies $v = \zeta^j(1 - \zeta^{j'-j})/(1 - \zeta) \in \mathbb{Z}[\zeta]^\times$. Since $y(1 - \zeta)$ divides yp (using Lemma 3), we have $\mathfrak{d} \mid (yp)$. We also know by (1) that $\mathfrak{d}$ divides $(z)^p$. Since yp and z^p are relatively prime integers, we conclude that $\mathfrak{d}$ is the unit ideal, so the ideals $(x + \zeta^j y)$ are relatively prime. The product of these ideals is $(z)^p$, so unique ideal factorization implies each factor is a pth power. Taking $j = 1$,

$$(x + \zeta y) = \mathfrak{a}^p,$$

for some ideal $\mathfrak{a}$. Therefore, $\mathfrak{a}^p$ is trivial in the class group, so $\mathfrak{a}$ is principal because p is regular, say $\mathfrak{a} = (t)$ with $t \in \mathbb{Z}[\zeta]$. Thus

$$x + \zeta y = ut^p$$

for some unit u in $\mathbb{Z}[\zeta]$. Writing $t = b_0 + b_1\zeta + \cdots + b_{p-2}\zeta^{p-2}$, with b_j in $\mathbb{Z}$, we get (using $\zeta^p = 1$)

$$t^p \equiv b_0^p + b_1^p + \cdots + b_{p-2}^p \equiv b_0 + b_1 + \cdots + b_{p-2} \bmod p\mathbb{Z}[\zeta]. \qquad (2)$$

Thus $t^p \equiv \overline{t}^p \bmod p\mathbb{Z}[\zeta]$. Since $u \in \mathbb{Z}[\zeta]^\times$, Corollary 5 implies that $u/\overline{u}$ is a root of unity, so by Lemma 6, $u/\overline{u} = \pm\zeta^j$ for some $0 \le j \le p-1$. If $u/\overline{u} = \zeta^j$, then

$$\begin{aligned} x + \zeta y &= ut^p \\ &= \zeta^j \overline{u} t^p \\ &\equiv \zeta^j \overline{u}\overline{t}^p \bmod p\mathbb{Z}[\zeta] \\ &\equiv \zeta^j (x + \overline{\zeta} y) \bmod p\mathbb{Z}[\zeta]. \end{aligned}$$

Thus

$$\frac{u}{\overline{u}} = \zeta^j \Rightarrow x + y\zeta - y\zeta^{j-1} - x\zeta^j \equiv 0 \bmod p\mathbb{Z}[\zeta]. \qquad (3)$$

Similarly,

$$\frac{u}{\overline{u}} = -\zeta^j \Rightarrow x + y\zeta + y\zeta^{j-1} + x\zeta^j \equiv 0 \bmod p\mathbb{Z}[\zeta]. \qquad (4)$$

We want to show neither of these congruences can hold when $0 \le j \le p-1$ and x and y are integers prime to p.

Note that $1, \zeta, \ldots, \zeta^{p-2} \bmod p\mathbb{Z}[\zeta]$ were shown to be linearly independent over $\mathbb{Z}/(p)$ in Lemma 9.

Since x and y are nonzero mod p, we find that both (3) and (4) lead to a contradiction if j is such that $1, \zeta, \zeta^{j-1}$ and ζ^j are pairwise distinct elements. In other words, (3) and (4) lead to a contradiction if $3 \le j \le p-2$. In order to treat the remaining cases of $j \in \{0, 1, 2, p-1\}$, note that we may take $p \geq 5$, because for $p = 3$ and x, y, z prime to p, the congruence $x^3 + y^3 \equiv z^3 \bmod 9$ fails, since for all $a \in (\mathbb{Z}/9\mathbb{Z})^\times$, we have $\in a^3 \in \{\pm 1\}$. Therefore, let $p \geq 5$. If $j = p - 1$ then (3) becomes

$$\begin{aligned} 0 &\equiv x(1 - \zeta^{p-1}) + y(\zeta - \zeta^{p-2}) \\ &= 2x + (x + y)\zeta + x(\zeta^2 + \cdots + \zeta^{p-3}) + (x - y)\zeta^{p-2} \bmod p\mathbb{Z}[\zeta], \end{aligned}$$

which contradicts the linear independence of $1, \zeta, \ldots, \zeta^{p-2} \bmod p\mathbb{Z}[\zeta]$ over $\mathbb{Z}/(p)$, where the last equality is due to $-\zeta^{p-1} = 1 + \zeta + \cdots + \zeta^{p-2}$. The case of (4) and $j = p - 1$ analogously leads to a contradiction. If $j = 0$ then (3) becomes $y(\zeta - \zeta^{-1}) \equiv 0 \bmod p\mathbb{Z}[\zeta]$. Since y is not divisible by p, this relation is equivalent to $\zeta^2 + 1 \equiv 0 \bmod p\mathbb{Z}[\zeta]$, again a contradiction to the linear independence of $1, \zeta, \ldots, \zeta^{p-2}$ over $\mathbb{Z}/(p)$ since $p \geq 5$. Similarly, (4) with $j = 0$ implies $2x\zeta + y\zeta^2 + y \equiv 0 \bmod p\mathbb{Z}[\zeta]$, so again we get a contradiction. Setting $j = 2$ in (3) or (4) leads to contradictions of linear independence as well. ($1 - x\zeta^2 \equiv 0 \bmod p\mathbb{Z}[\zeta]$ in (3) and $x + 2y\zeta + x\zeta^2 \equiv 0 \bmod p\mathbb{Z}[\zeta]$ in (4)). We now are left with the case $j = 1$. In the case of (4), $j = 1$ implies $(x + y)(1 + \zeta) \equiv 0 \bmod p\mathbb{Z}[\zeta]$, so $x + y \equiv 0 \bmod p\mathbb{Z}$, since by Lemma 3, $1 + \zeta \in \mathbb{Z}[\zeta]^\times$. Thus $z^p = x^p + y^p \equiv (x + y)^p \equiv 0 \bmod p\mathbb{Z}$, so p divides z. That violates the condition $p \mid xyz$, so we get a contradiction. The only case remaining is $j = 1$ in (3). To repeat the results from above, we have shown that if $x^p + y^p = z^p$ and x, y, z are not divisible by p, then $x + \zeta y = ut^p$, where $u/\overline{u} = \zeta$. Setting $j = 1$ in (3) yields

$$x(1 - \zeta) + y(\zeta - 1) = 0 \bmod p\mathbb{Z}[\zeta].$$

Writing $p = u(1 - \zeta)^{p-1}$, this implies

$$x \equiv y \bmod (1 - \zeta)^{p-2}.$$

Since $p-2 \geq 1$ and x and y are in $\mathbb{Z}$, this forces $x \equiv y \bmod p\mathbb{Z}$ because $\mathbb{Z} \cap (1-\zeta^{p-2})\mathbb{Z}[\zeta] \subseteq \mathbb{Z} \cap (1-\zeta)\mathbb{Z}[\zeta] = p\mathbb{Z}$ by Lemma 3. Running through the proof with y and $-z$ interchanged, we get $x \equiv -z \bmod p\mathbb{Z}$, so

$$0 = x^p + y^p - z^p \equiv 3x^p \bmod p\mathbb{Z}.$$

Since $p \neq 3$ and x is prime to p, we have a contradiction. This completes the proof of Case I for p a regular prime.

3.2 Case II: $p \mid xyz$

Since x, y, z are assumed to be relatively prime, p does not divide each of x, y, z. Since p is odd, we may write the equation in the symmetric form $x^p + y^p + z^p = 0$. If p divides two of x, y, z, say x and y, then it divides the third, z, as well: $0 = x^p + y^p + z^p \equiv x + y + z \equiv z \bmod p$. So removing the highest common factor of p from the three numbers, we can assume p divides exactly one of the numbers, say $p \mid z$. Writing $z = p^r z_0$, with z_0 prime to p and $r \geq 1$, Fermat's equation reads

$$x^p + y^p + w(1-\zeta)^{rp(p-1)} z_0^p = 0, \tag{5}$$

for some $w \in \mathbb{Z}[\zeta]^\times$ and p not dividing xyz_0.

Since $(1-\zeta)$ is the only prime above p in $\mathbb{Z}[\zeta]$ (cf. Lemma 3) and x, y, z_0 are in $\mathbb{Z}$, saying xyz_0 is not divisible by p is equivalent to saying xyz_0 is not divisible by $(1-\zeta)$ in $\mathbb{Z}[\zeta]$. Instead of (5), we are going to prove a stronger result.

Theorem 12. (cf. [2, Theorem 2, page 4]) *For a regular prime $p \geq 3$, there do not exist α, β, γ in $\mathbb{Z}[\zeta]$, all nonzero, such that*

$$\alpha^p + \beta^p + \varepsilon(1-\zeta)^{pn}\gamma^p = 0, \tag{6}$$

where $\varepsilon \in \mathbb{Z}[\zeta]^{\times}$, $n \geq 1$, and $(1-\zeta)$ does not divide $\alpha\beta\gamma$.

In particular, (5) and Theorem 12 show Fermat's Last Theorem for exponent p has no solution in Case II when p is regular.

Proof. By (6), we have the ideal equation

$$\prod_{j=0}^{p-1}(\alpha + \zeta^j \beta) = (1-\zeta)^{pn}(\gamma)^p. \tag{7}$$

Since γ is nonzero, the left side is nonzero, so $\alpha+\beta$, $\alpha+\zeta\beta, \ldots, \alpha+\zeta^{p-1}\beta$ are all nonzero. Unlike Case I, the factors on the left side of the last equation will not be relatively prime ideals. Because in Case I, where we showed that such a decomposition cannot have common prime factors, the argument that yp and z^p are relatively prime is used. But this argument can not be applied here, as we have assumed $p \mid z$. Instead, we are going to argue that all these factors are divisible by $(1-\zeta)$ and moreover, that at least one of them is divisible by $(1-\zeta)^2$. Therefore, we will work with congruences mod $(1-\zeta)$ and mod $(1-\zeta)^2$. We have $\mathbb{Z}/(p) \cong \mathbb{Z}[\zeta]/(1-\zeta)$ and $\mathbb{Z}/(p)[X]/(X-1)^2 \cong \mathbb{Z}[\zeta]/(1-\zeta)^2$ by Lemma 9. In particular, this implies that the ideal $(1-\zeta) \subseteq \mathbb{Z}[\zeta]/(1-\zeta)^2$ has cardinality p. This is true because a congruence of any $\delta(1-\zeta)$ is characterized by δ modulo $(1-\zeta)$ (and because of $|(\mathbb{Z}[\zeta]/(1-\zeta))| = p$). Also by this characterization, we find that among the p pairwise distinct multiples of $1-\zeta$ in $\mathbb{Z}[\zeta]/(1-\zeta)^2$ there is precisely one equal to zero. By Lemma 3, $\alpha+\zeta^j\beta \equiv \alpha+\beta \bmod (1-\zeta)$ for all $j \in \{0, \ldots, p-1\}$, so if $(1-\zeta)$ divides one of the factors $(\alpha+\zeta^j\beta)$ (in (7)), then it divides all of these factors. In order to show the above claim, it remains to see that for at least one $j_0 \in \{0, \ldots, p-1\}$ we have $a + \zeta^{j_0}\beta \equiv 0 \bmod (1-\zeta)^2$. We proceed by means of contradiction, i.e. we assume that the p factors on the left hand side of (7) are all nonzero multiples of $(1-\zeta)$ modulo $(1-\zeta)^2$. However, there are only $p-1$ pairwise distinct nonzero elements in the ideal $(1-\zeta) \subseteq \mathbb{Z}[\zeta]/(1-\zeta)^2$, so we must have

$$\alpha + \zeta^j \beta \equiv \alpha + \zeta^{j'} \beta \bmod (1-\zeta)^2$$

for some $0 \leq j < j' \leq p-1$. That means $(1-\zeta^{j'-j})\beta \equiv 0 \bmod (1-\zeta)^2$. Since $1-\zeta^{j'-j}$ is associated to $1-\zeta$, this congruence relation implies that $(1-\zeta) \mid \beta$. But this is a contradiction to the hypothesis of the theorem. So in fact, for some $j_0 \in \{0, 1, \ldots, p-1\}$ we have $\alpha + \zeta^{j_0}\beta \equiv 0 \bmod (1-\zeta)^2$. Moreover, this forces n to be strictly greater than 1. We proceed by claiming that the above j_0 is unique. For if we assumed there were two distinct $j_0, j_0' \in \{0, 1, \ldots, p-1\}$ such that $0 \equiv \alpha + \zeta^{j_0}\beta \equiv \alpha + \zeta^{j_0'}\beta$, then we would run into the same contradiction as in the last paragraph: $(1-\zeta^{j_0'-j_0})\beta \equiv 0 \bmod (1-\zeta)^2$ and then $(1-\zeta) \mid \beta$. Replacing β with $\zeta^{j_0}\beta$ in (7), we may assume that $j_0 = 0$, so $\alpha + \beta \equiv 0 \bmod (1-\zeta)^2$ and $(\alpha + \zeta^j\beta) \not\equiv 0 \bmod (1-\zeta)^2$ for all $j \in \{1, \ldots, p-1\}$. We now claim that for any two factors on the left hand side of (7), their greatest common divisor in the sense of ideals is equal to $\mathfrak{d}(1-\zeta)$, where $\mathfrak{d} = (\alpha, \beta)$. To prove this, let $\alpha + \zeta^j\beta$ and $\alpha + \zeta^{j'}\beta$ be two distinct factors in (7). Since at least one of $\alpha + \zeta^j\beta$ and $\alpha + \zeta^{j'}\beta$ is divisible by $1-\zeta$ only once, we may assume that $\mathfrak{d}$ and $1-\zeta$ are relatively prime. As a common factor of these two, $\mathfrak{d}$ is also a factor of $\zeta^{-j}(\alpha + \zeta^j\beta) = \zeta^{-j}\alpha + \beta$ and $\zeta^{-j'}(\alpha + \zeta^{j'}\beta) = \zeta^{-j'}\alpha + \beta$, as well as of the differences $(\alpha + \zeta^j\beta) - (\alpha + \zeta^{j'}\beta) = \zeta^j(1-\zeta^{j'-j})\beta$ and $(\zeta^{-j}\alpha + \beta) - (\zeta^{-j'}\alpha + \beta) = \zeta^{-j}(1-\zeta^{-j'+j})\alpha$. Since $1-\zeta^{j'-j}$ and $1-\zeta^{-j'+j}$ are associated to $1-\zeta$, $\mathfrak{d}$ is a common divisor of α and β, so $\mathfrak{d}$ divides (α, β). Conversely, (α, β) is a common factor of all the factors on the left hand side of (7), and by the hypothesis of the theorem, (α, β) is relatively prime to $1-\zeta$, so also (α, β) divides $\mathfrak{d}$. Altogether, we find that the greatest common divisor of two factors of the decomposition in (7) is equal to $\mathfrak{d}(1-\zeta)$ with $\mathfrak{d} = (\alpha, \beta)$. That means that the complementary divisor of $\mathfrak{d}(1-\zeta)$ in $(\alpha + \zeta^j\beta)$ does not divide any of the other factors. Since any prime ideal appears p times in the decomposition on the right hand side of (7), the complementary divisor is of the form $\mathfrak{c}_j^p$ by the unique prime factorization for ideals. Thus, $(\alpha + \zeta^j\beta) = \mathfrak{d}(1-\zeta)\mathfrak{c}_j^p$ for $1 \leq j \leq p-1$ and $(\alpha + \beta) = \mathfrak{d}(1-\zeta)^{np-(p-1)}\mathfrak{c}_0^p$

because of (7). From this description we find that for each $1 \leq j \leq p-1$, $\mathfrak{c}_j^p \mathfrak{c}_0^{-p}$ is a principal fractional ideal:

$$\begin{aligned}\mathfrak{c}_j^p \mathfrak{c}_0^{-p} &= (\alpha + \zeta^j \beta)\mathfrak{d}^{-1}(1-\zeta)^{-1}(\alpha+\beta)^{-1}\mathfrak{d}(1-\zeta)^{np-(p-1)} \\ &= (\frac{\alpha+\zeta^j\beta}{\alpha+\beta}(1-\zeta)^{p(n-1)}). \qquad (8)\end{aligned}$$

Since p is regular, $\mathfrak{c}_j \mathfrak{c}_0^{-1}$ is a principal fractional ideal. That means that some $t_j \in \mathbb{Q}(\zeta)^\times$ satisfies $\mathfrak{c}_j \mathfrak{c}_0^{-1} = t_j \mathbb{Z}[\zeta]$. Note that t_j is prime to $1-\zeta$ because so are $\mathfrak{c}_\mathrm{j}$ and $\mathfrak{c}_0$. Plugging this into (8), we obtain the equation of ideals

$$(t_j)^p = (\alpha + \zeta^j \beta)\mathfrak{d}^{-1}(1-\zeta)^{-1}(\alpha+\beta)^{-1}\mathfrak{d}(1-\zeta)^{np-(p-1)},$$

and therefore

$$(\alpha+\zeta^j\beta)(\alpha+\beta)^{-1} = (t_j)^p(1-\zeta)^{-p(n-1)}.$$

For the generators this can be written as an equation of elements

$$\frac{\alpha+\zeta^j\beta}{\alpha+\beta} = \frac{\varepsilon_j t_j^p}{(1-\zeta)^{p(n-1)}}, \qquad (9)$$

where $1 \leq j \leq p-1$ and $\varepsilon_j \in \mathbb{Z}[\zeta]^\times$.

Now consider the following elementwise equation:

$$\zeta(\alpha+\overline{\zeta}\beta) + (\alpha+\zeta\beta) - (1+\zeta)(\alpha+\beta) = 0.$$

Dividing by $\alpha+\beta$ and using $\overline{\zeta} = \zeta^{p-1}$, we obtain

$$\frac{\zeta(\alpha+\zeta^{p-1}\beta)}{\alpha+\beta} + \frac{\alpha+\zeta\beta}{\alpha+\beta} - (1+\zeta) = 0.$$

Plugging (9) into this equation, we get

$$\frac{\zeta\varepsilon_{p-1}t_{p-1}^p}{(1-\zeta)^{p(n-1)}}+\frac{\varepsilon_1 t_1^p}{(1-\zeta)^{p(n-1)}}-(1+\zeta)=0.$$

Multiplying this relation by $(1-\zeta)^{p(n-1)}$ yields

$$\zeta\varepsilon_{p-1}t_{p-1}^p+\varepsilon_1 t_1^p-(1+\zeta)(1-\zeta)^{p(n-1)}=0. \qquad (10)$$

Write $t_j = x_j/y_j$ for some $x_j, y_j \in \mathbb{Z}[\zeta]$. Since t_j is prime to $1-\zeta$, and since $1-\zeta$ generates a prime ideal, x_j and y_j are each divisible by the same power of $1-\zeta$. We can therefore remove this power of $1-\zeta$ from both x_j and y_j, and thus assume x_j and y_j are prime to $1-\zeta$. Feeding the formulae $t_1 = x_1/y_1$ and $t_{p-1} = x_{p-1}/y_{p-1}$ into (10), we get

$$\zeta\varepsilon_{p-1}\frac{x_{p-1}^p}{y_{p-1}^p}+\varepsilon_1\frac{x_1^p}{y_1^p}-(1+\zeta)(1-\zeta)^{p(n-1)}=0. \qquad (11)$$

We let $c_{p-1} := x_{p-1}y_1$, $c_1 := x_1 y_{p-1}$ and $c_0 := y_1 y_{p-1}$. Then we multiply (11) by $y_1^p y_{p-1}^p$ and obtain that this equation is equivalent to

$$\zeta\varepsilon_{p-1}c_{p-1}^p+\varepsilon_1 c_1^p-(1+\zeta)(1-\zeta)^{p(n-1)}c_0^p=0.$$

Again, since x_1, x_{p-1}, y_1 and y_{p-1} are prime to $(1-\zeta)$, so are c_0, c_1 and c_{p-1}. Dividing by $\zeta\varepsilon_{p-1}$, we get

$$c_{p-1}^p+\frac{\varepsilon_1}{\zeta\varepsilon_{p-1}}c_1^p-\frac{1+\zeta}{\zeta\varepsilon_{p-1}}(1-\zeta)^{p(n-1)}c_0^p=0. \qquad (12)$$

This equation is very similar to (6), with n replaced by $n-1$. For example, the coefficient of $(1-\zeta)^{p(n-1)}c_0^p$ is a unit in $\mathbb{Z}[\zeta]$ (cf. Lemma 3) and c_0, c_1, c_{p-1} are prime to $(1-\zeta)$. Comparing (6) and (12), we note that the coefficient of β^p is 1, while the coefficient of c_1^p is not necessarily 1. If the coefficient of c_1^p, $\varepsilon_1/(\zeta\varepsilon_{p-1})$, were a pth power in $\mathbb{Z}[\zeta]$ (necessarily the pth power of a unit, since $\varepsilon_1/(\zeta\varepsilon_{p-1})$ is itself a unit), then we could write $(c_1')^p = (\varepsilon_1/(\zeta\varepsilon_{p-1}))c_1^p$ as a new pth power in $\mathbb{Z}[\zeta]$. Then the resulting equation would be

$$c_{p-1}^p + (c_1')^p + (1+\zeta)(1-\zeta)^{p(n-1)}c_0^p = 0,$$

so it would be just like (6), with n replaced by $n-1$. In order to show that $\varepsilon_1/(\zeta\varepsilon_{p-1})$ is in fact a pth power, we need the following preparation:

Claim: $\varepsilon_1/(\zeta\varepsilon_{p-1})$ as above is congruent to a rational integer (i.e. to an element of $\mathbb{Z}$) modulo $p\mathbb{Z}[\zeta]$.

