THE GRUNWALD–WANG THEOREM AND ISOMORPHIC RADICAL EXTENSIONS:
WHY 2 IS THE EVIL PRIME

A DISSERTATION
SUBMITTED TO THE DEPARTMENT OF MATHEMATICS
OF STANFORD UNIVERSITY
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
BACHELOR OF SCIENCE
WITH HONORS

Robin Zhang
June 2017

© Copyright by Robin Zhang 2017
All Rights Reserved

Abstract

This thesis will introduce the study of powers in number fields through two similar questions. The first is the Grunwald–Wang theorem that examines the relationship between being an n-th power in a number field K globally and being an n-th power almost everywhere locally (a "Hasse Principle" for n-th powers). We also discuss the history and motivation of the Grunwald–Wang theorem and provide some examples.

We will then consider a question for two irreducible polynomials $X^n - a$ and $X^n - b$ over a field K of characteristic 0 such that respective roots α and β generate isomorphic degree-n radical extensions of K. In this second scenario, we analyze if the ratio b^j/a must be an n-th power in K for some integer j coprime to n when $K(\alpha) \cong K(\beta)$.

In both questions, the presence of distinct quadratic subextensions of cyclotomic and radical extensions give rise to explicit classes of counterexamples. Finally, we explore how properties of 2-power cyclotomic extensions provide obstructions in both situations.

Acknowledgments

I am eager to thank my advisor, Brian Conrad, for his generous time and patience. His numerous suggestions and explanations have been incredibly helpful throughout the problem-solving and writing processes. More generally, the advice that I received from Brian throughout my undergraduate career at Stanford has been invaluable. I am humbled to have had such a dedicated and knowledgeable teacher.

I would also like to thank all of my friends for enduring my habits and late nights throughout the time that I have spent working on this thesis, and for constantly making my life richer and happier. Finally, I warmly thank my parents, Shou-Wu and Min, and my brother, Andy, for all of the love and laughter that we share.

Contents

Chapter 1

Introduction

The proof did not apply when, roughly speaking, $[K : F]$ *was even.*

–Xianghao Wang [11, p.471]

1.1 Motivation

In elementary number theory, one can use quadratic reciprocity to prove that a nonzero integer a is a square in $\mathbf{Z}$ if it is a quadratic residue modulo p for all but finitely many primes p. We can then attempt to generalize this result to higher powers: if an integer a is an n-th power modulo p for all but finitely many primes p, then is a an n-th power in $\mathbf{Z}$? By Hensel's lemma, we may translate the question to the p-adic numbers $\mathbf{Q}_p$ since for all odd $p \nmid a$, a is an n-th power in $\mathbf{Q}_p$ if and only if a is an n-th power modulo p. We may also further generalize the question by replacing $\mathbf{Z}$ with any number field K, so we may now ask the question:

Question 1.1.1. *Let* K *be a number field. If* $a \in K^\times$ *is an* n*-th power in* $K_\mathfrak{p}$ *for all but finitely many primes* $\mathfrak{p}$ *of* K*, then is* a *an* n*-th power in* K*?*

In 1933, Wilhelm Grunwald published a paper giving an erroneous proof for "Grunwald's theorem", a statement about the existence of prescribed cyclic extensions of K that implies that Question 1.1.1 always has an affirmative answer, using analytic number theory and class field theory [5]. This was supplemented by a second published proof of Grunwald's theorem by George Whaples in 1942 that eliminated the need for analytic number theory [13]. However, they were both wrong! There are counter-examples to Question 1.1.1 even when $K = \mathbf{Q}$:

Example 1.1.2. Let $K = \mathbf{Q}$, $n = 8$, and $a = 16$. Observe that $16 = 2^4 = (-2)^4 = (1+i)^8$, so 16 is an 8th power modulo an odd prime p if one of $\{-1, 2, -2\}$ is a quadratic residue modulo p. But for every odd prime p, one of $\{-1, -2, 2\}$ is a quadratic residue modulo p, so 16 is always an 8-th

power modulo an odd prime p and so 16 is an 8-th power in $\mathbf{Q}_p$ for all odd primes p. On the other hand, 16 is not an 8-th power in $\mathbf{Q}$.