Proof of the claim. Write (12) modulo $p\mathbb{Z}[\zeta]$:

$$c_{p-1}^p + \frac{\varepsilon_1}{\zeta\varepsilon_{p-1}}c_1^p \equiv 0 \bmod p\mathbb{Z}[\zeta].$$

Similarly to (2), we may argue that c_{p-1}^p and c_1^p are both congruent to rational integers modulo $p\mathbb{Z}[\zeta]$. Since c_1 is prime to $1-\zeta$, we can invert c_1 modulo $p\mathbb{Z}[\zeta]$ to get

$$\frac{\varepsilon_1}{\zeta\varepsilon_{p-1}} \equiv -c_{p-1}^p c_1^{-p} \equiv \text{rational integer} \bmod p\mathbb{Z}[\zeta].$$

Note that $(c_1 + p\mathbb{Z}[\zeta])^{-1}$ is still congruent to a rational integer because $\mathbb{Z}/p\mathbb{Z}$ is a field. □

Now that this claim has been proved, we proceed with the following interlude about Kummer's Lemma. As already mentioned, the main ideas of its proof are taken from [5, pages 80–81].

Lemma 13. (*Kummer's Lemma,* cf. [5, Theorem 5.36, page 79]) *Assume p is a regular prime and let ε be a unit of $\mathbb{Q}(\zeta)$. If ε is congruent to a rational integer* mod p *then ε is the* pth *power of a unit of $\mathbb{Q}(\zeta)$.*

Remarks.
1. Recall from our conventions that by the units of $\mathbb{Q}(\zeta)^\times$ we mean the elements of $\mathbb{Z}[\zeta]^\times$.
2. (cf. [5, page 79]) Note that this congruence is mod p, which is much stronger than $\mathrm{mod}(1-\zeta)$, which always holds.

The source for the following proof of this lemma is the seceond proof of [5, Theorem 5.36, page 79]. It can be found in [5, pages 80–81] and uses results from class field theory. For these results, we occasionally refer to [3] and [4].

Proof. (cf. [5, pages 80–81]) We may assume $\varepsilon \in \mathbb{R}$, or more precisely $\varepsilon \in \mathbb{Q}(\zeta)^+$ (cf. Lemma 8). The proof of this fact is taken from [5, page 79]. By Lemma 10, we may write $\varepsilon = \zeta^a \varepsilon_1$ with ε_1 real. Every element of $\mathbb{Z}[\zeta+\zeta^{-1}]$ is congruent mod $(1-\zeta)(1-\zeta^{-1}) = 2-(\zeta+\zeta^{-1})$ to a rational integer (replace $\zeta+\zeta^{-1}$ by 2). Also $\zeta^a = (1+(\zeta-1))^a \equiv 1+a(\zeta-1) \bmod (\zeta-1)^2$. Since $\zeta^a\varepsilon_1$ is congruent to a rational integer mod $(\zeta-1)^2$, we must have $p \mid a$ and therefore, $\zeta^a = 1$, meaning that $\varepsilon = \varepsilon_1$ is real. Moreover, if ε^{p-1} is a pth power, say $\varepsilon^{p-1} = \eta^p$ with $\eta \in \mathbb{Z}[\zeta]^\times$, then so is $\varepsilon = (\varepsilon/\eta)^p$. Therefore, we may assume $\varepsilon \equiv 1 \bmod p$.

Let $\pi = 1-\zeta$. Each element in $\mathbb{Z}[\zeta]$ is congruent to some element in $\mathbb{Z}$ modulo $(1-\zeta)$. To see this, recall that $1, \zeta, \ldots, \zeta^{p-2}$ generate $\mathbb{Z}[\zeta]$ over $\mathbb{Z}$.

If $x = \sum_{j=0}^{p-2} a_j \zeta^j \in \mathbb{Z}[\zeta]$ for some $a_j \in \mathbb{Z}$, then $x \equiv \sum_{j=0}^{p-2} a_j \bmod \pi$. By Lemma 3, we obtain

$$x - \sum_{j=0}^{p-2} a_j = \sum_{j=0}^{p-2} a_j(\zeta^j - 1) = \sum_{j=1}^{p-2} a_j(\zeta^j - 1) \in (1-\zeta),$$

as claimed.

Therefore, we may write $\varepsilon = 1 + pa + p\pi y$ for some $a \in \mathbb{Z}$, $y \in \mathbb{Z}[\zeta]$. Recall that ε is a unit in $\mathbb{Z}[\zeta]$, so $N(\varepsilon)$ must be a unit in $\mathbb{Z}$, that is, $N(\varepsilon) = \pm 1$. We claim that $N(\varepsilon)$ is congruent to $(1+pa)^{p-1}$ mod $p\pi$. This can be proved in a straightforward way by using the properties of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ and by using the fact that for any $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, $\sigma(\pi)$ is associated to $\pi = 1 - \zeta$ by Lemma 3:

$$\begin{aligned} N(\varepsilon) = N(1+pa+p\pi y) &= \prod_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})} \sigma(1+pa+p\pi y) \\ &= \prod_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})} (1+pa+p\sigma(\pi)\sigma(y)) \\ &\equiv \prod_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})} (1+pa) = (1+pa)^{p-1} \bmod (p\pi). \end{aligned}$$

This implies that

$$\begin{aligned} 1 \equiv N(\varepsilon) &\equiv (1+pa)^{p-1} \\ &\equiv 1 + (p-1)pa \equiv 1 - pa \bmod (p\pi), \end{aligned}$$

so we have $1 \equiv 1 - pa \mod p\pi$, in other words, $pa \in (p\pi)$ and thus $\pi \mid a$. Now we have $\varepsilon - 1 \in (p\pi)$ and hence $(\varepsilon - 1)/p \in (\pi)$.
Since $\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta)^+$ is totally ramified of degree 2, $\pi^+ := \pi\overline{\pi}$ is a uniformizer of $\mathbb{Q}(\zeta)^+$. Together with $\mathfrak{o}_{\mathbb{Q}(\zeta)} = \mathbb{Z}[\zeta]$ (cf. Lemma 2) and $\mathfrak{o}_{\mathbb{Q}(\zeta)^+} = \mathbb{Z}[\zeta + \zeta^{-1}]$ (cf. Lemma 11), this gives

$$\begin{aligned} \pi\mathbb{Z}[\zeta] \cap \mathbb{Q}(\zeta)^+ = \pi\mathbb{Z}[\zeta] \cap \mathbb{Z}[\zeta + \zeta^{-1}] &= \pi^+\mathbb{Z}[\zeta + \zeta^{-1}] \\ &= \pi\overline{\pi}\mathbb{Z}[\zeta + \zeta^{-1}] \subseteq \pi^2\mathbb{Z}[\zeta]. \end{aligned}$$

Since ε is assumed to be real, we get $(\varepsilon - 1)/p \in \mathbb{Z}[\zeta] \cap \mathbb{Q}(\zeta)^+ \subseteq (\pi)^2$ and then $\varepsilon - 1 \in (p\pi^2) = (\pi)^{p+1}$, so $(\varepsilon - 1)/\pi^p \equiv 0 \bmod \pi$.

Consider the following polynomial

$$f(X) := \frac{(\pi X - 1)^p + \varepsilon}{\pi^p} \in \mathbb{Z}_p[\zeta][X].$$

It is monic. We have $f(0) = (\varepsilon - 1)/\pi^p \equiv 0 \bmod (\pi)$, as seen above. Furthermore, we have $f'(0) \not\equiv 0 \bmod (p)$, since the constant coefficient of $f'(X)$ is equal to $p/\pi^{p-1} \in \mathbb{Z}[\zeta]^\times$. Thus the reduction of f modulo (π) splits into two relatively prime factors, of which one is linear and monic. By Hensel's Lemma, we know that this factorization lifts to $\mathbb{Z}_p[\zeta][X]$, such that one of the factors is linear and monic. So in fact, f has a root in $\mathbb{Z}_p[\zeta]$. Denote this root by $x \in \mathbb{Z}_p[\zeta]$. Then $\pi x - 1 \in \mathbb{Z}_p[\zeta]$ and $(\pi x - 1)^p = \varepsilon$. Hence ε admits a pth root in $\mathbb{Z}_p[\zeta]$, that means $\varepsilon^{1/p} \in \mathbb{Z}_p[\zeta]$. Since ε is assumed to be a unit in $\mathbb{Z}[\zeta]$ and $\mathbb{Z}[\zeta]^\times \subseteq \mathbb{Z}_p[\zeta]^\times$, we have $\varepsilon^{1/p} \in \mathbb{Z}_p[\zeta]^\times$.

At this point, we have proved the following:

Proposition 14. *$\varepsilon \in \mathbb{Z}[\zeta]$ as above satisfies $\varepsilon^{1/p} \in \mathbb{Z}_p[\zeta]$.* □

We now give a second proof of this assertion. It relies on p-adic analysis and the underlying material can be found in [5, pages 49–51].

Proof. We claim that $\exp((1/p)\log_p(\varepsilon))$ converges in $\mathbb{Q}_p(\zeta)$. If this is the case then $\varepsilon^{1/p} = \exp((1/p)\log_p(\varepsilon))$. To show this, we define the p-adic exponential function by

$$\exp(X) := \sum_{n=0}^{\infty} \frac{X^n}{n!},$$

(cf. [5, page 49]) and the p-adic logarithm by

$$\log_p(1 + X) := \sum_{n=1}^{\infty} \frac{(-1)^{n+1} X^n}{n}.$$

(cf. [5, page 50]).

Lemma 15. (cf. [5, page 50] and [5, Lemma 5.5, page 51]) *The p-adic exponential function has radius of convergence equal to $p^{-1/(p-1)}$, and the p-adic logarithm has radius of convergence at most 1. Moreover, we have $|\log_p(1+x)| = |x|$ if $|x| < p^{-1/(p-1)}$.*

Proof. Omitted, see [5, pages 49–50] and [5, page 51]. □

Since we have $\varepsilon \equiv 1 \bmod (\pi)^{p+1}$, we know that

$$|\varepsilon - 1| = p^{-(p+1)/(p-1)} < p^{-1/(p-1)},$$

so $\log_p(\varepsilon) = \log_p(1 + (\varepsilon - 1))$ converges in $\mathbb{Q}_p(\zeta)$ and satisfies

$$|\log_p(\varepsilon)| = |\varepsilon - 1| = p^{-(p+1)/(p-1)}.$$

Thus by Lemma 15, we have

$$\left|\frac{1}{p}\log_p(\varepsilon)\right| = \left|\frac{\varepsilon - 1}{p}\right| = p^{-2/(p-1)} < p^{-1/(p-1)},$$

so $\exp((1/p)\log_p(\varepsilon))$ converges in $\mathbb{Q}_p(\zeta)$. By the completeness of $\mathbb{Q}_p(\zeta)$ and the property of $\mathbb{Z}_p[\zeta]$ of being closed in $\mathbb{Q}_p(\zeta)$, we get

$$\varepsilon^{1/p} = \exp\left(\frac{1}{p}\log_p(\varepsilon)\right) \in \mathbb{Z}_p[\zeta].$$

This proves Proposition 14. □

To proceed with the proof of Lemma 13, note that in particular, Proposition 14 implies that

$$[\mathbb{Q}_p(\zeta, \varepsilon^{1/p}) : \mathbb{Q}_p(\zeta)] = 1. \tag{13}$$

With this fact in mind, we are going to use the following proposition, which we are going to prove using results about cyclic extensions, taken from [1], as well as using facts from class field theory, found in [3] and [4]. By means of contradiction we assume from now on that $\mathbb{Q}(\zeta)$ does not contain any pth root $\varepsilon^{1/p}$ of ε. Then we have:

Proposition 16.

(i) $[\mathbb{Q}(\zeta, \varepsilon^{1/p}) : \mathbb{Q}] = p$.

(ii) *The prime ideal* $(\pi) = (1 - \zeta)$ *of* $\mathbb{Z}[\zeta]$ *is unramified in* $\mathbb{Q}(\zeta, \varepsilon^{1/p})$ *and splits completely.*

(iii) $\mathbb{Q}(\zeta, \varepsilon^{1/p})$ *is a subfield of the maximal abelian unramified extension of* $\mathbb{Q}(\zeta)$ *(the Hilbert class field of* $\mathbb{Q}(\zeta)$*).*

Proof. For the proof of (i), we refer to [1, 4.8, Satz 3, page 202], by which $\mathbb{Q}(\zeta, \varepsilon^{1/p})/\mathbb{Q}(\zeta)$ is a cyclic Galois extension of degree p and by which $g(X) := X^p - \varepsilon \in \mathbb{Q}(\zeta)[X]$ is the minimal polynomial of $\varepsilon^{1/p}$ over $\mathbb{Q}(\zeta)$. Here we use our assumption $\varepsilon^{1/p} \notin \mathbb{Q}(\zeta)$ so that $[\mathbb{Q}(\zeta, \varepsilon^{1/p}) : \mathbb{Q}(\zeta)] > 1$.

Let $G := \mathrm{Gal}(\mathbb{Q}(\zeta, \varepsilon^{1/p})/\mathbb{Q}(\zeta))$, $\mathfrak{p} := (1 - \zeta) = (\pi)$, and let $\mathfrak{q}$ be a prime ideal lying above $\mathfrak{p}$ in $\mathbb{Q}(\zeta, \varepsilon^{1/p})$. Furthermore, let $G_{\mathfrak{q}} = G_{\mathfrak{q}}(\mathbb{Q}(\zeta, \varepsilon^{1/p})/\mathbb{Q}(\zeta)) = \{\sigma \in G \mid \sigma(\mathfrak{q}) = \mathfrak{q}\}$ denote its corresponding decomposition group. Due to the correspondence of prime ideals and valuations, and precisely by [4, Satz II.9.6, page 179], we have

$$G_{\mathfrak{q}} = G_{\mathfrak{q}}(\mathbb{Q}(\zeta, \varepsilon^{1/p})/\mathbb{Q}(\zeta)) \cong \mathrm{Gal}(\mathbb{Q}_p(\zeta, \varepsilon^{1/p})/\mathbb{Q}_p(\zeta)). \tag{14}$$

Since $\mathbb{Q}(\zeta, \varepsilon^{1/p})/\mathbb{Q}(\zeta)$ is Galois, we know from ramification theory that G acts on the set of prime ideals $\mathfrak{q}$ lying over $\mathfrak{p}$ (cf. [3, Lemma 4.8, page 93]), and that this action is transitive (cf. [3, Proposition 4.9, page 93]). It follows that $e := e(\mathfrak{q}/\mathfrak{p})$ and $f := f(\mathfrak{q}/\mathfrak{p})$ are independent of $\mathfrak{q}$ lying above $\mathfrak{p}$ (cf. [3, Corollary 4.11, (i) and (ii)]). Moreover, if we have $\mathfrak{p} = \prod_{j=1}^{r} \mathfrak{q}_j^{e_j} = \prod_{j=1}^{r} \mathfrak{q}_j^{e}$, then we have $efr = [\mathbb{Q}(\zeta, \varepsilon^{1/p}) : \mathbb{Q}(\zeta)] = p$, $(G : G_{\mathfrak{q}}) = r$ and $ef = |G_{\mathfrak{q}}|$ (cf. [3, Corollary 4.11 (iii), page 94]). Using (13) and (14), we obtain

$$ef = |G_{\mathfrak{q}}| = |\mathrm{Gal}(\mathbb{Q}_p(\zeta, \varepsilon^{1/p})/\mathbb{Q}_p(\zeta))| = 1,$$

and therefore $e = f = 1$, $r = p$. So in fact, (π) is unramified in $\mathbb{Q}(\zeta, \varepsilon^{1/p})$ and splits completely. This proves (ii).

For (iii), note first that $g(X)$ is separable, hence is equal to the characteristic polynomial of $\varepsilon^{1/p}$ over $\mathbb{Q}(\zeta)$. As a cyclic extension, $\mathbb{Q}(\zeta, \varepsilon^{1/p})/\mathbb{Q}(\zeta)$ is abelian. To show that all other primes of $\mathbb{Q}(\zeta)$ are unramified in $\mathbb{Q}(\zeta, \varepsilon^{1/p})$, note first that the archimedean primes are all complex, hence do not ramify (see [4, pages 193–194]). To treat the case of the nonarchimedean primes other than (π), we use the following result about finite extensions of number fields L/K:

Lemma 17. (cf. [4, Korollar 2.12, page 213]) *A prime ideal $\mathfrak{p}$ of K ramifies in L, if and only if $\mathfrak{p}$ divides the discriminant ideal $\mathfrak{d}$.*

Proof. Omitted, see [4, page 213]. □

Let $\vartheta := \varepsilon^{1/p}$. ϑ may be chosen as a primitive element, and $(1, \vartheta, \ldots, \vartheta^{p-1})$ as a basis of $\mathbb{Q}(\zeta, \vartheta)$ over $\mathbb{Q}(\zeta)$. If we let $d(1, \vartheta, \ldots, \vartheta^{p-1})$ be the discriminant of this basis, Tr the trace of $\mathbb{Q}(\vartheta, \zeta)/\mathbb{Q}(\zeta)$, and if we write $G = \{\sigma_1, \ldots, \sigma_p\}$, then we obtain

$$\begin{aligned}
d(1,\vartheta,\dots,\vartheta^{p-1}) &= \det((Tr(\vartheta^i\vartheta^j))_{i,j}) = \det((\sum_{k=1}^{p}\sigma_k(\vartheta^i\vartheta^j))_{i,j}) \\
&= \det((\sum_{k=1}^{p}\sigma_k(\vartheta^i)\sigma_k(\vartheta^j))_{i,j}) = \det((\sigma_k(\vartheta^i))_{i,k}^T(\sigma_k(\vartheta^j))_{j,k}) \\
&= \det((\sigma_k(\vartheta^i))_{i,k})^2 = \det((\sigma_k(\vartheta)^i)_{i,k})^2 \\
&= \prod_{1\le k<l\le p}(\sigma_k(\vartheta)-\sigma_l(\vartheta))^2 = \prod_{k\neq l}(\sigma_k(\vartheta)-\sigma_l(\vartheta)). \qquad (15)
\end{aligned}$$

Note that the matrix $(\sigma_k(\vartheta)^i)_{i,k}$ is a Vandermonde matrix. Without loss of generality, we may assume that $\sigma_1 = \mathrm{id}$. Since $g(X) = \prod_{k=1}^{p}(X-\sigma_k(\vartheta))$, applying the product rule yields

$$g'(\vartheta) = \prod_{k=2}^{p}(\vartheta-\sigma_k(\vartheta)).$$

Since $\sigma_k\sigma_l \neq \sigma_l$ for all $k \in \{2,\dots,p\}, l \in \{1,\dots,p\}$, it follows that

$$\begin{aligned}
N(g'(\vartheta)) &= \prod_{l=1}^{p}\sigma_l(\prod_{k=2}^{p}(\vartheta-\sigma_k(\vartheta))) = \prod_{l=1}^{p}\prod_{k=2}^{p}(\sigma_l(\vartheta)-\sigma_l(\sigma_k(\vartheta))) \\
&= \prod_{l=1}^{p}\prod_{k=2}^{p}(\sigma_l(\vartheta)-\sigma_k(\sigma_l(\vartheta))) = \prod_{l=1}^{p}\prod_{\substack{\tilde{k}=1\\ \tilde{k}\neq l}}^{p}(\sigma_l(\vartheta)-\sigma_{\tilde{k}}(\vartheta)) \\
&= \prod_{\tilde{k}\neq l}(\sigma_{\tilde{k}}(\vartheta)-\sigma_l(\vartheta)). \qquad (16)
\end{aligned}$$

Therefore, we get $d(1,\vartheta,\dots,\vartheta^{p-1}) = N(g'(\vartheta))$, and by considering (15) and (16) as equations of ideals,

$$\begin{aligned}
(d(1,\vartheta,\dots,\vartheta^{p-1})) &= (N(g'(\vartheta))) = (N(p\vartheta^{p-1})) = (p^pN(\vartheta)^{p-1}) \\
&= (\pi)^{(p-1)p}(N(\vartheta))^{p-1} = (\pi)^{(p-1)p}.
\end{aligned}$$

In the last step, $(N(\vartheta)) = (1)$ is true because $\vartheta^p = \varepsilon$ is a unit. Thus by Lemma 17, the nonarchimedean primes other than (π) are all unramified in $\mathbb{Q}(\zeta, \vartheta)$, since they do not divide $(\pi)^{(p-1)p}$.
Altogether, all primes of $\mathbb{Q}(\zeta)$ are unramified in $\mathbb{Q}(\zeta, \vartheta)$. Hence $\mathbb{Q}(\zeta, \varepsilon^{1/p})/\mathbb{Q}(\zeta)$ is unramified abelian, so $\mathbb{Q}(\zeta, \vartheta)$ is a subfield of the maximal unramified abelian extension of $\mathbb{Q}(\zeta)$. This proves (iii). □

Returning to the proof of Kummer's Lemma, the Galois group of the Hilbert class field of $\mathbb{Q}(\zeta)$ is isomorphic to the ideal class group of $\mathbb{Q}(\zeta)$ (cf. [4, Satz II.6.9, page 418]). Thus $|G| = p$ needs to divide the class number of $\mathbb{Q}(\zeta)$. But this contradicts the assumption that p is regular. Hence our original assumption is false and ε is a pth power of a unit in $\mathbb{Z}[\zeta]$. This completes the proof of Kummer's Lemma. □

Back to the proof of Case II: Applying Kummer's Lemma, we may replace the coefficient of c_1^p in (12) with 1, obtaining

$$c_{p-1}^p + c_1^p + (1+\zeta)(1-\zeta)^{p(n-1)}c_0^p = 0. \tag{17}$$

This has the same form and conditions as the original equation, but $n \geq 1$ is replaced with $n-1$. We may repeat this reduction until $n = 2$. But then (17) still holds and is of the form $c_{p-1}^p + c_1^p + (1+\zeta)(1-\zeta)^p c_0^p = 0$, so $n = 1$, but this case we have earlier shown to be false. Therefore we reach a contradiction, from which we conclude that our assumption of the existence of a solution is not true. This proves Theorem 12. □

As explained above, this also finishes the proof of Case II, so the proof of Theorem 1 is now complete. □

Remark. Note that the assertion of Fermat's Last Theorem is false, if x, y, z are assumed to be elements of an arbitrary ring of integers. For example, consider $x = \zeta_3$, $y = \zeta_3^2$, $z = -1$ as elements of $\mathbb{Q}(\zeta_3)$. Then we have $x, y, z \in \mathbb{Z}[\zeta_3]$ and $x^5 + y^5 = z^5$, where we recall that by Lemma 2, $\mathbb{Z}[\zeta_3]$ is equal to the ring of integers of $\mathbb{Q}(\zeta_3)$.

4 Kummer's criterion

In general, it is often not easy to compute the class number of a number field K, so the question arises, whether there are some criteria for the regularity of prime numbers. The aim of this section is to prove the following theorem, which was found by Kummer. For this we need the following definition:

Definition 18. (cf. [5, page 31])
For $n \geq 0$ the (ordinary) Bernoulli numbers $B_n \in \mathbb{Q}$ are defined by the formal power series expansion

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}.$$

Main theorem 19. (*Kummer's criterion*, cf. [5, page 6]) *Let $p \geq 3$ be a prime number and let h_p be the class number of $\mathbb{Q}(\zeta)$, where ζ is a primitive* pth *root of unity. Then p satisfies $p \mid h_p$ if and only if p divides the numerator of some Bernoulli number B_k, where $2 \leq k \leq p-3$ is even.*

To prepare the proof of this theorem, we state some results about the set of characters of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. Then the so-called *generalized Bernoulli numbers* will be defined. These are used to construct p-adic L-functions. Then, it is explained that $\mathbb{Q}(\zeta)$ is a so-called *CM-field*, which causes the class number of $\mathbb{Q}(\zeta)$ to be divisible by the class number of $\mathbb{Q}(\zeta)^+$. This allows us to define the *relative class number of* $\mathbb{Q}(\zeta)$ by $h_p^- := h_p/h_p^+$.
With all this information, we are then ready to show the theorem that p satisfies $p \mid h_p^-$ if and only if p divides the numerator of the Bernoulli number B_k for some $k = 2, 4, \ldots, p-3$ (cf. [5, Theorem 5.16, page 62]).

In order to complete the proof of Kummer's criterion, we shall then prove that $p \mid h_p^+$ implies $p \mid h_p^-$ (see [5, Theorem 5.34, page 78]). Instead of the proof in [5, pages 78–79], this thesis aims to provide a proof which uses class field theory and some results about the so-called *orthogonal idempotents* of a finite abelian group, as well as about the structure of the ideal class groups of $\mathbb{Q}(\zeta)$ and $\mathbb{Q}(\zeta)^+$.

Throughout this section, for any $a \in \{1, \ldots, p-1\}$, σ_a denotes the element of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ given by $\sigma_a : (\zeta \mapsto \zeta^a)$. If for $a \in \{1, \ldots, (p-1)/2\}$, σ_a is used as a Galois automorphism of $\mathbb{Q}(\zeta)^+ = \mathbb{Q}(\zeta + \zeta^{-1})$, then we regard it as the restriction of $\sigma_a \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ to $\mathbb{Q}(\zeta)^+$.

4.1 Characters of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$

For the general theory of Dirichlet characters and their basic properties we refer to [5, pages 20–21]. In our situation, we think of Dirichlet characters as characters of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, just by using the canonical isomorphism $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})^\times$.

Remark. Note that if G is a finite group and if $\chi : G \to \mathbb{C}^\times$ is a group homomorphism then the image of χ consits of roots of unity. Realizing $\overline{\mathbb{Q}}$ as a subfield of $\mathbb{C}$ we may equally well view χ as a group homomorphism $G \to \overline{\mathbb{Q}}^\times$. Embedding $\overline{\mathbb{Q}}$ into a larger field F (e.g. the field $\mathbb{C}_p$ considered below) we may and will often view χ as a map $G \to F^\times$. The statements we prove will all be independent of the choice of these embeddings.

Lemma 20. (cf. [5, page 51], [5, page 57]) *Given $a \in \mathbb{Z}_p^\times$, there exists a unique $(p-1)$st root of unity $\omega(a) \in \mathbb{Z}_p$ such that $\omega(a) \equiv a \bmod p$. Moreover, ω may be regarded as a Dirichlet character of conductor p and of order $p-1$.*

Proof. Consider the polynomial

$$f(X) := X^{p-1} - 1 \in \mathbb{Z}_p[X].$$

Let $\pi : \mathbb{Z}_p \to \mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$ denote the canonical projection. We have

$$^{\pi}f(X) = (X-1)(X-2)\dots(X-(p-1)) \in \mathbb{F}_p[X].$$

By Hensel's Lemma, $f(X)$ splits into $p-1$ linear factors, each of which is linear. Hence there are $p-1$ pairwise distinct roots of f (and therefore $(p-1)$st roots of unity) in $\mathbb{Z}_p$ and for each $a + p\mathbb{Z}_p \in \mathbb{F}_p^\times$ there is precisely one such root which is congruent to a mod p. That means π restricts to a bijection of $\mathbb{F}_p^\times$ and μ_{p-1}. Define the map $\tilde{\omega} : \mathbb{F}_p^\times \to \mu_{p-1}$ as the inverse. Since π is multiplicative, so is $\tilde{\omega}$. Define

$$\omega : \mathbb{Z}_p \to \mu_{p-1} \cup \{0\}, \quad \omega(x) := \begin{cases} (\tilde{\omega}\pi)(x) & \text{if } x \in \mathbb{Z}_p^\times, \\ 0 & \text{if } x \in p\mathbb{Z}_p. \end{cases}$$

Clearly, ω is multiplicative, it is of conductor p, and it is of order $p-1$. To see this, note that the relation

$$\omega(a)^m = \tilde{\omega}(\pi(a))^m = \tilde{\omega}(\pi(a^m)) = \tilde{\omega}(1 + p\mathbb{Z}_p) = 1$$

holds for all $a \in \mathbb{Z}_p^\times$, if and only if $m = k(p-1)$ for some $k \in \mathbb{Z}$.
Altogether, ω can in fact be regarded as a Dirichlet character of conductor p and of order $p-1$. □

By an abuse of notation, we often write ω instead of $\tilde{\omega}$, where we use that ω is of order $p-1$ and independent of a representative mod p. Also, for any $k \in \mathbb{Z}$, define $\omega^k : \mathbb{Z}_p \to \mathbb{C}^\times$ by $\omega^k(a) := \tilde{\omega}(a^k + p\mathbb{Z}_p)$. In particular, for $k \in (p-1)\mathbb{Z}$, $\omega^k = 1$ is equal to the trivial character. For all k not divisible by $p-1$, ω^k is a primitive Dirichlet character of conductor p. Note

that $\{\omega^i \mid i \in \mathbb{Z}\}$ is equipped with a group structure by pairwise multiplication. By the above definitions, $\omega^k = \omega^l$ for all $k \equiv l \bmod (p-1)$, so $\{\omega^i \mid i \in \mathbb{Z}\} = \{\omega^i \mid 0 \leq i \leq p-2\} \cong \mathbb{Z}/(p-1)\mathbb{Z}$ as abelian groups.
$\omega^0, \omega^1, \ldots, \omega^{p-2}$ are the only characters of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. On the one hand, let $\chi : \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \to \mathbb{C}^\times$ be an arbitrary character. Since $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is cyclic, χ is well-defined by sending a generator $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ to an element of $\mathbb{C}^\times$ whose order divides $p-1$, that is, to a $(p-1)$st root of unity. So there are at most $p-1$ pairwise distinct characters χ on $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. On the other hand, the maps ω^k, $0 \leq k \leq p-2$, are all pairwise distinct. By the above isomorphism $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$, any character of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ can be seen as a character of $(\mathbb{Z}/p\mathbb{Z})^\times$. Thus $\omega^0, \omega^1, \ldots, \omega^{p-2}$ are in fact the only characters of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$. In particular, we have shown:

Lemma 21. $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})^* \cong \{\omega^i \mid 0 \leq k \leq p-2\} \cong \mathbb{Z}/(p-1)\mathbb{Z}$ as abelian groups. □

Since $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$, we often use the notation $\omega^k(a)$, $k \in \mathbb{Z}$, $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ instead of $\omega^k(\sigma_a)$, $k \in \mathbb{Z}$, $\sigma_a \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, where generally σ_a denotes the Galois automorphism sending ζ to ζ^a.

Definition 22. (cf. [5, page 20]) *For any $n \in \mathbb{Z}_{n\geq 0}$, a character $\chi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$ is called even if $\chi(-1) = 1$ and odd if $\chi(-1) = -1$.*

Lemma 23. *For any $i \in \mathbb{Z}$, the character ω^i is even if i is even and odd else. Therefore, the set of odd characters of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is given by $\{\omega^i \mid i = 1, 3, \ldots, p-2\}$ and the set of even characters of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is given by $\{\omega^i \mid i = 0, 2, \ldots, p-3\}$.*

Proof. By the last definition, a character χ of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$ is even if $\chi(\sigma_{-1}) = \chi(-1) = 1$ and odd if $\chi(\sigma_{-1}) = \chi(-1) = -1$.

For $k \in \mathbb{Z}$, we have

$$\omega^k(-1) = \tilde{\omega}((-1)^k + p\mathbb{Z}_p) = \begin{cases} \tilde{\omega}(1 + p\mathbb{Z}_p) = 1 & \text{if } k \text{ is even,} \\ \tilde{\omega}(-1 + p\mathbb{Z}_p) = -1 & \text{if } k \text{ is odd,} \end{cases}$$

by the definitions of the maps ω and $\tilde{\omega}$ in the proof of Lemma 20. Therefore, the characters ω^k of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$ are even if k is even and odd else. Since $\omega^k = \omega^l$ for all $k, l \in \mathbb{Z}$ with $k \equiv l \bmod (p-1)$, the set of odd characters of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}))$ is given by $\{\omega^i \mid i = 1, 3, \ldots, p-2\}$ and the set of even characters of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}))$ is given by $\{\omega^i \mid i = 0, 2, \ldots, p-3\}$. □

Lemma 24. (cf. [5, Exercise 3.6 (a), page 29]) *Let χ be a nontrivial Dirichlet character of conductor f. Then*

$$\sum_{n=1}^{f} \chi(n) = 0.$$

Proof. Since χ is nontrivial, there is some $b \in (\mathbb{Z}/f\mathbb{Z})^\times$ with $\chi(b) \neq 1$. If we define $\tilde{n} := bn$ for $n \in \{1, \ldots, f\}$, we obtain

$$(\sum_{n=1}^{f} \chi(n))\chi(b) = \sum_{n=1}^{f} \chi(nb) = \sum_{\tilde{n}=1}^{f} \chi(\tilde{n}) = (\sum_{n=1}^{f} \chi(n)) \cdot 1.$$

Since $\chi(b) \neq 1$ this implies

$$\sum_{n=1}^{f} \chi(n) = 0.$$

□

Since for any integer i not divisible by $p-1$, ω^i is of conductor p,

$$\sum_{n=1}^{p} \omega^i(n) = 0. \tag{18}$$

In the following, for G a finite abelian group, we let G^* denote the group of characters of G. Moreover, if $H \subseteq G$ is a subgroup, then we use the definition of the orthogonal complement of H from [5, page 23],

$$H^\perp := \{\chi \in G^* \mid \chi(h) = 1 \text{ for all } h \in H\}. \tag{19}$$

Note that we have a natural isomorphism

$$(G/H)^* \cong H^\perp \tag{20}$$

(cf. [5, page 23]).

Lemma 25. *There is an isomorphism of abelian groups*

$$\mathrm{Gal}(\mathbb{Q}(\zeta)^+/\mathbb{Q})^* \cong \{\omega^i \mid 0 \leq i \leq p-2 \text{ even}\}.$$

Proof. Use

$$\mathrm{Gal}(\mathbb{Q}(\zeta)^+/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})/\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta)^+),$$

as well as $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})^* \cong \{\omega^i \mid 0 \leq i \leq p-2\}$ (by Lemma 21) and $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta)^+) = \{\mathrm{id}, (\zeta \mapsto \zeta^{-1})\}$. These results yield

$$\begin{aligned}
\mathrm{Gal}(\mathbb{Q}(\zeta)^+/\mathbb{Q})^* &\cong (\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})/\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta)^+))^* \\
&\overset{(20)}{\cong} (\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta)^+))^\perp \\
&\overset{(19)}{\cong} \{\omega^i \mid 0 \leq i \leq p-2,\ \omega^i(\mathrm{id}) = \omega^i((\zeta \mapsto \zeta^{-1})) = 1\} \\
&= \{\omega^i \mid 0 \leq i \leq p-2 \text{ even}\}
\end{aligned}$$

□

Later, we will use the following general fact:

Lemma 26. (cf. [5, Lemma 3.1, page 22]) *If G is a finite abelian group, then $G \cong G^*$ (noncanonically).*

Proof. Omitted. □

4.2 The generalized Bernoulli numbers

Definition 27. (cf. [5, page 31]) *Let χ be a Dirichlet character of conductor f. The generalized Bernoulli numbers $B_{n,\chi} \in \mathbb{C}$ for $n \geq 0$ are defined by the formal power seies expansion*

$$\sum_{a=1}^{f} \frac{\chi(a)te^{at}}{e^{tf}-1} = \sum_{n=0}^{\infty} B_{n,\chi}\frac{t^n}{n!}.$$

Multiplying this equation by $e^{tf}-1$, we obtain

$$\sum_{a=1}^{f} \chi(a)te^{at} = (e^{tf}-1)\sum_{n=0}^{\infty} B_{n,\chi}\frac{t^n}{n!}. \tag{21}$$

We have

$$\sum_{a=1}^{f} \chi(a)te^{at} = \sum_{n=0}^{\infty}[\sum_{a=1}^{f}\chi(a)a^n]\frac{t^{n+1}}{n!} = \sum_{n=0}^{\infty}[(n+1)\sum_{a=1}^{f}\chi(a)a^n]\frac{t^{n+1}}{(n+1)!} \tag{22}$$

and

$$\begin{aligned}
(e^{tf}-1)(\sum_{s=0}^{\infty} B_{s,\chi}\frac{t^s}{s!}) &= (\sum_{r=1}^{\infty}\frac{f^r t^r}{r!})(\sum_{s=0}^{\infty} B_{s,\chi}\frac{t^s}{s!}) \\
&= t(\sum_{r=0}^{\infty}\frac{f^{r+1}t^r}{(r+1)!})(\sum_{s=0}^{\infty} B_{s,\chi}\frac{t^s}{s!}) \\
&= \sum_{n=0}^{\infty}[t\sum_{\substack{0\le r,s\le n,\\ r+s=n}}\frac{f^{r+1}(n+1)!}{(r+1)!s!}B_{s,\chi}]\frac{t^n}{(n+1)!} \\
&= \sum_{n=0}^{\infty}[\sum_{r=0}^{n} f^{r+1}\binom{n+1}{r+1}B_{n-r,\chi}]\frac{t^{n+1}}{(n+1)!}. \qquad (23)
\end{aligned}$$

Plugging the results of (22) and (23) into (21), we obtain that for each $n \geq 0$,

$$(n+1)\sum_{a=1}^{f}\chi(a)a^n = \sum_{r=0}^{n} f^{r+1}\binom{n+1}{r+1}B_{n-r,\chi}. \qquad (24)$$

Letting $n=0$, this reduces to

$$\sum_{a=1}^{f}\chi(a) = fB_{0,\chi}. \qquad (25)$$

If χ is nontrivial then by Lemma 24, $B_{0,\chi}=0$, since $f\neq 0$. If $\chi = 1$ then $B_{0,1}=1$, since in this case, (25) reads $f=\sum_{a=1}^{f}1=\sum_{a=1}^{f}\chi(a)=fB_{0,\chi}$. To summerize,

$$B_{0,\chi} = \begin{cases} 1 & \text{if } \chi \text{ is trivial,} \\ 0 & \text{if } \chi \text{ is nontrivial.} \end{cases} \qquad (26)$$

Furthermore, (24) in the case of $n=1$ and χ nontrivial says that

$$2\sum_{a=1}^{f}\chi(a)a = \binom{2}{1}fB_{1,\chi} + \binom{2}{2}f^2B_{0,\chi} \overset{(26)}{=} 2fB_{1,\chi}.$$

If χ is trivial and $n = 1$ then (24) yields

$$2 = 2\sum_{a=1}^{f}\chi(a)a = \binom{2}{1}fB_{1,\chi} + \binom{2}{2}f^2B_{0,\chi} \overset{(26)}{=} 2B_{1,\chi} + 1.$$

From these two equations we find that

$$B_{1,\chi} = \begin{cases} \frac{1}{2} & \text{if } \chi \text{ is trivial,} \\ \frac{1}{f}\sum_{a=1}^{f}\chi(a)a & \text{if } \chi \text{ is nontrivial.} \end{cases} \tag{27}$$

We are now going to work out certain congruence relations between the generalized Bernoulli numbers and the ordinary ones. At first, multiply the definition

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}$$

by $e^t - 1$ and use the expansion of the exponential function:

$$\begin{aligned} t &= (e^t - 1)(\sum_{s=0}^{\infty} B_s \frac{t^s}{s!}) = (\sum_{r=1}^{\infty} \frac{t^r}{r!})(\sum_{s=0}^{\infty} B_s \frac{t^s}{s!}) \\ &= t(\sum_{r=0}^{\infty} \frac{t^r}{(r+1)!})(\sum_{s=0}^{\infty} B_s \frac{t^s}{s!}) = t(\sum_{n=0}^{\infty}(\sum_{\substack{0\leq r,s\leq n \\ r+s=n}} \frac{1}{(r+1)!s!}B_s)t^n) \\ &= \sum_{n=0}^{\infty}(\sum_{\substack{0\leq r,s\leq n \\ r+s=n}} \frac{(n+1)!}{(r+1)!s!}B_s)\frac{t^{n+1}}{(n+1)!} = \sum_{n=0}^{\infty}(\sum_{r=0}^{n}\binom{n+1}{r+1}B_{n-r})\frac{t^{n+1}}{(n+1)!}. \end{aligned}$$

Comparing coefficients, we find that

$$1 = \sum_{r=0}^{0}\binom{0+1}{r+1}B_{0-r} = B_0,$$

and therefore, if $n \geq 1$,

$$0 = \sum_{r=0}^{n} \binom{n+1}{r+1} B_{n-r} = B_0 + \sum_{r=0}^{n-1} \binom{n+1}{r+1} B_{n-r} = 1 + \sum_{r=0}^{n-1} \binom{n+1}{r+1} B_{n-r}.$$

In particular, this leads to $B_1 = -1/2$.

Considering the generalized Bernoulli numbers again, note that when $\chi = 1$, we have

$$\sum_{n=0}^{\infty} B_{n,1} \frac{t^n}{n!} = \frac{te^t}{e^t - 1} = \frac{t}{e^t - 1} + \frac{t(e^t - 1)}{e^t - 1} = \frac{t}{e^t - 1} + t = (\sum_{n=0}^{\infty} B_n \frac{t^n}{n!}) + t,$$

so by comparing coefficients we find that

$$B_{n,1} = B_n \quad \text{if } n \geq 2.$$

To summerize, we have

$$B_{n,1} = \begin{cases} 1 = B_0 & \text{if } n = 0, \\ \frac{1}{2} = B_1 + 1 & \text{if } n = 1, \\ B_n & \text{if } n \geq 2. \end{cases} \tag{28}$$

Lemma 28. *For $n \geq 3$ odd, we have $B_n = 0$.*

Proof. Note that we have

$$\sum_{n=0}^{\infty} B_n \frac{(-t)^n}{n!} = \frac{-t}{e^{-t} - 1} = \frac{-te^t}{1 - e^t} = t + \frac{t}{e^t - 1} = t + \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}.$$

By comparing the coefficients of these two formal power seies we obtain $-B_n = B_n$ for all odd integers $n \geq 3$, i.e. we have $B_n = 0$ for all $n \geq 3$ for all odd integers $n \geq 3$. □

Remark. Moreover, comparing the coefficients of t in the above formal power seies expansion yields $-B_1 = 1 + B_1$ and then $B_1 = -1/2$. So this is another way of deducing this result.