Example 1.1.3. Let $K = \mathbf{Q}(\sqrt{7})$, $n = 8$, and $a = 16$. By the reasoning in Example 1.1.2, 16 is an 8-th power in $\mathbf{Q}_p$ for all odd primes p. Furthermore, $\mathbf{Q}_2(\sqrt{7}) = \mathbf{Q}_2(i)$, so 16 is also an 8-th power in the 2-adic completions of K (as well as the archimedean completions, both of which are $\mathbf{R}$). Yet, 16 is not an 8-th power in $\mathbf{Q}(\sqrt{7})$ so we now have a counter-example in which there are *no* omitted places.

In 1948, Xianghao (also spelled Shianghao or Shianghaw) Wang pointed out Example 1.1.2 [11]. In 1950, Hasse and Wang independently proved the correct formulation of Grunwald's statement, known as the Grunwald–Wang theorem, with a description of all counter-examples [6, 12]. We provide an overview of the Grunwald–Wang theorem and some of the intricacies of 2-power cyclotomic extensions that lead to the counter-examples to Question 1.1.1 in Chapter 2.

Note that Question 1.1.1 asks when $X^n - a$ has a root in a number field K for $a \in K^\times$. Instead, let us consider the opposite extreme: when $X^n - a$ and $X^n - b$ are irreducible over K.

Let α be a root of $X^n - a$ and β a root of $X^n - b$, so the extensions $K(\alpha)/K$ and $K(\beta)/K$ are intrinsic to a and b, respectively, by irreducibility over K. When $b^j/a = c^n$ for some $c \in K^\times$ for $j \in \mathbf{Z}$ coprime to n (a symmetric condition on a and b since then $a^{j'}/b \in (K^\times)^n$ for $j' \equiv j^{-1} \pmod{n}$), then β^j/c is a root of $X^n - a$ and so $K(\alpha) \subset K(\beta)$. Equality between $K(\alpha)$ and $K(\beta)$ is then forced by comparing K-degrees. The sufficiency of this condition on a and b motivates a necessity question [4]:

Question 1.1.4. *If $K(\alpha) \cong K(\beta)$ over K, then is b^j/a necessarily an n-th power in K for some integer j coprime to n?*

In Chapter 3, we explore Question 1.1.4 and how affirmative answers may be given for various cases depending on the intersection of K and $\mathbf{Q}(\zeta_n)$. As with the examination of the Grunwald–Wang theorem, the intricacies of 2-power cyclotomic fields lead to some classes of counter-examples. When $K \cap \mathbf{Q}(\zeta_n) = \mathbf{Q}$, there are precisely *two families* of counter-examples, and they occur only when n is divisible by 8. The lowest-degree case of the first family (Example 3.4.3) with $K = \mathbf{Q}$ and "simplest" coefficients is as follows:

Example 1.1.5. Let $K = \mathbf{Q}, n = 8, a = -1, b = -16$. By Eisenstein's criterion, X^8+1 is irreducible over $\mathbf{Q}$. By the argument below, $X^8 + 16$ is also irreducible over $\mathbf{Q}$.

Let x be a root of $X^8 + 16$. Note that $z := (1/2)x^2$ is a root of the polynomial $\Phi_8 := X^4 + 1$. Then, $x^2 = 2z$ for z a primitive 8-th root of unity, so x is either quadratic over $\mathbf{Q}(z) = \mathbf{Q}(\zeta_8)$ or $x \in \mathbf{Q}(\zeta_8)$. Suppose that $x \in \mathbf{Q}(\zeta_8)$. Then $2z = x^2$ is a square in $\mathbf{Q}(\zeta_8)$ which implies that the quantity $iz = z^3$ (since z is a primitive 8-th root of unity) is a square since

$$iz = \frac{-2z}{(1+i)^2}.$$

But z^3 is also a primitive 8-th root of unity so if z^3 is a square in $\mathbf{Q}(\zeta_8)$ then $\mathbf{Q}(\zeta_8)$ must contain a primitive 16-th root of unity. By degree considerations, this is impossible. Therefore, x is quadratic over the quartic field $\mathbf{Q}(\zeta_8)$, i.e. $[\mathbf{Q}(x) : \mathbf{Q}] = 8$. Hence, $X^8 + 16$ is irreducible.