We now consider the general Bernoulli numbers $B_{n,\chi}$ for $n \geq 0$ and $\chi = \omega^i$, $i \in \mathbb{Z}$. Since ω^{-1} is nontrivial, it satisfies $B_{0,\omega^{-1}} = 0$ by (26). Moreover, the images of the ω^i are all $(p-1)$st roots of unity and therefore are all elements of $\mathbb{Q}(\zeta_{p-1})$. By Lemma 20, the $(p-1)$st roots of unity can all be regarded as elements of $\mathbb{Z}_p \subseteq \mathbb{Q}_p$. Hence all the generalized Bernoulli numbers B_{n,ω^i} lie in $\mathbb{Q}(\zeta_{p-1})$ (for $n \geq 0$, $i \in \mathbb{Z}$) and therefore in $\mathbb{Q}_p$. From this point of view, congruences of the B_{n,ω^i} modulo $\mathbb{Z}_p$ are well-defined (where $\mathbb{Z}_p$ is regarded as additive subgroup of $\mathbb{Q}_p$). Recall that by the remark at the beginning of Subsection 4.1, the characters ω^i are viewed as maps with image in $\mathbb{C}_p^\times$. Since $\omega^{-1} \neq 1$, it is of conductor p, so (27) yields

$$\begin{aligned} B_{1,\omega^{-1}} &= \frac{1}{p}\sum_{a=1}^{p} \omega^{-1}(a)a = \frac{1}{p}\sum_{a=1}^{p-1} \omega^{-1}(a)a = \frac{1}{p}\sum_{a=1}^{p-1} \tilde{\omega}((a+p\mathbb{Z}_p)^{-1})a \\ &\equiv \frac{1}{p}\sum_{a=1}^{p-1} a^{-1}a = \frac{p-1}{p} \bmod \mathbb{Z}_p. \end{aligned} \tag{29}$$

Lemma 29. (cf. [5, page 101]) *Suppose $i \in \mathbb{Z}$ with $(p-1) \nmid i$ is even and prime to p. Then $B_{1,\omega^i} = 0$.*

Proof. Let $i \in \mathbb{Z}$ be even with $(p-1) \nmid i$. Then ω^i is of conductor p, so by (27),

$$B_{1,\omega^i} = \frac{1}{p}\sum_{a=1}^{p-1} \omega^i(a)a.$$

Obviously,

$$\frac{1}{p}\sum_{a=1}^{p-1}\omega^i(a)a = \frac{1}{p}\sum_{a=1}^{p-1}\omega^i(-a)(p-a),$$

and since ω^i is even, $\omega^i(a) = \omega^i(-a)$ for all $a \in \{1, \ldots, p-1\}$, so altogether we obtain

$$\begin{aligned} 2B_{1,\omega^i} &= \frac{1}{p}\sum_{a=1}^{p-1}\omega^i(a)a + \frac{1}{p}\sum_{a=1}^{p-1}\omega^i(-a)(p-a) \\ &= \frac{1}{p}\sum_{a=1}^{p-1}\omega^i(a)(a+(p-a)) = \frac{1}{p}\sum_{a=1}^{p-1}\omega^i(a)p = \sum_{a=1}^{p-1}\omega^i(a) \overset{(18)}{=} 0. \end{aligned}$$

□

4.3 p-adic L-functions

We are going to use the following five results in order to deduce some important congruence results of Bernoulli numbers. Their assertions and the respective proofs can be found in [5, pages 57–61]. For further information about p-adic L-functions, we refer to [5, §5.2, pages 55–59].

Let $\mathbb{C}_p$ be the completion of the algebraic closure of $\mathbb{Q}_p$ with respect to the p-adic absolute value (cf. [5, pages 47–48]) and let

$$\mathfrak{o}_{\mathbb{C}_p} = \{z \in \mathbb{C}_p \mid |z| \leq 1\}.$$

Sometimes, the referenced literture uses a variable q defined by

$$q := \begin{cases} p & \text{for } p \geq 3, \\ 4 & \text{for } p = 2, \end{cases}$$

where p is a prime number (cf. [5, page 51]). In our situation, we assume $p \geq 3$, so we replace q by p. Recall that by the remark at the beginning of Subsection 4.1, for a finite abelian group G and a group homomorphism

$\chi : G \to \mathbb{C}^\times$ we will view χ as a map $G \to \mathbb{C}_p^\times$.

Theorem and Definition 30. (cf. [5, Theorem 5.11, page 57]) *Let χ be a Dirichlet character of conductor f_χ and let F be any multiple of p and f_χ. Then there exists a p-adic meromorphic (analytic if $\chi \neq 1$) function $L_p(s, \chi)$ on $\{s \in \mathbb{C}_p \mid |s| < p^{(p-2)/(p-1)}\}$ such that*

$$L_p(1-n, \chi) = -(1 - \chi\omega^{-n}(p)p^{n-1})\frac{B_{n,\chi\omega^{-n}}}{n} \text{ for all } n \geq 1. \tag{30}$$

If $\chi = 1$ then $L_p(s, \chi)$ is analytic except for a simple pole at $s = 1$ with residue $(1 - 1/p)$. In fact, we have the formula

$$L_p(s, \chi) = \frac{1}{F}\frac{1}{s-1}\sum_{\substack{a=1 \\ p \nmid a}}^{F} \chi(a)\langle a\rangle^{1-s} \sum_{j=0}^{\infty} \binom{1-s}{j} \cdot B_j \cdot \left(\frac{F}{a}\right)^j .$$

Here, for any $a \in \mathbb{Z}_p$, $\langle a \rangle$ is defined by $\langle a \rangle := \omega^{-1}(a)a$, so that it satisfies

$$\langle a \rangle = \omega^{-1}(a)a \equiv 1 \bmod p.$$

Proof. Omitted, see [5, pages 57–58]. □

Remark. In particular, $L_p(n, \chi)$ is defined for all $n \in \mathbb{Z}$, since for all $n \in \mathbb{Z} \subseteq \mathbb{Z}_p$, $|n| \leq 1 < p^{(p-2)/(p-1)}$, where $|\cdot|$ denotes the p-adic absolute value.

Theorem 31. (cf. [5, Theorem 5.12, page 59]) *Suppose $\chi \neq 1$ is a Dirichlet character of conductor f_χ and $p^2 \nmid f_\chi$. Then*

$$L_p(s, \chi) = a_0 + a_1(s-1) + a_2(s-1)^2 + \ldots$$

with $|a_0| \leq 1$ and with $p \mid a_i$ for all $i \geq 1$.

Proof. Omitted, see [5, pages 59–60]. □

Corollary 32. (cf. [5, Corollary 5.13, page 61]) *Suppose* $\chi \neq 1$ *is a Dirichlet character of conductor* f_χ *and* $p^2 \nmid f_\chi$. *Let* $m, n \in \mathbb{Z}$. *Then* $L_p(n,\chi), L_p(m,\chi) \in \mathfrak{o}_{\mathbb{C}_p}$ *and*

$$L_p(n,\chi) \equiv L_p(m,\chi) \bmod p,$$

viewed as a congruence in $\mathfrak{o}_{\mathbb{C}_p}$.

Proof. Both sides are congruent to a_0 in the notation of Theorem 31. □

Corollary 33. (*Kummer's Congruences*, cf. [5, Corollary 5.14, page 61]) *Suppose* $m \equiv n \not\equiv 0 \bmod (p-1)$ *are positive even integers. Then*

$$\frac{B_m}{m}, \frac{B_n}{n} \in \mathbb{Z}_p \quad \text{and} \quad \frac{B_m}{m} \equiv \frac{B_n}{n} \bmod p.$$

Proof. Since $m \equiv n \not\equiv 0 \bmod (p-1)$, we have $\omega^m = \omega^n$ as nontrivial characters of conductor $f_{\omega^n} = f_{\omega^m} = p$. Hence the assumption $p^2 \nmid f_{\omega^n} = f_{\omega^m} = p$ of Corollary 32 is satisfied, so we have

$$L_p(1-m,\omega^m), L_p(1-n,\omega^n) \in \mathfrak{o}_{\mathbb{C}_p}$$

and

$$L_p(1-m,\omega^m) \equiv L_p(1-n,\omega^n) \bmod p,$$

viewed as a congruence in $\mathfrak{o}_{\mathbb{C}_p}$. Moreover, since n, m are even and positive, (28) gives $B_m = B_{m,1}$ and $B_n = B_{n,1}$. Applying Theorem 30 to the cases

$\chi = \omega^m$, respctively $\chi = \omega^n$, we find that

$$L_p(1-m, \omega^m) = -(1 - \omega^m \omega^{-m}(p) p^{m-1}) \frac{B_{m,\omega^m \omega^{-m}}}{m} = -(1 - p^{m-1}) \frac{B_{m,1}}{m},$$
$$L_p(1-n, \omega^n) = -(1 - \omega^n \omega^{-n}(p) p^{n-1}) \frac{B_{n,\omega^n \omega^{-n}}}{n} = -(1 - p^{n-1}) \frac{B_{n,1}}{n}.$$

We have already pointed out that the images of the characters ω^i, $i \in \mathbb{Z}$, are all $(p-1)$st roots of unity lying in $\mathbb{Z}_p$, so that for $i, k \in \mathbb{Z}$ the generalized Bernoulli numbers B_{k,ω^i} all lie in $\mathbb{Q}(\zeta_{p-1}) \subseteq \mathbb{Q}_p$. Altogether, we find that

$$L_p(1-m, \omega^m), L_p(1-n, \omega^n) \in \{z \in \mathbb{Q}_p \mid |z| \leq 1\} = \mathbb{Z}_p,$$

so that

$$L_p(1-m, \omega^m) \equiv L_p(1-n, \omega^n) \bmod p$$

may and will be viewed as a congruence in $\mathbb{Z}_p$.

Putting everything together, we obtain

$$\begin{aligned}\frac{B_m}{m} &= \frac{B_{m.1}}{m} \equiv (1 - p^{m-1}) \frac{B_{m,1}}{m} \bmod p \\ &= -L_p(1-m, \omega^m) \equiv -L_p(1-n, \omega^n) \bmod p \\ &= (1 - p^{n-1}) \frac{B_{n,1}}{n} \equiv \frac{B_{n,1}}{n} \bmod p \\ &= \frac{B_n}{n}\end{aligned}$$

with

$$\frac{B_m}{m}, \frac{B_n}{n} \in \mathbb{Z}_p,$$

as claimed. □

Corollary 34. (cf. [5, Corollary 5.15, page 61]) *Suppose n is odd and* *satisfies* $n \not\equiv -1 \bmod (p-1)$. *Then*

$$B_{1,\omega^n},\ \frac{B_{n+1}}{n+1} \in \mathbb{Z}_p \quad \text{and} \quad B_{1,\omega^n} \equiv \frac{B_{n+1}}{n+1} \bmod p.$$

Proof. Since $n \not\equiv -1 \bmod (p-1)$, we have $(p-1) \nmid (n+1)$, so $\omega^{n+1} \neq 1$. Therefore, it is of conductor $f_{\omega^{n+1}} = p$ and the assumption $p^2 \nmid f_\chi$ of Corollary 32 is true for $\chi = \omega^{n+1}$. Since n is odd and $p-1$ is even, we also have $(p-1) \nmid n$, so $\omega^n \neq 1$ and therefore $\omega^n(p) = 0$. By the properties of the ω^k, $k \in \mathbb{Z}$ (see Subsection 4.1), $\omega^n = \omega^{n+1}\omega^{-1}$ and $\omega^{n+1}\omega^{-(n+1)} = 1$. Also, $B_{n+1,1} = B_{n+1}$ by (28), and $L_p(0, \omega^{n+1}) \equiv L_p(1-(n+1), \omega^{n+1}) \bmod p$ by Corollary 32. Similarly to the previous corollary, this congruence may not only be viewed in $\mathfrak{o}_{\mathbb{C}_p}$ but also in $\mathbb{Z}_p$. Altogether, we find that

$$\begin{aligned}
B_{1,\omega^n} &= (1-\omega^n(p)p^0)B_{1,\omega^n} = (1-\omega^{n+1}\omega^{-1}(p)p^{1-1})\frac{B_{1,\omega^{n+1}\omega^{-1}}}{1} \\
&\overset{(30)}{=} -L_p(1-1, \omega^{n+1}) = -L_p(0, \omega^{n+1}) \\
&\equiv -L_p(1-(n+1), \omega^{n+1}) \bmod p \\
&\overset{(30)}{=} (1-\omega^{n+1}\omega^{-(n+1)}(p)p^{(n+1)-1})\frac{B_{n+1,\omega^{n+1}\omega^{-(n+1)}}}{n+1} \\
&= (1-p^n)\frac{B_{n+1,1}}{n+1} = (1-p^n)\frac{B_{n+1}}{n+1} \equiv \frac{B_{n+1}}{n+1} \bmod p,
\end{aligned}$$

as claimed. □

4.4 Properties of $\mathbb{Q}(\zeta)$ as a *CM*-field and its relative class number

We are going to introduce a class of fields called *CM-fields* and to show that $\mathbb{Q}(\zeta)$ is a such a CM-field. The underlying material can be found in [5, pages 38–40].

Definition 35. (cf. [5, page 38]) *A CM-field is an imaginary quadratic* *extension of a totally real number field.*

Lemma 36. (cf. [5, page 39]) *Let K be a CM-field with K^+ its maximal totally real subfield. Then complex conjugation on $\mathbb{C}$ induces an automorphism on K which is independent of the embedding into $\mathbb{C}$. Moreover, for any $\varepsilon \in K^\times$, $\varepsilon/\overline{\varepsilon}$ is a root of unity, and K^+ is precisely the set of elements $x \in K$ with $\overline{x} = x$.*

Proof. Let $\phi, \psi : K \to \mathbb{C}$ be two embeddings. We are going to show that $\phi^{-1}(\overline{\phi(\alpha)}) = \psi^{-1}(\overline{\psi(\alpha)})$ for all $\alpha \in K$. The extension $\phi(K)/\phi(K^+)$ is quadratic, hence it is normal. Moreover, complex conjugation fixes $\phi(K^+)$, since $\phi(K^+) \subseteq \mathbb{R}$. Denote the complex conjugation on $\phi(K)$ as a $\phi(K^+)$-linear map by $c : \phi(K) \to \mathbb{C}$ and its image by $c(\phi(K)) = \overline{\phi}(K)$. By normality, we have $\overline{\phi}(K) = c(\phi(K)) \subseteq \phi(K)$. The bijectivity of complex conjugation then yields $\overline{\phi}(K) = \phi(K)$. Together with the injectivity of ϕ, $\phi^{-1}(\overline{\phi}) : K \to K$ is a well-defined automorphism of K. Since K^+ is totally real, we have $\phi(K^+) \subseteq \mathbb{R}$ and thus for all $x \in K^+$, $\phi^{-1}(\overline{\phi})(x) = \phi^{-1}(c(\phi(x))) = \phi^{-1}(\phi(x)) = x$. So $\phi^{-1}(\overline{\phi})$ fixes K^+, that is, $\phi^{-1}(\overline{\phi}) \in \mathrm{Gal}(K/K^+)$. Similarly, $\psi^{-1}(\overline{\psi}) \in \mathrm{Gal}(K/K^+)$. Since K is imaginary, there are certain $x, y \in K$ such that $c(\phi(x)) \neq \phi(x)$ and then $\phi^{-1}(\overline{\phi})(x) = \phi^{-1}(c(\phi(x))) \neq \phi^{-1}(\phi(x)) = x$, respectively $\psi^{-1}(\overline{\psi})(y) \neq y$. Thus neither $\phi^{-1}(\overline{\phi})$ nor $\psi^{-1}(\overline{\psi})$ are the identity on K. But since $\mathrm{Gal}(K/K^+)$ consists of only two elements, $\phi^{-1}(\overline{\phi}) = \psi^{-1}(\overline{\psi})$. So we may define complex conjugation on K by $\overline{(\cdot)} : K \to K$, $\alpha \mapsto \overline{\alpha} = \phi^{-1}(\overline{\phi})(\alpha) = \psi^{-1}(\overline{\psi})(\alpha)$ (where ϕ, ψ are embeddings of K into $\mathbb{C}$). Consequently, $|\alpha|^2 = \alpha\overline{\alpha}$ is well-defined and independent of the embedding. In particular, for any $\varepsilon \in K^\times$, $|\varepsilon/\overline{\varepsilon}|^2 = (\varepsilon\overline{\varepsilon})/(\overline{\varepsilon}\varepsilon) = 1$, independently of the embedding, so $\varepsilon/\overline{\varepsilon}$ is a root of unity in K, as follows from Lemma 4. To see the last assertion of this lemma, let $x \in K$ with $\overline{x} = x$ be arbitrary and choose any two embeddings ϕ, ψ of K into $\mathbb{C}$. By the above, we have $\phi^{-1}(\overline{\phi})(x) = \psi^{-1}(\overline{\psi})(x)$, in other words, $\phi^{-1}(\overline{\phi(x)}) = \psi^{-1}(\overline{\psi(x)})$. Letting

$\psi = \mathrm{id}_K$, we find that $\phi^{-1}(\overline{\phi(x)}) = \overline{x}$. Applying ϕ to this equation yields $\overline{\phi(x)} = \phi(\overline{x})$, so $\overline{\phi(x)} = \phi(x)$ by the assumption on x. Thus $x \in K^+$. Since also all elements $x \in K^+$ satisfy $\overline{x} = x$, this proves the claim that K^+ is precisely the set of elements $x \in K$ with $\overline{x} = x$. □

Proposition 37. (cf. [5, Theorem 4.12, page 40]) *Let K be a CM-field with E the group of units of its ring of integers and let W be the group of roots of unity in E. Let K^+ be its maximal totally real subfield and E^+ the group of units in the ring of integers of K^+. Then*

$$Q := (E : WE^+) \in \{1, 2\}.$$

Proof. (cf. [5, page 40]) Let $\phi : E \to W$ be the group homomorphism defined by $\phi : \varepsilon \mapsto \varepsilon/\overline{\varepsilon}$. By the previous lemma, we know that $\phi(\varepsilon) \in W$, so ϕ is well-defined. Let $\psi : E \to W/W^2$ be the group homomorphism induced by ϕ. We claim that $\ker(\psi) = WE^+$. In the following proof of this equation, we use the variable ζ as an element of W, not as usual as a pth root of unity.
To show the inclusion $\ker(\psi) \subseteq WE^+$, let $\varepsilon \in \ker(\psi)$, i.e. there is some $\zeta \in W$ such that $\varepsilon/\overline{\varepsilon} = \zeta^2$. This implies $\varepsilon\zeta^{-1} = \varepsilon\overline{\zeta} = \overline{\varepsilon}\zeta$, and then $\varepsilon\zeta^{-1} \in E^+$, by Lemma 36. Hence we obtain $\varepsilon = (\varepsilon\zeta^{-1})\zeta \in WE^+$, proving the first inclusion.
For the reverse inclusion, let $\zeta \in W$ and $\varepsilon \in E^+$. Then $\phi(\varepsilon/\overline{\varepsilon}) = (\varepsilon\zeta)/\overline{(\varepsilon\zeta)} = \zeta/\zeta^{-1} = \zeta^2 \in W^2$, so $\varepsilon\zeta \in \ker(\psi)$, proving the second inclusion. Hence we have $WE^+ = \ker(\psi)$, as claimed. Now we obtain $E/\ker(\psi) \cong \psi(E) \subseteq W/W^2$ as abelian groups. From Lemma 6, it follows that $|W/W^2| = 2$. Therefore,

$$Q = (E : WE^+) = |E/WE^+| = |E/\ker(\psi)| = |(\psi)(E)| \leq 2,$$

as claimed. □

Corollary 38. (cf. [5, Corollary 4.13, page 40] and [5, Proposition 1.5, pages 3–4]) *In the case of $K = \mathbb{Q}(\zeta)$, we have $Q = 1$.*

Proof. The ring of integers of $\mathbb{Q}(\zeta)$ is $\mathbb{Z}[\zeta]$ (cf. Lemma 2), so in this case we have $E = \mathbb{Z}[\zeta]^\times$. By Lemma 10, we know that if ε is a unit of $\mathbb{Z}[\zeta]$ then there exist some $\varepsilon_1 \in \mathbb{Q}(\zeta + \zeta^{-1})$ and $r \in \mathbb{Z}$ such that $\varepsilon = \varepsilon_1 \zeta^r \in WE^+ = \ker(\psi)$, where $\psi : E \to W/W^2$ is the above mentioned homomorphism in the proof of the last proposition. So in this case, ψ is trivial, in other words, $Q = (E : WE^+) = |\psi(\mathbb{Z}|\zeta]^\times)| = 1$. □

Theorem and Definition 39. (cf. [5, Theorem 4.10, page 39]) *Let K be a CM-field, K^+ its maximal real subfield, and let h and h^+ be the respective class numbers. Then h^+ divides h. The quotient $h^- := h/h^+$ is called the relative class number.*

Proof. The proof follows the line of arguments of the respective proof of [5, Proposition 4.11, page 39], we only change the notation of the respective Hilbert class fields. We need the following lemma (a result from class field theory, a proof of which can also be found in [5, page 39]):

Lemma 40. (cf. [5, Proposition 4.11, page 39]) *Let K/L be an extension of number fields such that there is no nontrivial unramified (at all primes, including archimedean ones) subextension F/L with* $\mathrm{Gal}(F/L)$ *abelian. Let h_K and h_L denote the respective class numbers of K and L. Then $h_L \mid h_K$.*

Proof. Let L_1 be the maximal unramified (at all primes, including archimedean ones) abelian extension of L, that means L_1 is the Hilbert class field of L. By class field theory, $\mathrm{Gal}(L_1/L)$ is isomorphic to the ideal class group of L (see [4, Satz II.6.9, page 418]). Since there is no nontrivial unramified abelian subextension of K/L, we obtain $L_1 \cap K = L$. By Galois theory, $\mathrm{Gal}(L_1/L) = \mathrm{Gal}(L_1/(K \cap L_1)) \cong \mathrm{Gal}(KL_1/K)$. Let K_1 denote the maximal unramified abelian extension of K, in other words, the Hilbert class field of K. It is a general fact that the extension KL_1/K is unramified abelian, so we have $KL_1 \subseteq K_1$. Again by [4, Satz II.6.9, page 418], $\mathrm{Gal}(K_1/K)$ is isomorphic to the ideal class group of K. In particular, we find that

$$h_K = [K_1 : K] = [K_1 : KL_1][KL_1 : K] = [K_1 : KL_1][L_1 : L] = [K_1 : KL_1]h_L,$$

so in fact, $h_L \mid h_K$, proving this lemma. □

Returning to the proof of the theorem, we note that all the archimedean primes of K^+ are given by real embeddings, so they are all totally ramified (cf. [4, pages 193–194]). Altogether, K/K^+ satisfies the assumption of Lemma 40, so by this lemma, h^+ divides h. □

Corollary 41. *$\mathbb{Q}(\zeta)$ is a CM-field.*

Proof. $\mathbb{Q}(\zeta)$ is of degree 2 over $\mathbb{Q}(\zeta + \zeta^{-1})$ which, by Lemma 8, is equal to the maximal totally real subfield of $\mathbb{Q}(\zeta)$. □

In the following, we will always let the relative class number of $\mathbb{Q}(\zeta)$ be denoted by h_p^-.