For a root α of $X^8 + 1$, observe that $\alpha^4 = i$ and so $i \in \mathbf{Q}(\alpha)$. Let $\beta := (1+i)\alpha$, so $\mathbf{Q}(\alpha) = \mathbf{Q}(\beta)$. Then $\beta^8 = 16\alpha^8 = -16$ so β is a root of $X^8 + 16$. On the other hand, $b^j/a = (-1)^{j+1}2^{4j}$ is never an 8-th power in $\mathbf{Q}$ for any odd $j \in \mathbf{Z}$.

The lowest-degree case of the second family (Example 3.4.4) with $K = \mathbf{Q}$ and minimal coefficients is as follows:

Example 1.1.6. Let $K = \mathbf{Q}, n = 16, a = -1, b = -256$. By Eisenstein's criterion, $X^{16} + 1$ is irreducible over $\mathbf{Q}$. By a similar argument as the one given for $X^8 + 16$ above, $X^{16} + 256$ is also irreducible over $\mathbf{Q}$.

For a root α of $X^{16} + 1$, observe that $\alpha^8 = i$ and so $i \in \mathbf{Q}(\alpha)$. Let $\beta := (1+i)\alpha$, so $\mathbf{Q}(\alpha) = \mathbf{Q}(\beta)$. Then $\beta^{16} = 256\alpha^{16} = -256$ so β is a root of $X^{16} + 256$. On the other hand, $b^j/a = (-1)^{j+1}2^{8j}$ is never an 16-th power in $\mathbf{Q}$ for any odd $j \in \mathbf{Z}$.

In Chapter 3, we shall systematically construct these two families of examples and show that they are the only examples wherein Question 1.1.4 has a negative answer when $K \cap \mathbf{Q}(\zeta_n)$.

Chapter 2

The Grunwald–Wang Theorem

> *In the spring of 1948, Bill Mills, one of the students Artin had brought with him from Indiana, talked on "Grunwald's theorem" in the seminar. Some days later I was with Artin in his office when Wang appeared. He said he had a counterexample to a lemma which had been used in the proof. An hour or two later, he produced a counterexample to the theorem itself... Of course he [Artin] was astonished, as were all of us students, that a famous theorem with two published proofs, one of which we had all heard in the seminar without our noticing anything, could be wrong. But it was a good lesson!*
>
> –John Tate [10, p.30]

2.1 The Story

From a historical perspective, the story of the Grunwald–Wang theorem originates from the work of Grunwald's advisor Helmut Hasse. In his proof of the Albert–Brauer–Hasse–Noether theorem on central simple algebras over number fields, Hasse proved the following existence theorem in 1931 [10, p.27]:

Theorem 2.1.1 (Hasse's existence theorem)**.** *Let K be a number field and S a finite set of primes of K. Let $n_{\mathfrak{p}} \in \mathbf{N}$ be given for each $\mathfrak{p} \in S$. Then there exists a cyclic extension L/K of degree $\mathrm{lcm}_{\mathfrak{p}\in S}\{n_{\mathfrak{p}}\}$ such that $n_{\mathfrak{p}} \mid [L_{\mathfrak{p}} : K_{\mathfrak{p}}]$ for each $\mathfrak{p} \in S$ where $L_{\mathfrak{p}}$ denotes the completion of L at any place above $\mathfrak{p}$.*

While this theorem was enough for the purpose of proving the Albert–Brauer–Hasse–Noether theorem, Hasse wanted a version of the existence theorem "in its greatest possible generality" [10, p.28]. At Hasse's urging the following year, Grunwald used the methods from his doctoral thesis to prove a stronger existence theorem *prescribing* the completion $L_{\mathfrak{p}}$ as a cyclic degree-$n_{\mathfrak{p}}$ extension of $K_{\mathfrak{p}}$:

Claim 2.1.2 ("Grunwald's theorem")**.** *Let K be a number field and S a finite set of primes of K. Let $E_\mathfrak{p}/K_\mathfrak{p}$ be a given cyclic extension for each $\mathfrak{p} \in S$. Then there exists a cyclic extension L/K of degree $\operatorname{lcm}_{\mathfrak{p}\in S}[E_\mathfrak{p} : K_\mathfrak{p}]$ such that $L_\mathfrak{p} \cong E_\mathfrak{p}$ over $K_\mathfrak{p}$ for each $\mathfrak{p} \in S$.*

Recall that in Chapter 1, we have a counter-example to Question 1.1.1 in Example 1.1.2. We may use this counter-example to produce a direct counter-example to "Grunwald's theorem" itself:

Example 2.1.3. Let $K = \mathbf{Q}$ and let $S = \{2\}$. Let E_2 be the unramified extension of $\mathbf{Q}_2$ of degree 8. Then there no cyclic extensions $L/\mathbf{Q}$ of degree 8 such that $L_2 \cong E_2$ over $\mathbf{Q}_2$.