Theorem 42. (cf. [5, Theorem 5.16, page 62]) *Let p be an odd prime and let h_p^- be the relative class number of $\mathbb{Q}(\zeta)$. Then $p \mid h_p^-$ if and only if p divides the numerator of B_j for some $j \in \{2, 4, \ldots, p-3\}$.*

Proof. We follow the proof in [5, page 62]. Let $K = \mathbb{Q}(\zeta)$. Letting E denote the group of units of the ring if integers of K and W the group of roots of unity in K, as well as $Q = (E : WE^+)$, we have $Q = 1$ by Corollary 38. Furthermore, if $w := |W|$ then we have $w = 2p$, since $W = \mu_{2p}$, by Lemma 6. We will use the following result:

Theorem 43. (cf. [5, Theorem 4.17, page 43]) *Let K be a CM-field with ring of integers $\mathfrak{o}_K$, further let $E := \mathfrak{o}_K^\times$, W the group of roots of unity in K, $Q = (E : WE^+)$ and $w = |W|$. Then*

$$h_K^- = Qw \prod_{\chi \, \mathrm{odd}} (-\frac{1}{2} B_{n,\chi}), \tag{31}$$

where the product is taken over all odd characters belonging to K.

Proof. Omitted, see the explanations in [5] preceding [5, Theorem 4.17, page 43]. The proof uses analytic class number formulae. □

Remark. There is a correspondence between groups of Dirichlet characters and subfields of cyclotomic fields as explained in [5, pages 21–22]: For a group X of Dirichlet characters let n be the least common multiple of the conductors of all characters of X. Therefore, X is a subgroup of characters of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Let H be the intersection of the kernels of all characters in X and let K be the fixed field of H. Then K is called the field belonging to X. It is a general fact that X is precisely the set of characters of $\mathrm{Gal}(K/\mathbb{Q})$ and that there is a group isomorphism $X \cong \mathrm{Gal}(K/\mathbb{Q})$ (see also Lemma 26). Therefore, when we use the term "characters belonging to a field K" (where K will always be a subfield of a cyclotomic field), we mean the characters defined on $\mathrm{Gal}(K/\mathbb{Q})$.

Returning to the proof of Theorem 42, note that by Lemma 23, the set of odd characters of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is given by $\{\omega^i \mid i = 1, 3, \ldots, p-2\}$. Hence, in the case of $K = \mathbb{Q}(\zeta)$ (with $h_K^- = h_p^-$), (31) reads

$$h_p^- = 2p \prod_{\substack{j \, \mathrm{odd} \\ j=1}}^{p-2} (-\frac{1}{2} B_{1,\omega^j}). \tag{32}$$

Then since $B_{1,\omega^{p-2}} = B_{1,\omega^{-1}} \equiv (p-1)/p \bmod \mathbb{Z}_p$ (see (29)), we find that

$$\begin{aligned} 2p(-\frac{1}{2}B_{1,\omega^{p-2}}) = 2p(-\frac{1}{2}B_{1,\omega^{-1}}) &\equiv 2p(-\frac{1}{2}\frac{p-1}{p}) \bmod p \\ &= 1 - p \equiv 1 \bmod p. \end{aligned}$$

This in turn plugged into (32) yields

$$h_p^- \equiv \prod_{\substack{j \text{ odd} \\ j=1}}^{p-4} (-\frac{1}{2}B_{1,\omega^j}) \bmod p.$$

Then by Corollary 34,

$$h_p^- \equiv \prod_{\substack{j=1 \\ j \text{ odd}}}^{p-4} (-\frac{1}{2}\frac{B_{j+1}}{j+1}) \bmod p.$$

That means p divides h_p^- if and only if p divides some of the numerators of the Bernoulli numbers B_k, for $k = 2, 4, \ldots, p-3$. This completes the proof of this theorem. □

Theorem 42 tells us that if p divides some of the numerators of the Bernoulli numbers B_k, for $k = 2, 4, \ldots, p-3$, then p divides $h_p = h_p^+ h_p^-$, in other words, then p is irregular. Among other propositions, which we shall prove in the next steps, this theorem helps us to prove the result that there are infinitely many irregular primes (cf. [5, Theorem 5.17, page 62]). In order to prove this, we need to introduce the Bernoulli polynomials and to prove the *von Staudt–Clausen theorem*. We do this by methods taken from [5].

Definition 44. (cf. [5, page 31]) *The Bernoulli polynomials $B_n(X)$ are* *given by*

$$\frac{te^{Xt}}{e^t-1} = \sum_{n=0}^{\infty} B_n(X)\frac{t^n}{n!}.$$

Since the generating function of the polynomials $B_n(X)$ is the product of

$$\frac{t}{e^t-1} = \sum_{r=0}^{\infty} B_r\frac{t^r}{r!} \qquad \text{and} \qquad e^{Xt} = \sum_{s=0}^{\infty} \frac{(Xt)^s}{s!},$$

it follows easily that

$$B_n(X) = \sum_{r=0}^{n} \binom{n}{r} B_r X^{n-r}. \tag{33}$$

Indeed,

$$\begin{aligned}
\sum_{n=0}^{\infty} B_n(X)\frac{t^n}{n!} &= \frac{t}{e^t-1}e^{Xt} = (\sum_{r=0}^{\infty} B_r\frac{t^r}{r!})(\sum_{s=0}^{\infty} X^s\frac{t^s}{s!}) \\
&= \sum_{n=0}^{\infty}(\sum_{\substack{0\le r,s\le n\\ r+s=n}} \frac{1}{r!s!}B_rX^s)t^n = \sum_{n=0}^{\infty}(\sum_{\substack{0\le r,s\le n\\ r+s=n}} \frac{n!}{r!s!}B_rX^s)\frac{t^n}{n!} \\
&= \sum_{n=0}^{\infty}(\sum_{r=0}^{n}\binom{n}{r}B_rX^{n-r})\frac{t^n}{n!},
\end{aligned}$$

so (33) follows directly from comparing coefficients.

We are going to use the following result, which together with its proof can be found in [5, Proposition 4.1, page 32]. Here, χ is a Dirichlet character of conductor f and the $B_{n,\chi}$, $n \geq 0$, are the respective generalized Bernoulli numbers.

Proposition 45. *Let F be any multiple of f. Then*

$$B_{n,\chi} = F^{n-1} \sum_{a=1}^{F} \chi(a) B_n(\frac{a}{F}).$$

Proof. On the one hand, we have

$$\begin{aligned} &\sum_{n=0}^{\infty} F^{n-1} \sum_{a=1}^{F} \chi(a) B_n(\frac{a}{F}) \frac{t^n}{n!} = \sum_{n=0}^{\infty} \frac{1}{F} \sum_{a=1}^{F} \chi(a) B_n(\frac{a}{F}) \frac{(Ft)^n}{n!} \\ =&\frac{1}{F} \sum_{a=1}^{F} \chi(a) \frac{(Ft) e^{(a/F)(Ft)}}{e^{Ft}-1} = \sum_{a=1}^{F} \chi(a) \frac{te^{at}}{e^{Ft}-1}. \end{aligned} \tag{34}$$

On the other hand, if we let $g = F/f$ and write $a = b + cf$ with $1 \leq b \leq f$:

$$\begin{aligned} \sum_{a=1}^{F} \chi(a) \frac{te^{at}}{e^{Ft}-1} &= \sum_{b=1}^{f} \sum_{c=0}^{g-1} \chi(b) \frac{te^{(b+cf)t}}{e^{fgt}-1} \\ &= \sum_{b=1}^{f} \chi(b) \frac{te^{bt}}{e^{fgt}-1} \sum_{c=0}^{g-1} (e^{ft})^c \\ &= \sum_{b=1}^{f} \chi(b) \frac{te^{bt}}{e^{fgt}-1} \frac{e^{fgt}-1}{e^{ft}-1} \\ &= \sum_{b=1}^{f} \chi(b) \frac{te^{bt}}{e^{ft}-1} = \sum_{n=0}^{\infty} B_{n,\chi} \frac{t^n}{n!}. \end{aligned} \tag{35}$$

Comparing (34) and (35) leads to

$$\sum_{n=0}^{\infty} F^{n-1} \sum_{a=1}^{F} \chi(a) B_n(\frac{a}{F}) \frac{t^n}{n!} = \sum_{n=0}^{\infty} B_{n,\chi} \frac{t^n}{n!},$$

which gives us the desired result by comparing coefficients. □

We are now ready to deduce the von Staudt–Clausen theorem.

Theorem 46. (von Staudt–Clausen, cf. [5, Theorem 5.10, page 56]) *Let n be an even and positive integer. Then*

$$B_n + \sum_{(p-1)|n} \frac{1}{p} \in \mathbb{Z},$$

where the sum is over those primes p such that $p-1$ divides n (in particular, 2 and 3 appear in the denominator of each such Bernoulli number). Consequently, we have $pB_n \in \mathbb{Z}_p$ for all integers $n \geq 0$ and all primes p.

Proof. By induction on n we shall first prove the following assertions for all integers $n \geq 0$: We have $pB_n \in \mathbb{Z}_p$ for all primes p. Moreover, if n is positive and even then it also satisfies $B_n \equiv 0 \bmod \mathbb{Z}_p$ for all primes p with $(p-1) \nmid n$ and $B_n \equiv -1/p \bmod \mathbb{Z}_p$ for all primes p with $(p-1) \mid n$.

For the beginning of the induction consider the cases $n = 0$ and $n = 1$. We have $B_0 = 1 \in \mathbb{Z}_p$ for every prime p, $B_1 = -1/2 \equiv 0 \mod \mathbb{Z}_p$ for all odd primes p and $B_1 = -1/2 = -1/p$ for $p = 2$. Therefore $pB_0, pB_1 \in \mathbb{Z}_p$ for all primes p, so the beginning of the induction is done.

For the induction step, we choose an arbitrary integer $n \geq 2$ and assume that the above assertions hold for all integers m with $0 \leq m < n$ and for all primes p. We claim that the statements are also true for n and for all primes p. To show this, note first that if $n \geq 2$ is odd then we have $B_n = 0$ by Lemma 28 and hence $pB_n \in \mathbb{Z}_p$ for all primes p, so in this case our claim is true. Therefore, we assume n to be even. Applying Proposition 45 to $\chi = 1$

and $F = p$, we obtain

$$\begin{aligned} B_n = B_{n,1} &= p^{n-1}\sum_{a=1}^{p} B_n\left(\frac{a}{p}\right) \\ &\overset{(33)}{=} p^{n-1}\sum_{a=1}^{p}\sum_{r=0}^{n}\binom{n}{r}\cdot B_r\cdot\left(\frac{a}{p}\right)^{n-r} \\ &= \sum_{a=1}^{p}\sum_{r=0}^{n}\binom{n}{r} pB_r a^{n-r}p^{r-2} \\ &\equiv \sum_{a=1}^{p}(pB_0a^np^{-2} + npB_1a^{n-1}p^{-1} + pB_np^{n-2}) \bmod \mathbb{Z}_p, \end{aligned}$$

where the last congruence uses the induction hypothesis.
Since $B_1 = -1/2$, $B_1 \in \mathbb{Z}_p$ if $p \neq 2$. Since n is even, $nB_1 \in \mathbb{Z}_2$. Hence $npB_1a^{n-1}p^{-1} = nB_1a^{n-1} \in \mathbb{Z}_p$ for all primes p, and therefore we may omit the term with B_1, so

$$B_n \equiv \sum_{a=1}^{p}(pB_0a^np^{-2} + pB_np^{n-2}) = \frac{1}{p}(\sum_{a=1}^{p-1} a^n) + p^nB_n \bmod \mathbb{Z}_p,$$

where in the last step we use $B_0 = 1$ and $\sum_{a=1}^{p} B_n = pB_n$. Thus we have

$$(1-p^n)B_n \equiv \frac{1}{p}\sum_{a=1}^{p} a^n \bmod \mathbb{Z}_p. \tag{36}$$

If $(p-1) \mid n$ then $a^n \equiv 1 \bmod p\mathbb{Z}_p$ for all $a \in \{1,\ldots,p-1\}$. If $(p-1) \nmid n$ then $(\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$, $a + p\mathbb{Z}_p \mapsto a^n + p\mathbb{Z}_p$, is a bijection, so in this case we have $\sum_{a=1}^{p-1} a^n \equiv \sum_{a=1}^{p-1} a \bmod p\mathbb{Z}_p = p(p-1)/2 \equiv 0 \bmod p\mathbb{Z}_p$. Putting these into (36), we obtain

$$(1-p^n)B_n \equiv \begin{cases} \frac{p-1}{p} \bmod \mathbb{Z}_p \equiv -\frac{1}{p} \bmod \mathbb{Z}_p & \text{if } (p-1) \mid n, \\ 0 \bmod \mathbb{Z}_p & \text{if } (p-1) \nmid n. \end{cases}$$

Set $\varepsilon := -1/p$ if $(p-1) \mid n$ and $\varepsilon := 0$ else. Since $(1-p^n)B_n + \varepsilon \in \mathbb{Z}_p$ and $1 - p^n \in \mathbb{Z}_p^\times$ we get $B_n + (1-p^n)^{-1} \in \mathbb{Z}_p$. But $1 - p^n \equiv 1 \bmod p\mathbb{Z}_p$ implies $(1-p^n)^{-1} \equiv 1 \bmod p\mathbb{Z}_p$ and therefore $(1-p^n)^{-1}\varepsilon \equiv \varepsilon \bmod p\mathbb{Z}_p$, using $\varepsilon \in \{-1/p, 0\}$. Altogether, $B_n \equiv \varepsilon \bmod \mathbb{Z}_p$, concluding the induction step.

Now consider $B_n + \sum_{(p-1)|n} 1/p$. By the above, this is in $\mathbb{Z}_p$ for every p, so there are no primes in the denominator. Therefore it must be an integer. To see that 2 and 3 appear in the denominator of B_n for all positive even integers n, note that we have $1 = (2-1) \mid n$ and $2 = (3-1) \mid n$ for all such n. By the above statements agian, this implies $B_n \equiv -1/2 \bmod \mathbb{Z}_2$ and $B_n \equiv -1/3 \bmod \mathbb{Z}_3$ for all positive even integers n. This completes the proof of the theorem. □

Now we are ready to prove the above mentioned fact that there are infinitely many irregular primes. Both the statement and its proof can be found in [5, Theorem 5.17, page 62].

Theorem 47. *There are infinitely many irregular primes.*

Proof. Suppose $p_1, \ldots, p_r$ are all the irregular primes and let

$$m = N(p_1 - 1)\ldots(p_r - 1),$$

where N will be chosen later. We have $|B_n/n| \to \infty$ as $n \to \infty$, n even (cf. [5, page 62]). If we choose N large enough, then $|B_m/m| > 1$. Then there exists a prime p which divides the numerator of B_m/m. For any $i = 1, \ldots, r$, $(p_i - 1) \mid m$, so by Theorem 46, $B_m \equiv -1/p_i \bmod \mathbb{Z}_{p_i}$ for any $i = 1, \ldots, r$, meaning that for any $i = 1, \ldots, r$, p_i is in the denominator of B_m. Thus we cannot have $p = p_i$ for any i. Without loss of generality, we may assume that $p \nmid N$, since N only needs to be large enough. Therefore, we have $p \nmid m$. Also by Theorem 46, the fact that p divides the numerator of B_m implies that $(p-1) \nmid m$, in other words, $m \not\equiv 0 \bmod (p-1)$. Thus we may choose $m' \equiv m \bmod (p-1)$, $0 < m' < p-1$. Then by Corollary 33 we have

$$\frac{B_m}{m} \equiv \frac{B_{m'}}{m'} \bmod p.$$

Since p divides the numerator of B_m/m and since $p \nmid m$, this congruence implies that p divides the numerator of $B_{m'}/m'$. Due to our choice of m', p also divides the numerator of $B_{m'}$. Now we note that m' is even, because we have $m' \equiv m \bmod (p-1)$, where p may assumed to be odd. In particular, $m' \in \{2, 4, \ldots, p-3\}$. By Theorem 42, p is irregular. This is a contradiction. It follows that there are infinitely many irregular primes, as claimed. □

To prove the converse of Theorem 19, i.e. that $p \mid h_p$ implies that p divides the numerator of B_k, for some $k = 2, 4, \ldots, p-3$, we need the following extra result.

Theorem 48. (cf. [5, Theorem 5.34, page 78]) *If $p \mid h_p^+$ then $p \mid h_p^-$. Therefore, $p \mid h_p$ if and only if p divides the numerator of B_j for some $j = 2, 4, \ldots, p-3$.*

The proof of this theorem in [5, pages 78–79] uses p-adic L-functions. There is an alternative proof using class field theory but not p-adic L-functions. The goal of the following subsections is to provide this second proof. One of its essential elements is the fact that if C is the ideal class group of $\mathbb{Q}(\zeta)$ and C^+ the ideal class group of $\mathbb{Q}(\zeta)^+$, then the natural map $C^+ \to C$ is an injection. If L_1 and L_1^+ denote the (big) Hilbert class fields of $\mathbb{Q}(\zeta)$ and $\mathbb{Q}(\zeta)^+$, then there are isomorphisms $C \cong \mathrm{Gal}(L_1/\mathbb{Q}(\zeta))$ and $C^+ \cong \mathrm{Gal}(L_1^+/\mathbb{Q}(\zeta)^+)$ (cf. [4, Satz II.6.9, page 418]). Let A denote the p-Sylow subgroup of C and let A^+ denote the p-Sylow subgroup of C^+. Then $C^+ \to C$ restricts to an injection of subgroups $A^+ \to A$. Let $G = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ and $G^+ = \mathrm{Gal}(\mathbb{Q}(\zeta)^+/\mathbb{Q})$. We are going to define a Galois module structure on the p-Sylow subgroups of these two ideal class groups, as well as to construct the so called *idempotents* of $\mathbb{Z}_p[G]$ and $\mathbb{Z}_p[G^+]$, which will allow us to decompose these two modules into submodules. In particular, the injection $A^+ \to A$ turns out to be an injection of Galois modules. Using the hypothesis $p \mid h_p^+$, which implies that there are some submodules of A^+ of nonzero p-rank, we are going to prove that there are some more submodules of A which are of nonzero p-rank. From this, we get that then also h_p^- is divisible by p, which will complete the proof of Theorem 19.

4.5 Properties of the orthogonal idempotents of $\overline{\mathbb{Q}}[G]$ for a finite abelian group G

Definition 49. (cf. [5, page 100]) *Let G be a finite abelian group and G^* its character group. Let $\chi \in G^*$ and define*

$$\varepsilon_\chi = \frac{1}{|G|} \sum_{\sigma \in G} \chi(\sigma)\sigma^{-1} \in \overline{\mathbb{Q}}[G],$$

where $\overline{\mathbb{Q}}$ is the algebraic closure of $\mathbb{Q}$. The ε_χ's are called the orthogonal idempotents of the group ring $\overline{\mathbb{Q}}[G]$.

Remark. For a finite abelian group G, the trivial charcter of G will be denoted by $1 : G \to \overline{\mathbb{Q}}^\times$. It satisfies $1(\sigma) = 1$ for all $\sigma \in G$.

Lemma 50. (cf. [5, page 100]) *Let G be a finite abelian group and G^* its character group. Let $\chi \in G^*$. Then the following relations are true:*

(i) $\varepsilon_\chi^2 = \varepsilon_\chi$;

(ii) $\varepsilon_\chi \varepsilon_\psi = 0$ if $\chi \neq \psi$;

(iii) $1 = \sum_{\chi \in G^*} \varepsilon_\chi$;

(iv) $\varepsilon_\chi \sigma = \chi(\sigma)\varepsilon_\chi$ (for all $\sigma \in G$).

Proof. In the following computations, we basically use the properties of Dirichlet characters and of G as a finite abelian group. Let $\chi \in G^*$ be arbitrary.
For (i), write

$$\begin{aligned}
\varepsilon_\chi^2 &= (\frac{1}{|G|}\sum_{\sigma\in G}\chi(\sigma)\sigma^{-1})^2 \\
&= \frac{1}{|G|^2}\sum_{\sigma\in G}\sum_{\tilde\sigma\in G}(\chi(\sigma)\sigma^{-1})(\chi(\tilde\sigma)\tilde\sigma^{-1}) && \mid \sigma' := \tilde\sigma\sigma \\
&= \frac{1}{|G|^2}\sum_{\sigma\in G}\sum_{\sigma'\in G}(\chi(\sigma)\sigma^{-1})(\chi(\sigma'\sigma^{-1})(\sigma'\sigma^{-1})^{-1}) \\
&= \frac{1}{|G|^2}\sum_{\sigma\in G}\sum_{\sigma'\in G}(\chi(\sigma)\sigma^{-1})(\chi(\sigma')\chi(\sigma^{-1})\sigma(\sigma')^{-1}) \\
&= \frac{1}{|G|^2}\sum_{\sigma'\in G}\sum_{\sigma\in G}\chi(\sigma')(\sigma')^{-1} \\
&= \frac{1}{|G|}\sum_{\sigma'\in G}\chi(\sigma')(\sigma')^{-1} = \varepsilon_\chi.
\end{aligned}$$

For (ii), let $\psi \neq \chi$ be arbitrary and write

$$\begin{aligned}
\varepsilon_\chi \varepsilon_\psi &= (\frac{1}{|G|}\sum_{\sigma\in G} \chi(\sigma)\sigma^{-1})(\frac{1}{|G|}\sum_{\tilde{\sigma}\in G} \psi(\tilde{\sigma})\tilde{\sigma}^{-1}) \\
&= \frac{1}{|G|^2}\sum_{\sigma\in G}\sum_{\tilde{\sigma}\in G}(\chi(\sigma)\sigma^{-1})(\psi(\tilde{\sigma})\tilde{\sigma}^{-1}) && \mid \sigma' := \tilde{\sigma}\sigma \\
&= \frac{1}{|G|^2}\sum_{\sigma\in G}\sum_{\sigma'\in G} \chi(\sigma)\sigma^{-1}\psi(\sigma'\sigma^{-1})(\sigma'\sigma^{-1})^{-1} \\
&= \frac{1}{|G|^2}\sum_{\sigma\in G}\sum_{\sigma'\in G} \chi(\sigma)\sigma^{-1}\psi(\sigma')\psi(\sigma^{-1})(\sigma'\sigma^{-1})^{-1} \\
&= \frac{1}{|G|^2}(\sum_{\sigma\in G} \chi(\sigma)\psi(\sigma^{-1})\sigma^{-1}\sigma)(\sum_{\sigma'\in G} \psi(\sigma')(\sigma')^{-1}) \\
&= \frac{1}{|G|^2}\underbrace{(\sum_{\sigma\in G} \chi(\sigma)\psi(\sigma)^{-1})}_{=0}(\sum_{\sigma'\in G} \psi(\sigma')(\sigma')^{-1}) = 0.
\end{aligned}$$

Here $\sum_{\sigma\in G}\chi(\sigma)\psi(\sigma)^{-1} = 0$ follows from Lemma 24, since the map

$$G \to \overline{\mathbb{Q}}^\times, \quad \sigma \mapsto \chi(\sigma)\psi(\sigma)^{-1},$$

is a nontrivial Dirichlet character (due to $\chi \neq \psi$).

For (iv), let $\sigma \in G$ be arbitrary. Then

$$\begin{aligned}
\varepsilon_\chi \sigma &= \sum_{\sigma' \in G} \chi(\sigma')(\sigma')^{-1}\sigma && \mid \chi(\sigma)\chi(\sigma^{-1}) = 1 \\
&= \sum_{\sigma' \in G} \chi(\sigma)\chi(\sigma^{-1})\chi(\sigma')(\sigma')^{-1}(\sigma^{-1})^{-1} \\
&= \sum_{\sigma' \in G} \chi(\sigma)\chi(\sigma^{-1}\sigma')(\sigma')^{-1}(\sigma^{-1})^{-1} \\
&= \sum_{\sigma' \in G} \chi(\sigma)\chi(\sigma^{-1}\sigma')(\sigma^{-1}\sigma')^{-1} \\
&= \chi(\sigma) \sum_{\sigma' \in G} \chi(\sigma^{-1}\sigma')(\sigma^{-1}\sigma')^{-1} && \mid \tilde{\sigma} := \sigma^{-1}\sigma' \\
&= \chi(\sigma) \sum_{\tilde{\sigma} \in G} \chi(\tilde{\sigma})\tilde{\sigma}^{-1} = \chi(\sigma)\varepsilon_\chi,
\end{aligned}$$

as claimed in (iv).
For (iii), note that from (i) and (ii) we obtain

$$\varepsilon_\chi = \varepsilon_\chi^2 = \varepsilon_\chi \sum_{\psi \in G^*} \varepsilon_\psi.$$

Moreover, we have the following variant of Lemma 24:

Claim. *Let G be a finite abelian group. Then we have*

$$\sum_{\chi \in G^*} \chi(\rho) = \begin{cases} 0 & \text{if } \rho \neq 1, \\ |G^*| = |G| & \text{if } \rho = 1. \end{cases}$$

Proof of the claim. If $\rho = 1 \in G$ then we have

$$\sum_{\chi \in G^*} \chi(\rho) = \sum_{\chi \in G^*} 1 = |G^*| = |G|,$$

where in the last step we use Lemma 26. If $\rho \neq 1$ then the subgroup $\langle \rho \rangle$

(generated by ρ in G) is nontrivial. By (20), we have $\langle\rho\rangle^{\perp} \subsetneq G^*$, i.e. there is a $\psi \in G^*$ with $\psi(\rho) \neq 1$ (cf. (19)). If we define $\tilde{\chi} := \psi\chi$ for $\chi \in G^*$, we obtain

$$\sum_{\chi \in G^*} \chi(\rho) = \sum_{\tilde{\chi} \in G^*} \tilde{\chi}(\rho) = \sum_{\chi \in G^*} (\psi\chi)(\rho) = \sum_{\chi \in G^*} \psi(\rho)\chi(\rho) = \psi(\rho) \sum_{\chi \in G^*} \chi(\rho).$$

This implies

$$(1 - \psi(\rho)) \sum_{\chi \in G^*} \chi(\rho) = 0.$$

Since $\psi(\rho) \neq 1$, this leads to $\sum_{\chi \in G^*} \chi(\rho) = 0$, proving the claim. □

Returning to the proof of the lemma, we note that if $\sigma \in G$ is arbitrary then the above claim implies

$$\begin{aligned}(\sum_{\chi \in G^*} \varepsilon_\chi) \cdot \sigma \overset{\text{(iv)}}{=} \sum_{\chi \in G^*} \chi(\sigma)\varepsilon_\chi &= \sum_{\chi \in G^*} \frac{1}{|G|} \sum_{\tau \in G} \chi(\sigma)\chi(\tau)\tau^{-1} \\ &= \sum_{\tau \in G} \frac{1}{|G|} \sum_{\chi \in G^*} \chi(\sigma\tau)\tau^{-1} = \sigma,\end{aligned}$$

using the orthogonality relations above. Since any element of $\overline{\mathbb{Q}}[G]$ is a linear combination of σ's, this implies $\sum_{\chi \in G^*} \varepsilon_\chi = 1$, proving (iii).

This completes the proof of the lemma. □

Corollary 51. (cf. [5, page 100]) *Let G be a finite abelian group. Then the idempotents of $\overline{\mathbb{Q}}[G]$ satisfy the following relations:*

(i) *If M is a module over $\overline{\mathbb{Q}}[G]$ then we have the following decomposition into $\overline{\mathbb{Q}}[G]$-submodules:*

$$M = \bigoplus_{\chi \in G^*} M_\chi, \qquad \text{where } M_\chi = \varepsilon_\chi M;$$

(ii) *For $\chi \in G^*$, M_χ is the χ-eigenspace of the G-action on M, i.e.*

$$M_\chi = \{m \in M \mid \sigma m = \chi(\sigma) m \text{ for all } \sigma \in G\}.$$

Proof. For (i), let M be a module over $\overline{\mathbb{Q}}[G]$ and let $m \in M$ be arbitrary. Then by Lemma 50 (iii),

$$m = 1 \cdot m = \sum_{\chi \in G^*} \varepsilon_\chi m \in \sum_{\chi \in G^*} M_\chi.$$

To show that this is a direct sum, write $0 = \sum_{\chi \in G^*} \varepsilon_\chi m_\chi$, for suitable $m_\chi \in M$, $\chi \in G^*$. By Lemma 50 (i) and (ii), this condition implies $0 = \varepsilon_\psi \cdot 0 = \sum_{\chi \in G^*} \varepsilon_\psi \varepsilon_\chi m_\chi = m_\psi$ for all $\psi \in G^*$. This proves (i).

For (ii), let $\sigma \in G$, $m_\chi \in M_\chi$ be arbitrary, say $m_\chi = \varepsilon_\chi a_\chi$ for some $a_\chi \in M$. Then

$$\begin{aligned}\sigma m_\chi &\overset{\text{Lemma 50 (iii)}}{=} (\sum_{\psi \in G^*} \varepsilon_\psi) \sigma m_\chi = \sum_{\psi \in G^*} (\varepsilon_\psi \sigma)(\varepsilon_\chi a_\chi) \\ &\overset{\text{Lemma 50 (iv)}}{=} \sum_{\psi \in G^*} \psi(\sigma) \varepsilon_\psi \varepsilon_\chi a_\chi \overset{\text{Lemma 50 (i),(ii)}}{=} \chi(\sigma) \varepsilon_\chi a_\chi = \chi(\sigma) m_\chi,\end{aligned}$$

as claimed. Therefore, M_χ is contained in the χ-eigenspace.
For the reverse inclusion, let $m \in M$ be an element of the χ-eigenspace of the G-action on M, i.e. assume m to satisfy $\sigma m = \chi(\sigma) m$ for all $\sigma \in G$. Then

$$\begin{aligned}\varepsilon_\chi m &= \frac{1}{|G|} \sum_{\sigma \in G} \chi(\sigma) \sigma^{-1} m = \frac{1}{|G|} \sum_{\sigma \in G} \chi(\sigma^{-1}) \sigma m \\ &= \frac{1}{|G|} \sum_{\sigma \in G} \chi(\sigma^{-1}) \chi(\sigma) m = m,\end{aligned}$$

so $m \in \varepsilon_\chi M = M_\chi$. This proves (ii). □

Of course, all the above works if $\overline{\mathbb{Q}}$ is replaced by any (commutative) ring which contains the values of all $\chi \in G^*$ and in which $|G|$ is invertible.
In particular, let p be an odd prime and let $G = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$. Then G^* can be identified with $\{\omega^i \mid 0 \le i \le p-2\}$ (cf. Lemma 21). We shall work in the group ring $\mathbb{Z}_p[G]$. The idempotents of $\mathbb{Z}_p[G]$ are

$$\varepsilon_i = \frac{1}{p-1}\sum_{a=1}^{p-1} \omega^i(a)\sigma_a^{-1}, \qquad 0 \le i \le p-2.$$

We define ε_- and ε_+ in $\mathbb{Z}_p[G]$ by

$$\varepsilon_- = \frac{1-\sigma_{-1}}{2} \quad \text{and} \quad \varepsilon_+ = \frac{1+\sigma_{-1}}{2}.$$

Corollary 52. (cf. [5, page 100]) *The following equations hold:*

$$\varepsilon_- = \sum_{\substack{i=0 \\ i \text{ odd}}}^{p-2} \varepsilon_i \quad \text{and} \quad \varepsilon_+ = \sum_{\substack{i=0 \\ i \text{ even}}}^{p-2} \varepsilon_i.$$

Therefore, we obtain a decomposition $A = \varepsilon_- A \oplus \varepsilon_+ A$ for any $\mathbb{Z}_p[G]$-module.

Proof. By Lemma 50 (iii) and (iv), we have

$$1 = \sum_{i=0}^{p-2} \varepsilon_i = \sum_{\substack{i=0 \\ i \text{ even}}}^{p-2} \varepsilon_i + \sum_{\substack{i=0 \\ i \text{ odd}}}^{p-2} \varepsilon_i$$

and

$$\sigma_{-1} = \sum_{i=0}^{p-2} \varepsilon_i \sigma_{-1} = \sum_{i=0}^{p-2} \omega^i(-1)\varepsilon_i = \sum_{\substack{i=0 \\ i \text{ even}}}^{p-2} \varepsilon_i - \sum_{\substack{i=0 \\ i \text{ odd}}}^{p-2} \varepsilon_i.$$

Both equations together yield

$$\frac{1-\sigma_{-1}}{2} = \sum_{\substack{i=0 \\ i \text{ odd}}}^{p-2} \varepsilon_i = \varepsilon_- \qquad \text{and} \qquad \frac{1+\sigma_{-1}}{2} = \sum_{\substack{i=0 \\ i \text{ even}}}^{p-2} \varepsilon_i = \varepsilon_+,$$

as claimed. The decomposition $A = \varepsilon_- A \oplus \varepsilon_+ A$ follows immediately. □

The Stickelberger element of G is defined as $\theta = (1/p) \sum_{a=1}^{p-1} a\sigma_a^{-1} \in \mathbb{Z}_p[G]$ (cf. [5, page 93] and [5, page 100]). Using Lemma 50 (iv), we find that for any $i \in \{0, 1, \ldots, p-2\}$,

$$\begin{aligned} \varepsilon_i \theta = \varepsilon_i \left(\frac{1}{p} \sum_{a=1}^{p-1} a\sigma_a^{-1} \right) &= \frac{1}{p} \sum_{a=1}^{p-1} a(\varepsilon_i \sigma_a^{-1}) \overset{\text{Lemma 50 (iv)}}{=} \frac{1}{p} \sum_{a=1}^{p-1} a\omega^i(a^{-1})\varepsilon_i \\ &= \frac{1}{p} \sum_{a=1}^{p-1} a\omega^{-i}(a)\varepsilon_i \overset{(27)}{=} \begin{cases} B_{1,\omega^{-i}}\varepsilon_i & \text{if } i \neq 0, \\ (p-1)B_{1,\omega^{-i}}\varepsilon_i & \text{if } i = 0. \end{cases} \end{aligned} \tag{37}$$

Similarly, for $i \in \{1, \ldots, p-2\}$ and $c \in \mathbb{Z}$ with $(c, p) = 1$ we obtain

$$\begin{aligned} \varepsilon_i(c - \sigma_c)\theta = c\varepsilon_i\theta - \varepsilon_i(\sigma_c\theta) &\overset{(37)}{=} cB_{1,\omega^{-i}}\varepsilon_i - \varepsilon_i \left(\frac{1}{p} \sum_{a=1}^{p-1} a\sigma_c\sigma_a^{-1} \right) \\ &= cB_{1,\omega^{-i}}\varepsilon_i - \frac{1}{p} \sum_{a=1}^{p-1} a\varepsilon_i(\sigma_c\sigma_a^{-1}) \\ &\overset{\text{Lemma 50 (iv)}}{=} cB_{1,\omega^{-i}}\varepsilon_i - \frac{1}{p} \sum_{a=1}^{p-1} a\omega^i(c)\omega^i(a^{-1})\varepsilon_i \\ &= cB_{1,\omega^{-i}}\varepsilon_i - \omega^i(c) \left(\frac{1}{p} \sum_{a=1}^{p-1} a\omega^{-i}(a) \right) \varepsilon_i \\ &\overset{(27)}{=} cB_{1,\omega^{-i}}\varepsilon_i - \omega^i(c)B_{1,\omega^{-i}}\varepsilon_i = (c - \omega^i(c))B_{1,\omega^{-i}}\varepsilon_i. \end{aligned} \tag{38}$$

For the above application of (27) note that ω^i is nontrivial and has conductor p for all $i \in \{1, \ldots, p-2\}$.

In the case of $i = 0$ and $c \in \mathbb{Z}$ with $(c, p) = 1$ we obtain

$$\begin{aligned}\varepsilon_i(c - \sigma_c)\theta &\overset{(37)}{=} (p-1)cB_{1,\omega^{-i}}\varepsilon_i - \varepsilon_i \left(\frac{1}{p} \sum_{a=1}^{p-1} a\sigma_c\sigma_a^{-1} \right) \\ &\overset{(38)}{=} (p-1)cB_{1,\omega^{-i}}\varepsilon_i - \omega^i(c) \left(\frac{1}{p} \sum_{a=1}^{p-1} a\omega^{-i}(a) \right) \varepsilon_i \\ &\overset{(27)}{=} (p-1)cB_{1,\omega^{-i}}\varepsilon_i - \omega^i(c)(p-1)B_{1,\omega^{-i}}\varepsilon_i \\ &= (p-1)(c - \omega^i(c))B_{1,\omega^{-i}}\varepsilon_i, \end{aligned} \tag{39}$$

where we use that ω^i is trivial.

Let A be the p-Sylow subgroup of the ideal class group of $K = \mathbb{Q}(\zeta)$. Since $A^{p^n} = 1$ for sufficiently large n, we make A into a $\mathbb{Z}_p$-module via scalar restriction along the ring homomorphism $\mathbb{Z}_p \twoheadrightarrow \mathbb{Z}/p^n\mathbb{Z}$. G also acts on A, so A is a $\mathbb{Z}_p[G]$-module. Note that a combination $\sum_{a=1}^{p-1} r_a\sigma_a \in \mathbb{Z}_p[G]$ of elements of G over $\mathbb{Z}_p$ acts on $x \in A$ by

$$(\sum_{a=1}^{p-1} r_a\sigma_a)(x) = \prod_{a=1}^{p-1} \sigma_a(x)^{r_a},$$

because we write A multiplicatively. Let

$$A = \bigoplus_{i=0}^{p-2} A_i$$

be the decomposition in Corollary 51 (i), where we set $A_i := A_{\omega^i} = \varepsilon_i A$. Stickelberger's theorem implies that $(c - \sigma_c)\theta$ annihilates A (see [5, Theorem 6.10, page 94] and [5, page 101]), hence each A_i. Therefore the chains of equations (38) and (39) imply the following: Let $c \in \mathbb{Z}$, $(c, p) = 1$ and $0 \le i \le p-2$. Then $(c - \omega^i(c))B_{1,\omega^{-i}}$ annihilates A_i.

If $i \neq 0$ is even, then by Lemma 29, $B_{1,\omega^{-i}} = 0$, so the above claim that $(c - \omega^i(c))B_{1,\omega^{-i}}$ annihilates A_i actually says nothing.
If $i = 0$ then (39) gives

$$\varepsilon_i(c - \sigma_c)\theta \overset{(39)}{=} (p-1)(c - \omega^i(c))B_{1,\omega^{-i}}\varepsilon_i = (p-1)\frac{c-1}{2}\varepsilon_0.$$

Note that this works for all $c \in \mathbb{Z}$ with $(c, p) = 1$. Taking $c = p + 2$ we get that A_0 is annihilated by $(p+1)(p-1)/2$ which is a unit in $\mathbb{Z}_p$. Multiplying with the inverse we get $A_0 = 1$.

Let i be odd. First consider the case $i = 1$. Let $c = 1 + p$. Since ω^{-1} is nontrivial and of conductor p, we may apply (38) and obtain

$$\begin{aligned}\varepsilon_i(c - \sigma_c)\theta &\overset{(38)}{=} (c - \omega^i(c))B_{1,\omega^{-i}}\varepsilon_i = (c - \omega(c))B_{1,\omega^{-1}}\varepsilon_i \\ &= pB_{1,\omega^{-1}}\varepsilon_i \overset{(27)}{=} (\sum_{a=1}^{p-1} a\omega^{-1}(a))\varepsilon_i.\end{aligned}$$

Note that

$$\sum_{a=1}^{p-1} a\omega^{-1}(a) \equiv p - 1 \not\equiv 0 \bmod p.$$

Since A_1 is a p-group, the fact that $\sum_{a=1}^{p-1} a\omega^{-1}(a)$ annihilates A_1 requires $A_1 = 1$.
Now consider the case of $i \neq 1$. Since $\mathbb{F}_p^\times$ is cyclic, we may choose a $c \in \mathbb{Z}$ such that $c + p\mathbb{Z}$ generates $\mathbb{F}_p^\times$. Since $i \neq 1$, we have

$$c \not\equiv c^i \equiv \omega^i(c) \bmod p, \quad \text{respectively} \quad c - \omega^i(c) \not\equiv 0 \bmod p,$$

both congruences viewed in $\mathbb{Z}_p$. Therefore, $c - \omega^i(c) \in \mathbb{Z}_p^\times$ and together with $(c - \omega^i(c))B_{1,\omega^{-i}}$ also $B_{1,\omega^{-i}}$ annihilates A_i. Thus, we have proved:

Proposition 53. (cf. [5, Proposition 6.16, page 101]) $A_0 = A_1 = 1$. *For* $i = 3, 5, \ldots, p-2$ *odd,* $B_{1,\omega^{-i}}$ *annihilates* A_i. □

Suppose $A_i \neq 1$ for $3 \leq i \leq p-2$ odd. Then we must have $B_{1,\omega^{-i}} \equiv 0 \bmod p$. Note that we have

$$B_{1,\omega^{-i}}, \frac{B_{1-i}}{1-i} \in \mathbb{Z}_p \quad \text{and} \quad B_{1,\omega^{-i}} \equiv \frac{B_{1-i}}{1-i} \bmod p$$

by Corollary 34. Since $1 - i \equiv p - i \not\equiv 0 \bmod (p-1)$, Corollary 33 gives

$$\frac{B_{1-i}}{1-i}, \frac{B_{p-i}}{p-i} \in \mathbb{Z}_p \quad \text{and} \quad \frac{B_{1-i}}{1-i} \equiv \frac{B_{p-i}}{p-i} \bmod p.$$

Together with $B_{1,\omega^{-i}} \equiv 0 \bmod p$, these relations imply

$$\frac{B_{1-i}}{1-i}, \frac{B_{p-i}}{p-i} \in \mathbb{Z}_p \quad \text{and} \quad \frac{B_{p-i}}{p-i} \equiv 0 \bmod p,$$

i.e. p divides the numerator of B_{p-i}. Thus we have proved the following:

Theorem 54. (Herbrand) (cf. [5, Theorem 6.17, page 101])
Let i *be odd,* $3 \leq i \leq p-2$. *If* $A_i \neq 1$ *then* $p \mid B_{p-i}$. □

Remark. In particular, Theorem 54 says that for any odd $3 \leq i \leq p-2$, $A_i \neq 1$ implies $p \mid h_p^-$, using Theorem 42.