Proof. Suppose $L_2 \cong E_2$. By the Kronecker–Weber theorem, we have $K \subset \mathbf{Q}(\zeta_n)$ for some $n \in \mathbf{N}$. Taking n to be the minimal such integer, we know from (2) being unramified in $L/\mathbf{Q}$ and from consideration of inertia groups in $\operatorname{Gal}\big(\mathbf{Q}(\zeta_n)/\mathbf{Q}\big)$ that n must be odd. Also note that $\operatorname{Gal}(L/\mathbf{Q}) \cong C_8$ where C_8 is the cyclic group of order 8. Then we have the induced surjective map $f : (\mathbf{Z}/n\mathbf{Z})^\times \twoheadrightarrow C_8$. Define $g : C_8 \twoheadrightarrow C_8/C_4 = \{1, -1\}$ to send 1 to the Jacobi symbol $(\frac{2}{n})$. Then we have the composition of maps

$$(\mathbf{Z}/n\mathbf{Z})^\times \xrightarrow{\ f\ } C_8 \xrightarrow{\ g\ } C_8/C_4 = \{1, -1\}.$$

Note that $2 \in (\mathbf{Z}/n\mathbf{Z})^\times$ corresponds to the Frobenius element Frob_2 at $2\mathbf{Z}$ through the isomorphism $\operatorname{Gal}\big(\mathbf{Q}(\zeta_n/\mathbf{Q})\big) \cong (\mathbf{Z}/n\mathbf{Z})^\times$. Since $L_2 \cong E_2$, Frob_2 corresponds to the generator σ of $\operatorname{Gal}(E_2/\mathbf{Q}_2)$ (i.e. $f(2) = 1$). Since $f(2)$ is therefore a generator of C_8 and g is surjective, $\big(\frac{2}{n}\big) = g \circ f(2) = -1$. By the definition of Jacobi symbols,

$$\left(\frac{2}{n}\right) = \prod_{\text{prime } q|n} \left(\frac{2}{q}\right)^{\operatorname{ord}_p(n)},$$

and so the Legendre symbol $\left(\frac{2}{p}\right)$ equals -1 for some prime $p \mid n$. By quadratic reciprocity, this only occurs when $p \equiv \pm 3 \pmod 8$.

Using the factorization $(\mathbf{Z}/n\mathbf{Z})^\times = \prod_{\text{prime } q|n}(\mathbf{Z}/q^{\operatorname{ord}_q(n)}\mathbf{Z})^\times$, we have an induced surjective map on the direct factor $(\mathbf{Z}/p\mathbf{Z})^\times$ of $(\mathbf{Z}/p^{\operatorname{ord}_p(n)})^\times$:

$$(\mathbf{Z}/p\mathbf{Z})^\times \xrightarrow{\ f_p\ } C_8 \xrightarrow{\ g\ } C_8/C_4.$$

In particular, f_p still sends 2 to the generator of C_8 by the same reasoning for f. Observe that $C_8 \cong (\mathbf{Z}/p\mathbf{Z})^\times/\ker f_p$, so $p \cong 1 \pmod 8$. Hence 2 is a square in $(\mathbf{Z}/p\mathbf{Z})^\times$, so $f_p(2) \in C_4$, contradicting the fact that $f_p(2)$ is a generator of C_8. □

Remark 2.1.4. An alternative proof of Example 2.1.3 proceeds as follows. Example 1.1.2 shows that 16 becomes a norm in $\mathbf{Q}_p$ for all odd primes p and is trivially a norm at even places since $\mathbf{R}_{>0}$ is divisible, so 16 is a norm in $\mathbf{Q}_2$ by the product formula for the norm residue symbol for cyclic

extensions. But then $E_2/\mathbf{Q}_2$ of degree 8 cannot be unramified because the ordinal of 16 is not divisible by 8.