4.6 The Galois module structure of the p-Sylow subgroups of the ideal class groups of $\mathbb{Q}(\zeta)$ and $\mathbb{Q}(\zeta)^+$

Let $G = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ and $G^+ = \mathrm{Gal}(\mathbb{Q}(\zeta)^+/\mathbb{Q})$. Let C and C^+ denote the ideal class group of $\mathbb{Q}(\zeta)$ respectively $\mathbb{Q}(\zeta)^+$. Let A be the p-Sylow subgroup of C and A^+ the p-Sylow subgroup of C^+.

Remark. Let $K = \mathbb{Q}(\zeta)$ and $K^+ = \mathbb{Q}(\zeta)^+$. Recall that if $\mathfrak{a} \subseteq K^+$ is a fractional ideal then so is $\mathfrak{a}\mathfrak{o}_K \subseteq K$ (the $\mathfrak{o}_K$-submodule of K generated by $\mathfrak{a}$). This defines a group homomorphism from fractional ideals in K^+ to fractional ideals in K. Obviously, it maps principal ideals to principal ideals, hence induces a group homomorphism $C^+ \to C$.

We now state a special result about cyclotomic fields, which together with a proof can be found in [5, Theorem 4.14, pages 40–41]:

Proposition 55. *Let $K = \mathbb{Q}(\zeta)$ and $K^+ = \mathbb{Q}(\zeta)^+$. Moreover, let C be the ideal class group of K and C^+ the ideal class group of the maximal totally real subfield K^+. Then the natural map $C^+ \to C$ is an injection.*

Proof. Suppose I is a fractional ideal of K^+ which becomes a principal ideal J in K. We must show I was principal to begin with. Write $J = \alpha\mathfrak{o}_K$ with $\alpha \in K$. Note that $\mathrm{Gal}(K/\mathbb{Q})$ acts on fractional ideals of K via $\sigma(\mathfrak{a}) = \{\sigma(x) \mid x \in \mathfrak{a}\}$. This preserves the group structure. Moreover, $\overline{\mathfrak{a}} := \sigma_{-1}(\mathfrak{a})$. We have

$$\overline{J} = \sigma_{-1}(I\mathfrak{o}_K) = \sigma_{-1}(I)\sigma_{-1}(\mathfrak{o}_K) = I\mathfrak{o}_K = J$$

because σ_{-1} fixes K^+. This implies

$$(\overline{\alpha}/\alpha)\mathfrak{o}_K = (\overline{\alpha}\mathfrak{o}_K)(\alpha\mathfrak{o}_K)^{-1} = \overline{J}J^{-1} = JJ^{-1} = 1 \cdot \mathfrak{o}_K.$$

Hence $\overline{\alpha}/\alpha$ is a unit (of $\mathfrak{o}_K$) and has absolute value 1. By Lemma 36 and Corollary 41, $\overline{\alpha}/\alpha$ is a root of unity. Let $\pi = \zeta - 1$. We have

$$\frac{\pi}{\overline{\pi}} = \frac{\zeta - 1}{\zeta^{-1} - 1} = \frac{\zeta^2 - \zeta}{1 - \zeta} = \frac{(-\zeta)(\zeta - 1)}{\zeta - 1} = -\zeta.$$

By Lemma 6, $-\zeta$ generates the group of roots of unity in K. Therefore, $\overline{\alpha}/\alpha = (\pi/\overline{\pi})^d$ for some d. Then $\overline{\alpha\pi^d} = \alpha\pi^d$. Since the π-adic valuation takes only even values on K^+ and since both $\alpha\pi^d$ and J are real,

$$d = v_\pi(\pi^d) = v_\pi(\frac{\alpha\pi^d}{\alpha}) = v_\pi(\alpha\pi^d) - v_\pi(\alpha) = v_\pi(\alpha\pi^d) - v_\pi(J)$$

is even. Hence $\overline{\alpha}/\alpha = (-\zeta)^d \in W^2$. In particular, $\overline{\alpha}/\alpha = \zeta_0^2$ for some primitive pth root of unity ζ_0, and

$$\frac{\overline{\alpha}}{\alpha} = \zeta_0^2 = \frac{\zeta_0}{\zeta_0^{-1}} = \frac{\zeta_0}{\overline{\zeta_0}},$$

so

$$\overline{\alpha}\overline{\zeta_0} = \alpha\zeta_0$$

is a real number. Since ζ_0 is a unit in $\mathfrak{o}_K$, we have $J = \alpha\mathfrak{o}_K = \alpha\zeta_0\mathfrak{o}_K$ with $\alpha\zeta_0 \in \mathbb{R}$. Consider the prime decompositions

$$I = \prod_{\mathfrak{p}} \mathfrak{p}^{n_\mathfrak{p}} \quad \text{and} \quad \alpha\zeta_0\mathfrak{o}_{K^+} = \prod_{\mathfrak{p}} \mathfrak{p}^{m_\mathfrak{p}}$$

of fractional ideals of K^+. Then

$$I\mathfrak{o}_K = \prod_{\mathfrak{p}} \prod_{\mathfrak{q}|\mathfrak{p}} \mathfrak{q}^{e(\mathfrak{q}/\mathfrak{p})n_\mathfrak{p}} \quad \text{and} \quad \alpha\zeta_0\mathfrak{o}_K = \prod_{\mathfrak{p}} \prod_{\mathfrak{q}|\mathfrak{p}} \mathfrak{q}^{e(\mathfrak{q}/\mathfrak{p})m_\mathfrak{p}}.$$

Since $I\mathfrak{o}_K = J = \alpha\zeta_0\mathfrak{o}_K$, the uniqueness of prime decomposition of fractional ideals of K (together with $e(\mathfrak{q}/\mathfrak{p}) \geq 1$) implies $m_\mathfrak{p} = n_\mathfrak{p}$ for all $\mathfrak{p}$ and hence $I = \alpha\zeta_0\mathfrak{o}_{K^+}$ is principal. This completes the proof. □

Lemma 56. *The orthogonal idempotents of* $\mathbb{Z}_p[G^+]$ *are given by*

$$\varepsilon_i^+ = \frac{1}{p-1}\sum_{a=1}^{p-1} \omega^i(a)\sigma_a^{-1},\ i\ = 0, 2, \ldots, p-3 \text{ even},$$

so they can be identified with the idempotents ε_i, $i = 0, 2, \ldots, p-3$ even, of $\mathbb{Z}_p[G]$.

Proof. By Lemma 25, the set of characters belonging to $\mathbb{Q}(\zeta)^+$ can be identified with $\{\omega^i \mid 0 \leq i \leq p-2 \,\text{even}\}$. For each $i \in \{0, 2 \ldots, p-3\}$ even and $a \in \{1, \ldots, (p-1)/2\}$, $\omega^i(a) = \omega^i(p-a)$. Also $|\mathrm{Gal}(\mathbb{Q}(\zeta)^+/\mathbb{Q})| = (p-1)/2$, and for each $a \in \{1, \ldots, (p-1)/2\}$, the restrictions of σ_a and σ_{p-a} to $\mathbb{Q}(\zeta)^+$ are equal. Altogether, we find that for each even $i \in \{0, 2, \ldots, p-3\}$,

$$\varepsilon_i^+ = \frac{2}{p-1} \sum_{a=1}^{(p-1)/2} \omega^i(a)\sigma_a^{-1} = \frac{1}{p-1} \sum_{a=1}^{p-1} \omega^i(a)\sigma_a^{-1} = \varepsilon_i$$

as claimed. □

In the following, we will denote the idempotents of $\mathbb{Z}_p[G^+]$ by ε_i, where $i \in \{0, 2, \ldots, p-3\}$ is even.

The map $C^+ \to C$ defined at the beginning of this subsection is an injective group homomorphism. Therefore, it induces an injective group homomorphism of p-Sylow subgroups $A^+ \to A$. Since G^+ is a quotient of G, we may regard A^+ as a $\mathbb{Z}_p[G]$-module, where the elements of G act on A^+ by restriction. Hence $A^+ \to A$ may be viewed as a homomorphism of $\mathbb{Z}_p[G]$-modules. Using Lemma 56, we find that for each $i \in \{0, 2, \ldots, p-3\}$ even, this map $A^+ \to A$ sends $\varepsilon_i A^+$ to $\varepsilon_i A$. Also, A^+ is isomorphic to a subgroup of $\varepsilon_+ A$, the "even" part of the above decomposition $A = \varepsilon_+ A \oplus \varepsilon_- A$ of A (see Corollary 52).

If $p \mid h_p^+$ then there is a subgroup $\varepsilon_i A^+ \subseteq A^+$ ($i = 0, 2, \ldots, p-3$ even) of nonzero p-rank. By the injection

$$A_i^+ := \varepsilon_i A^+ \to \varepsilon_i A = A_i,$$

A_i is of nonzero p-rank. We claim that in this case there is some $j = 1, 3, \ldots, p-2$, odd, such that also A_j is of positive p-rank. By this claim we will obtain $p \mid h_p^-$, as we shall discuss at the end of this thesis. The goal of this subsection is the following theorem, which can be found together with a proof in [5, Theorem 10.9, pages 189–191]:

Theorem 57. *Let A be the p-Sylow subgroup of the ideal class group of $\mathbb{Q}(\zeta)$ and let*

$$A = \bigoplus_{i=0}^{p-2} \varepsilon_i A$$

be the direct sum decomposition corresponding to the idempotents of the group ring $\mathbb{Z}_p[G]$. Let i be even and j odd with $i + j \equiv 1 \bmod (p-1)$. Then

$$p\text{-rank}(\varepsilon_i A) \leq p\text{-rank}(\varepsilon_j A).$$

For the proof, we need some preparation. The underlying material can be found in [5, 10.2, pages 188–189]. Let p be an odd prime and let L/K be a Galois extension with $\mathrm{Gal}(L/K) =: G$. We assume that $\zeta \in L$. Note that by our original definition, $G = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, so here we make an abuse of notation, since we are going to treat the special case of $L = \mathbb{Q}(\zeta)$ and $K = \mathbb{Q}$. Let L' be the maximal unramified elementary abelian p-extension of L. Then $H = \mathrm{Gal}(L'/L) \cong A/A^p$, where A is the p-Sylow subgroup of the ideal class group of L. To see the last isomorphism, let L_1 be the p-Hilbert class field of L. We may write $A \cong \mathrm{Gal}(L_1/L) \cong \mathbb{Z}/p^{n_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{n_r}\mathbb{Z}$ for some $r \geq 1$ and some $n_1, \ldots, n_r \geq 1$. Since $\prod_{i=1}^r \mathbb{Z}/p\mathbb{Z}$ is the maximal elementary

p-abelian quotient of $\prod_{i=1}^{r} \mathbb{Z}/p^{n_i}\mathbb{Z}$, we obtain

$$\begin{aligned} H = \operatorname{Gal}(L'/L) &\cong \prod_{i=1}^{r} \mathbb{Z}/p\mathbb{Z} \\ &\cong (\mathbb{Z}/p^{n_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{n_r}\mathbb{Z})/p(\mathbb{Z}/p^{n_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{n_r}\mathbb{Z}) \\ &\cong \operatorname{Gal}(L_1/L)/(\operatorname{Gal}(L_1/L))^p \cong A/A^p. \end{aligned}$$

We claim that L'/K is Galois and that H is a normal subgroup of $\operatorname{Gal}(L'/K)$. L'/K is separable due to the separability of L'/L and L/K. To see the normality of L'/K, let $\sigma : L' \to \mathbb{C}$ be a K-linear embedding of L'. Since L'/L is unramified, $\sigma(L')/\sigma(L)$ is also unramified. Due to the normality of L/K, $\sigma(L) = L$, so $\sigma(L')/L$ is unramified. By the maximality of L', $\sigma(L') \subseteq L'$, so L'/K is normal and H is a normal subgroup of $\operatorname{Gal}(L'/K)$. Note that G acts on H by $h^g = \tilde{g}h\tilde{g}^{-1}$, where $g \in G$ and $\tilde{g}$ is an arbitrary extension of g to L'. This action is well-defined, since it does not depend on the choice of $\tilde{g}$. Indeed, let $\tilde{g_1}$ and $\tilde{g_2}$ be two extensions of g to L'. Then for any $x \in L$,

$$(\tilde{g_2}^{-1}\tilde{g_1})(x) = g^{-1}(g(x)) = x,$$

so $\tilde{g_2}^{-1}\tilde{g_1} \in H$. Since H is abelian, we obtain

$$\tilde{g_2}^{-1}\tilde{g_1}h = h\tilde{g_2}^{-1}\tilde{g_1} \Leftrightarrow \tilde{g_1}h\tilde{g_1}^{-1} = \tilde{g_2}h\tilde{g_2}^{-1},$$

as claimed. Moreover, for any extension $\tilde{g}$ of $g \in G$ to L', $\tilde{g}h\tilde{g}^{-1} \in H$. This is true, because for any $x \in L$, we have $\tilde{g}^{-1}(x) = g^{-1}(x) \in L$, and therefore,

$$(\tilde{g}h\tilde{g}^{-1})(x) = \tilde{g}h(g^{-1}(x)) = \tilde{g}(g^{-1}(x)) = g(g^{-1}(x)) = x,$$

so $\tilde{g}h\tilde{g}^{-1} \in H$, as claimed. Thus H becomes a $\mathbb{Z}[G]$-module via conjugation as above. $\mathbb{Z}[G]$ also acts on A/A^p and in fact

$$H \cong A/A^p \qquad \text{as } \mathbb{Z}[G]\text{-modules}$$

(cf. [5, page 188] and [5, page 399]).

Since $H \cong \mathbb{Z}/p\mathbb{Z} \times \cdots \times \mathbb{Z}/p\mathbb{Z}$, each $\sigma \in H$ satisfies $\sigma^p = 1$, where H is written multiplicatively. In other words, L'/L is an abelian extension of exponent p. Also, L' contains a primitive pth root of unity. By [1, 4.9, Theorem 3, pages 209–210], there is a subgroup $C \subseteq L^\times$ with $(L^\times)^p \subseteq C$ and $L' = L(C^{1/p})$, in other words, L'/L is a Kummer extension. Let $B := C/(L^\times)^p$. There is a bilinear, nondegenerate pairing

$$H \times B \to \mu_p, \qquad \langle h, b\rangle = \frac{h(b^{1/p})}{b^{1/p}},$$

as can be checked using [1, 4.9, Satz 1, page 207] and the preceding statements. By [1, 4.9, Satz 1, page 207], there is an isomorphism $B \cong H^*$ and by Lemma 26, there is an isomorphism $H^* \cong H$, so altogether, we obtain

$$B \cong H^* \cong H \cong A/A^p \tag{40}$$

as abelian groups.

There is also a well-defiend action of G on B, given by

$$G \times B \to B,\ (g, b) \mapsto b^g := g(\tilde{b}) \bmod (L^\times)^p,$$

where $\tilde{b} \in L^\times$ with $\tilde{b} \bmod (L^\times)^p = b$ is an arbitrary representative of b. To see that this is well-defined, let $b_1, b_2 \in L^\times$ with $b_1 \equiv b_2 \bmod (L^\times)^p$, that means there is some $a \in L^\times$ such that $b_2 = a^p b_1$. Then we obtain

$$g(b_2) = g(a^p b_1) = g(a)^p g(b_1) \equiv g(b_1) \bmod (L^\times)^p,$$

so the above action is well-defined, as claimed.

Let $g \in G$, $b \in B$ be arbitrary. For g choose an arbitrary extension $\tilde{g} \in \mathrm{Gal}(L'/K)$ and let i be such that $\tilde{g}(b^{1/p}) = \zeta^i g(b)^{1/p}$. Noting that $\tilde{g}h\tilde{g}^{-1} \in H$ and $\langle h, b\rangle \in L$, we obtain

$$\begin{aligned}\langle h^g, b^g\rangle &= \frac{(\tilde{g}h\tilde{g}^{-1})(g(b)^{1/p})}{g(b)^{1/p}} = \frac{(\tilde{g}h\tilde{g}^{-1})(\zeta^{-i}\tilde{g}(b^{1/p}))}{\zeta^{-i}\tilde{g}(b^{1/p})} \\ &= \frac{\zeta^{-i}(\tilde{g}h\tilde{g}^{-1})(\tilde{g}(b^{1/p}))}{\zeta^{-i}\tilde{g}(b^{1/p})} = \frac{\tilde{g}h(b^{1/p})}{\tilde{g}(b^{1/p})} = \tilde{g}(\frac{h(b^{1/p})}{b^{1/p}}) = \langle h, b\rangle^g. \qquad (41)\end{aligned}$$

Let $b \in B$ (or more accurately $b \bmod (L^\times)^p \in B$). Since L'/L is unramified, so is $L(b^{1/p})/L$. We claim that there is a fractional ideal I of L such that $(b) = I^p$. To see this, let $\mathfrak{p}$ be a maximal ideal of $\mathfrak{o}_L$ and $\mathfrak{q} \subseteq \mathfrak{o}_{L(b^{1/p})}$ a prime ideal lying above $\mathfrak{p}$. Since $L(b^{1/p})/L$ is unramified, we have $v_\mathfrak{q}|_L = v_\mathfrak{p}$ and thus $v_\mathfrak{p}(b) = v_\mathfrak{q}(b) = p \cdot v_\mathfrak{q}(b^{1/p}) \in p\mathbb{Z}$. Therefore,

$$I := \prod_{\mathfrak{p}} \mathfrak{p}^{v_\mathfrak{p}(b)/p}$$

is a well-defined fractional ideal of L with

$$I^p = \prod_{\mathfrak{p}} \mathfrak{p}^{v_\mathfrak{p}(b)} = (b).$$

For any fractional ideal J we denote by $[J]$ its ideal class. Note first that if we choose a different representative $b' = bc$ of $b \in C/(L^\times)^p$, i.e. $c \in (L^\times)^p$, then the corresponding fractional ideal is $I' = I \cdot (c^{1/p})$ where $c^{1/p} \in L$. Thus, $[I'] = [I \cdot (c^{1/p})] = [I]$. Moreover, $[I]^p = [I^p] = [b] = 1$ in the ideal class group of L. This implies that the order of $[I]$ divides p. Consequently, $[I]$ is contained in the p-Sylow subgroup A and even in $A_p := \{x \in A \mid x^p = 1\}$. Altogether, we obatin a well-defined map $\phi : B \to A_p$, $b \mapsto [I]$, which is a group homomorphism by the properties of the valuations $v_\mathfrak{p}$. Let $g \in G$ be arbitrary. Then applying g to the equation $I^p = (b)$ gives $g(I)^p = g(I^p) = g((b)) = (g(b))$, so ϕ sends $g(b)$ to $[g(I)]$. Since $g \in G$ and $b \in B$ are arbitrary, ϕ is G-linear, i.e. for all $g \in G$, $b \in B$ we have $\phi(b^g) = \phi(b)^g$.

To describe the kernel of ϕ, let $b \in B$ such that $\phi(b) = 1$. Using the above definitions and notations, we write $\phi(b) = [I]$, where the fractional ideal I satisfies $(b) = I^p$. Then I is principal, say $I = (a)$ for some $a \in L^\times$. From this we find that $(b) = (a)^p = (a^p)$, i.e. we have $b = \varepsilon a^p$ for some $\varepsilon \in \mathfrak{o}_L^\times =: E$. Since $b \in \ker(\phi)$ is arbitrary, this implies that the kernel of ϕ is isomorphic to a subgroup of $E(L^\times)^p/(L^\times)^p$. By general facts from algebra, we obtain

$$\ker(\phi) \subseteq E(L^\times)^p/(L^\times)^p \cong E/E^p,$$

where the last isomorphism is G-linear.

To summarize, we have

$$\begin{aligned} &B \cong A/A^p, \quad \text{non-}G\text{-linearly,} \\ &\phi : B \to A_p, \quad G\text{-linearly, and} \\ &\ker\phi \cong \text{subgroup of } E/E^p, \quad G\text{-linearly.} \end{aligned}$$

As said above, we consider the case of $L = \mathbb{Q}(\zeta)$ and $K = \mathbb{Q}$, so $E = \mathbb{Z}[\zeta]^\times$ and $G = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. Furthermore, for any $N \geq 1$, let $E_{p^N} = E/E^{p^N}$.

Lemma 58. (cf. [5, page 153]) *For any $N \geq 1$,*

$$E/E^{p^N} \cong \mathbb{Z}/p\mathbb{Z} \times (\mathbb{Z}/p^N\mathbb{Z})^{(p-3)/2}$$

as abelian groups.

Proof. The group of roots of unity in $\mathbb{Q}(\zeta)$ is equal to the group of $(2p)$th roots of unity, denoted μ_{2p} (see Lemma 6). It is isomorphic to $\mathbb{Z}/2p\mathbb{Z}$. Let $E = \mathfrak{o}_L^\times$, where $L = \mathbb{Q}(\zeta)$. By Dirichlet's Unit Theorem, we have $\mathfrak{o}_L^\times \cong \mu_{2p} \times \mathbb{Z}^{r+s-1}$, where r is the number of real embeddings of L into $\mathbb{C}$ and s is the number of pairs of complex conjugate, nonreal embeddings of L into $\mathbb{C}$. Since the real numbers do not contain any primitive pth roots of unity (as $p \neq 2$), we have $r = 0$. From $p - 1 = [L : \mathbb{Q}] = r + 2s$, it follows that $s = (p-1)/2$. Altogether, we obtain $E \cong \mathbb{Z}/2p\mathbb{Z} \times \mathbb{Z}^{(p-3)/2}$, where the group on the left hand side of this isomorphism is understood as multiplicative, whereas the group on the right hand side is interpreted as an additive group. Then by elementary facts from algebra,

$$\begin{aligned} E/E^{p^N} &\cong (\mathbb{Z}/2p\mathbb{Z} \times \mathbb{Z}^{(p-3)/2})/p^N(\mathbb{Z}/2p\mathbb{Z} \times \mathbb{Z}^{(p-3)/2}) \\ &\cong (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}^{(p-3)/2})/p^N(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}^{(p-3)/2}) \\ &\cong (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}^{(p-3)/2})/(\mathbb{Z}/2\mathbb{Z} \times 0 \times p^N\mathbb{Z}^{(p-3)/2}) \\ &\cong 0 \times \mathbb{Z}/p\mathbb{Z} \times (\mathbb{Z}/p^N\mathbb{Z})^{(p-3)/2} \cong \mathbb{Z}/p\mathbb{Z} \times (\mathbb{Z}/p^N\mathbb{Z})^{(p-3)/2}. \end{aligned}$$

Note that $p^N(\mathbb{Z}/p\mathbb{Z}) \cong 0$ and $p^N(\mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$ for all positive integers N, where we use that p is odd, hence is a unit in $\mathbb{Z}/2\mathbb{Z}$. □

In order to study the action of $\mathbb{Z}_p[G]$ on E_{p^N}, let $\eta \in E_{p^N}$ and $a \in \mathbb{Z}_p$. Then there exists an $a_0 \in \mathbb{Z}$ such that $a \equiv a_0 \bmod p^N$. Since η is of order p^N, the action $\eta^a := \eta^{a_0}$ is well-defined (as it does not depend on the choice of the representative a_0), and gives E_{p^N} the structure of a $\mathbb{Z}_p$-module. Any $\sigma_a \in G$ may be reduced to an automorphism $\overline{\sigma_a}$ on E_{p^N}: Indeed, let $x, y \in E$ such that there is an $\alpha \in E$ with $y = \alpha^{p^N} x$. Then $\sigma_a(y) = \sigma_a(\alpha)^{p^N}\sigma_a(x)$, so $\overline{\sigma_a}(x) := \sigma_a(x) \bmod E^{p^N}$ is well-defined. Let $\tilde{\eta}$ be some representative of the above η. Then $\eta^{\overline{\sigma_a}} := \tilde{\eta}^{\sigma_a} \bmod E^{p^N} := \sigma_a(\tilde{\eta}) \bmod E^{p^N}$ is well-defined (it may be denoted by $\overline{\sigma_a}(\eta)$). This way we obtain a well-defined action of $\mathbb{Z}_p[G]$ on E_{p^N}. As a consequence, we obtain a decomposition as in Subsection 4.5:

$$E_{p^N} = \bigoplus_{i=0}^{p-2} \varepsilon_i E_{p^N}. \tag{42}$$

Before we analyze each summand, we need to have another look at how $\mathbb{Z}_p[G]$ acts on μ_p, the set of pth roots of unity (respectively on any cyclic group of order p). So let $z \in \mu_p$. It is known that $\mathrm{Gal}(\mathbb{Q}_p(\zeta)/\mathbb{Q}_p) \cong (\mathbb{Z}/p\mathbb{Z})^\times$. Let χ be the isomorphism

$$\chi : \mathrm{Gal}(\mathbb{Q}_p(\zeta)/\mathbb{Q}_p) \to (\mathbb{Z}/p\mathbb{Z})^\times, (\sigma_a : \zeta \mapsto \zeta^a) \mapsto a + p\mathbb{Z}.$$

Then we have

$$\sigma_a(z) =: z^{\sigma_a} = z^{\chi(\sigma_a)} = z^{a+p\mathbb{Z}} := z^a. \tag{43}$$

This is well-defined, since it does not depend on the choice of the representative a, due to the definition of z as a pth root of unity.
Furthermore, we have the isomorphism $(\mathbb{Z}/p\mathbb{Z})^\times \xrightarrow{\sim} \mu_{p-1}$, sending $a + p\mathbb{Z}$ to its corresponding $(p-1)$st root of unity $\omega(a) \in \mathbb{Z}_p^\times$ with $\omega(a) \equiv a \bmod p\mathbb{Z}_p$. Define

$$z^{\omega(a)} := z^{\omega(a) \bmod p} = z^{a+p\mathbb{Z}} = z^a, \tag{44}$$

which is well-defined, as it also does not depend on the choice of the representative a. Comparing (43) and (44), we obtain that for any pth root of unity $z \in \mu_p$,

$$z^{\omega(a)} = z^a = z^{\sigma_a}. \tag{45}$$

We write $\varepsilon_i E_{p^N}$ and $(E_{p^N})^{\varepsilon_i}$, synonymously, depending on whether we write E_{p^N} additively or multiplicatively.

To analyze each summand in (42), suppose first $i = 0$. Then

$$\varepsilon_i = \varepsilon_0 = \frac{1}{p-1}\sum_{a=1}^{p-1} \omega^0(a)\sigma_a^{-1} = \frac{1}{p-1}\sum_{a=1}^{p-1} \sigma_a^{-1} = \frac{1}{p-1}\sum_{a=1}^{p-1} \sigma_a,$$

so for each $x \in E$,

$$x^{(p-1)\varepsilon_0} = x^{\sum_{a=1}^{p-1}\sigma_a} = \prod_{a=1}^{p-1} \sigma_a(x) = N(x) \in \mathbb{Z}^\times = \{\pm 1\}.$$

Since $-1 \in E^{p^N}$ for all $N \geq 1$, $\varepsilon_0 x \equiv 1 \bmod E^{p^N}$ for all $x \in E$. Moreover, multiplication by $p-1$ is bijective on the p-group E_{p^N}. This implies that $\varepsilon_0 E_{p^N} = 1$ is trivial.

Next, let i be arbitrary. Let $\eta \in E$, so $\eta = \zeta^r \eta_0$, where $r \in \mathbb{Z}$ and $\overline{\eta_0} = \eta_0$ is real, using Lemma 10. By (45), $(\zeta^{-1})^{\omega(a)} = (\zeta^{-1})^a = (\zeta^{-1})^{\sigma_a}$, so

$$\begin{aligned}(\zeta^{-1})^{(p-1)\varepsilon_1} &= (\zeta^{-1})^{\sum_{a=1}^{p-1}\omega(a)\sigma_a^{-1}} = \prod_{a=1}^{p-1} (\zeta^{-\omega(a)})^{a^{-1}} \\ &= \prod_{a=1}^{p-1} (\zeta^{-a})^{a^{-1}} = \zeta^{-(p-1)} = \zeta.\end{aligned}$$

Thus $\zeta \in (p-1)\varepsilon_1 E_{p^N} = \varepsilon_1 E_{p^N}$, and $\langle\zeta\rangle \subseteq \varepsilon_1 E_{p^N}$. Now consider the real unit η_0:

$$\eta_0^{(p-1)\varepsilon_i} = \eta_0^{\sum_{a=1}^{p-1}\omega^i(a)\sigma_a^{-1}} \equiv \prod_{a=1}^{p-1} \sigma_a^{-1}(\eta_0)^{\omega^i(a)} \bmod E^{p^N}.$$

If i is odd, $\omega^i(a) = -\omega^i(-a)$, while $\sigma_a^{-1}(\eta_0) = \sigma_{-a}^{-1}(\eta_0)$. The factors for a and $-a$ cancel, so $\varepsilon_i(\eta_0) \equiv 1 \bmod E^{p^N}$ if i is odd, using once more that multiplication by $p-1$ is bijective on E_{p^N}. Thus we have shown the following decomposition:

Corollary 59. (cf. [5, Proposition 8.10, page 154]) We have

$$E_{p^N} = \langle\zeta\rangle \oplus \bigoplus_{\substack{i=2 \\ i \text{ even}}}^{p-3} \varepsilon_i E_{p^N}$$

and $\langle\zeta\rangle = \varepsilon_1 E_{p^N}$. □

Proof of Theorem 57. We apply the above discussion to $K = \mathbb{Q}$, $L = \mathbb{Q}(\zeta)$ and $G = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. By (40),

$$\begin{aligned} H &\cong A/A^p \quad \text{as } G\text{-modules, so} \\ \varepsilon_i H &\cong \varepsilon_i(A/A^p) \quad \text{for all } i \in \{0, 1, \ldots, p-2\}. \end{aligned}$$

Let $h \in \varepsilon_i H$, $b \in \varepsilon_k B$. Since $\langle h, b\rangle \in \mu_p$, (45) says that

$$\langle h, b\rangle^{\omega(a)} = \langle h, b\rangle^{\sigma_a}, \qquad a \in \{1, \ldots, p-1\}.$$

Next, we note that also $h \in H \cong A/A^p$ and $b \in B$ are elements of order dividing p, so analogously to (44), the following terms are well-defined:

$$h^{\omega(a)} := h^{a+p\mathbb{Z}} := h^a, \quad b^{\omega(a)} := b^{a+p\mathbb{Z}} := b^a, \quad a \in \{1, \ldots, p-1\}.$$

By the bilinearity of $\langle \cdot, \cdot \rangle$, we find that for any $i, k = 0, 1, \ldots, p-2$,

$$\langle h^{\omega^i(a)}, b^{\omega^k(a)}\rangle = \langle h^{a^i}, b^{a^k}\rangle = \langle h, b\rangle^{a^{i+k}} = \langle h, b\rangle^{\omega^{i+k}(a)}, \quad a \in \{1, \ldots, p-1\}.$$

In order to compute h^{σ_a}, for $h \in \varepsilon_i H$ and $a \in \{1, \ldots, p-1\}$, we change the notation of the action of $\mathbb{Z}_p[G]$ on H to make it easier to read. There is an $h_0 \in H$ with $h = \varepsilon_i h_0$, so by Lemma 50 (iv),

$$\sigma_a(h) = \sigma_a(\varepsilon_i h_0) = (\varepsilon_i \sigma_a) h_0 = \omega^i(a)\varepsilon_i h_0 = \omega^i(a) h.$$

So in the other notation, $h^{\sigma_a} = h^{\omega^i(a)}$. Similarly, we obtain $b^{\sigma_a} = b^{\omega^k(a)}$ for $b \in \varepsilon_k B, a \in \{1, \ldots, p-1\}$.
Both together yield

$$\begin{aligned} \langle h, b\rangle^{\omega(a)} &= \langle h, b\rangle^{\sigma_a} \overset{(41)}{=} \langle h^{\sigma_a}, b^{\sigma_a}\rangle \\ &= \langle h^{\omega^i(a)}, b^{\omega^k(a)}\rangle = \langle h, b\rangle^{\omega^{i+k}(a)}, \end{aligned} \tag{46}$$

for any $h \in \varepsilon_i H$, $b \in \varepsilon_k B$, $a \in \{1, \ldots, p-1\}$. If $i+k \not\equiv 1 \bmod (p-1)$, then (46) implies $\langle h, b\rangle = 1$. But since the pairing between B and H is nondegenerate, it follows that for all $i, j \in \{0, 1, \ldots, p-2\}$ with $i + j \equiv 1 \bmod (p-1)$, the induced pairing

$$\varepsilon_j B \times \varepsilon_i H \to \mu_p$$

is nondegenerate. Since

$$H \cong A/A^p \quad \text{as } \mathbb{Z}_p[G]\text{-modules,}$$

we have

$$\varepsilon_i H \cong \varepsilon_i(A/A^p) \quad \text{as } \mathbb{Z}_p[G]\text{-modules} \quad \text{for all } i \in \{0, 1, \ldots, p-2\}.$$

Moreover, the above nondegenerate pairing together with Lemma 26 gives an isomorphism

$$\varepsilon_i H \cong (\varepsilon_j B)^* \cong \varepsilon_j B$$

of abelian groups for all $i, j \in \{0, 1, \ldots, p-2\}$ with $i + j \equiv 1 \bmod (p-1)$. This is not an isomorphism of G-modules, since G-linearity is not true in general. Thus,

$$\varepsilon_j B \cong \varepsilon_i H \cong \varepsilon_i(A/A^p), \tag{47}$$

as abelian groups for all $i, j \in \{0, 1, \ldots, p-2\}$ with $i + j \equiv 1 \bmod (p-1)$.

Now the above map $\phi : B \to A_p$ is G-linear, so for all $j \in \{0, 1, \ldots, p-2\}$ the restriction

$$\phi|_{\varepsilon_j B} : \varepsilon_j B \to \varepsilon_j A_p \tag{48}$$

is well-defined. We also have

$$\ker \phi|_{\varepsilon_j B} \cong \text{subgroup of } \varepsilon_j(E/E^p). \tag{49}$$

for all $j \in \{0, 1, \ldots, p-2\}$.

Definition 60. *Let $p > 0$ be a prime number. The p-rank of a finite group is the largest integer n such that G has an elementary abelian subgroup of order p^n.*

In the following, let dim denote the dimension over $\mathbb{Z}/p\mathbb{Z}$.

As follows from its definition, H is isomorphic to the maximal elementary p-abelian quotient of A (cf. pages 72–73). Moreover, we have $H \cong A/A^p$ as $\mathbb{Z}_p[G]$-modules. Using the general fact that the maximal elementary p-abelian quotient of any finite abelian group is isomorphic to its maximal elementary p-abelian subgroup, we obtain

$$p\text{-rank}(A) = \dim(A/A^p). \tag{50}$$

By its definition on page 75, A_p consists precisely of all elements $x \in A$ with $x^p = 1$, i.e. A_p is the maximal elementary p-abelian subgroup of A. Hence we have

$$p\text{-rank}(A) = \dim(A_p). \tag{51}$$

By $\mathbb{Z}_p[G]$-linearity, (50) and (51) remain stable if they are reduced to the idempotent submodules. Thus, for all $i, j \in \{0, 1, \ldots, p-2\}$ we have

$$p\text{-rank}(\varepsilon_i A) = \dim(\varepsilon_i(A/A^p)) \tag{52}$$

and

$$p\text{-rank}(\varepsilon_j A) = \dim(\varepsilon_j A_p). \tag{53}$$

Together with the fact that $\ker\phi$ is isomorphic to a subgroup of E/E^p (see above), these relations imply the following for $i, j \in \{0, 1, \ldots, p-2\}$: If i is even and j odd with $i+j \equiv 1 \bmod (p-1)$ then

$$\begin{aligned}
p\text{-rank}(\varepsilon_i A) &\overset{(52)}{=} \dim(\varepsilon_i(A/A^p)) \\
&\overset{(47)}{=} \dim(\varepsilon_j B) = \dim(\ker \phi|_{\varepsilon_j B}) + \dim(\mathrm{im}\ \phi|_{\varepsilon_j B}) \\
&\overset{(48),(49)}{\leq} \dim(\varepsilon_j(E/E^p)) + \dim(\varepsilon_j A_p) \\
&\overset{(53)}{=} \dim(\varepsilon_j(E/E^p)) + p\text{-rank}(\varepsilon_j A).
\end{aligned}$$

By Corollary 59, $\dim(\varepsilon_j(E/E^p)) = 0$ if j is odd and not equal to 1, so in this case,

$$p\text{-rank}(\varepsilon_i A) \leq p\text{-rank}(\varepsilon_j A).$$

If $j = 1$, and therefore $i = 0$, then $\varepsilon_i A = \varepsilon_0 A = A_0 = 1 = A_1 = \varepsilon_1 A = \varepsilon_j A$ by Proposition 53. This completes the proof of Theorem 57. □

Corollary 61. *If $p \mid h_p^+$, then $p \mid h_p^-$.*

Proof. Let $p \mid h_p^+$. By Proposition 55, the natural map $C^+ \to C$ is an injection, where C is the ideal class group of $\mathbb{Q}(\zeta)$ and C^+ is the ideal class group of $\mathbb{Q}(\zeta)^+$. Let A^+ be the p-Sylow subgroup of C^+, and let A be the p-Sylow subgroup of C. The map of $C^+ \to C$ restricts to an injection of p-Sylow subgroups $A^+ \to A$. We have already shown that the characters of $\mathrm{Gal}(\mathbb{Q}(\zeta)^+/\mathbb{Q})$ can be identified with the even ones of the characters of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ (cf. Lemma 25). So if $\varepsilon_i = (1/(p-1)) \sum_{a=1}^{p-1} \omega^i(a)\sigma_a^{-1}$, $i = 0, 1, \ldots, p-2$, then the above injection restricts to injections of subgroups $\varepsilon_i A^+ \to \varepsilon_i A$, $i = 0, 2, \ldots, p-3$ even (as is also explained in the paragraph after Lemma 56 on page 71). Hence we reach the following injection of direct sums:

$$A^+ \cong \bigoplus_{\substack{i=0 \\ i \text{ even}}}^{p-2} \varepsilon_i A^+ \to \bigoplus_{i=0}^{p-2} \varepsilon_i A \cong A.$$

Furthermore, $h_p = |C| = |A|n$ and $h_p^+ = |C^+| = |A^+|n^+$, where $p \nmid n$ and $p \nmid n^+$, since A and A^+ are the p-Sylow subgroups of A and A^+. Also,

$$|A| = \prod_{i=0}^{p-2} |\varepsilon_i A|, \qquad \text{respectively} \qquad |A^+| = \prod_{\substack{i=0 \\ i \text{ even}}}^{p-2} |\varepsilon_i A^+|.$$

Thus it suffices to show that for some $j = 1, \dots, p-2$ odd, we have $p \mid |\varepsilon_j A|$. Since $p \mid h_p^+$, there is some even index $i = 0, 2, \dots, p-3$ such that $\varepsilon_i A^+$ is of nonzero p-rank. Then by the above injection, $\varepsilon_i A$ is of nonzero p-rank and by Theorem 57, the odd index $j \in \{1, \dots, p-2\}$ with $i + j \equiv 1 \bmod (p-1)$ satisfies

$$p\text{-rank}(\varepsilon_i A) \leq p\text{-rank}(\varepsilon_j A),$$

so in fact, $p \mid |\varepsilon_j A|$ with j odd. That completes the proof of this corollary.

□

We are now ready to finish the proof of Theorem 19. Because of Theorem 42 it remains to see that p divides h_p if and only if it divides h_p^-. However, $h_p = h_p^+ \cdot h_p^-$. Since p is a prime number, it divides h_p if and only if it divides h_p^+ or h_p^-. The claim therefore follows from Corollary 61. □

5 Final remarks

The theory about regular and irregular primes has lead to certain open problems. Among these are the conjecture of Vandiver that the assumption $p \mid h_p^+$ never happens (cf. [5, page 78]), as well as the question whether there are infinitely many regular primes, although by empirical results and probability arguments, it is supposed that approximately 39% of all primes are irregular and 61% are regular (cf. [5, page 7]).

References

[1] S. Bosch: Algebra, 8. Auflage, Springer Spektrum, Springer-Verlag, Berlin, Heidelberg, 2013, ISBN 978-3-642-39566-6

[2] K. Conrad: Fermat's last theorem for regular primes, *preprint*, available at `https://kconrad.math.uconn.edu/blurbs/gradnumthy/fltreg.pdf`

[3] J. Kohlhaase: Skriptum zur Vorlesung Algebraische Zahlentheorie 1, Universität Duisburg-Essen, Wintersemester 2021/22

[4] J. Neukirch: Algebraische Zahlentheorie, Unveränderter Nachdruck der ersten Auflage, die 1992 im Springer-Verlag Berlin Heidelberg unter dem Titel Algebraische Zahlentheorie, ISBN 3-540-54273-5, erschien; Springer-Verlag Berlin Heidelberg 1992, ursprünglich erschienen bei Springer-Verlag Berlin Heidelberg New York 2007; ISBN 978-3-540-37547-0, ISBN 978-3-540-37663-7 (eBook), DOI 10.1007/978-3-540-37663-7

[5] L. Washington: Introduction to Cyclotomic Fields, Second Edition, Springer, 1997, Springer Verlag New York, Berlin, Heidelberg, ISBN 0-387-94762-0

Eigenständigkeitserklärung

Hiermit bestätige ich, dass ich die vorliegende Arbeit selbständig verfasst und keine anderen als die angegebenen Hilfsmittel benutzt habe. Die Stellen der Arbeit, die dem Wortlaut oder dem Sinn nach anderen Werken (dazu zählen auch Internetquellen) entnommen sind, wurden unter Angabe der Quelle kenntlich gemacht.

Gelsenkirchen, den 03. Dezember 2023

Ort, Datum   Unterschrift