When Wang found Example 2.1.3 in 1948, many were concerned that Hasse's existence theorem and the dependent Albert–Brauer–Hasse–Noether theorem could also be false. However, Hasse [6] and Wang [12] independently gave correct formulations of what is now known as the Grunwald–Wang theorem in 1950. Although Hasse claimed that his existence theorem (Theorem 2.1.1) could be proven independently of the Grunwald–Wang Theorem, the only published proof was the deduction given by Grunwald from Claim 2.1.2 [10, p.27–28].

2.2 The Theorem

Here is a first version of the Grunwald–Wang Theorem, as in [1, Chapter X, Theorem 5]:

Theorem 2.2.1. *Let K be a number field, S a finite set of primes of K, and C_K the idèle class group of K. Moreover, let m be the greatest integer such that $\eta_m \in K$, where $\eta_m := \zeta_m + \zeta_m^{-1}$.*

Let $\chi_{\mathfrak{p}}$ be a given local continuous character on $G_{K_{\mathfrak{p}}}^{\mathrm{ab}}$ of some finite order $n_{\mathfrak{p}}$ for each $\mathfrak{p} \in S$. Then there exists a continuous finite order character χ of G_K^{ab} whose restriction to $G_{K_{\mathfrak{p}}}^{\mathrm{ab}}$ is $\chi_{\mathfrak{p}}$ for all $\mathfrak{p} \in S$ and whose order is $\operatorname{lcm}_{\mathfrak{p}\in S} n_{\mathfrak{p}}$ except exactly when the following conditions all occur (in which case the order can be arranged to be $2\operatorname{lcm}_{\mathfrak{p}\in S} n_{\mathfrak{p}}$):

1. *$A := \{-1, 2+\eta_m, -2-\eta_m\} \not\subset K^2$;*
2. *n is divisible by 2^{m+1};*
3. *$S_0 := \{\text{primes } \mathfrak{p} \text{ of } K : \mathfrak{p} \mid 2 \text{ and } A \not\subset K_{\mathfrak{p}}^2\} \subset S$.*

Not only did Theorem 2.2.1 fix the errors in "Grunwald's Theorem", it also gave Hasse's existence theorem as a direct consequence [6, 12]. However, the relation between the formulation of Theorem 2.2.1 in terms of characters and the local-global statement about powers in Question 1.1.1 is not immediately evident. While the original paper by Wang [12] proving Theorem 2.2.1 hints at an answer to Question 1.1.1, a clearer connection can be drawn through class field theory.

Looking at a (continuous) character

$$\chi : G_K \to \mu_n(\mathbf{C}) \cong \mathbf{Z}/n\mathbf{Z}$$

reduces to the study of a character

$$\chi^{\mathrm{ab}} : G_K^{\mathrm{ab}} \to \mathbf{Z}/n\mathbf{Z}.$$

The Artin map from the idèle class group C_K to G_K^{ab} induces a bijection between the open subgroups of finite index and induces isomorphisms between the associated quotients. This fundamental

information gives us an isomorphism

$$\mathrm{Hom}_{\mathrm{cont}}(G_K^{\mathrm{ab}}, \mathbf{Z}/n\mathbf{Z}) \cong \mathrm{Hom}_{\mathrm{cont}}(C_K, \mathbf{Z}/n\mathbf{Z}) = \mathrm{Hom}_{\mathrm{cont}}(C_K/C_K^n, \mathbf{Z}/n\mathbf{Z}).$$

But $C_K^n \subset C_K$ is closed with C_K/C_K^n compact and even profinite (this rests on compactness of the norm-1 idèle class group, or equivalently the main finiteness theorems for class groups and unit groups in algebraic number theory). Using the compatible local Artin map, Theorem 2.2.1 is thereby a statement about the surjectivity of the natural map

$$\mathrm{Hom}_{\mathrm{cont}}(C_K/C_K^n, \mathbf{Z}/n\mathbf{Z}) \longrightarrow \prod_{\mathfrak{p}\in S} \mathrm{Hom}_{\mathrm{cont}}\left({K_{\mathfrak{p}}}^{\times}/\left({K_{\mathfrak{p}}}^{\times}\right)^n, \mathbf{Z}/n\mathbf{Z}\right). \tag{2.1}$$

With some exact sequence considerations, one can show that the functor $\mathrm{Hom}_{\mathrm{cont}}(-, \mathbf{Z}/n\mathbf{Z})$ from profinite abelian groups that are killed by n to discrete $\mathbf{Z}/n\mathbf{Z}$-modules is exact and satisfies "double duality". Thus, the surjectivity of (2.1) is *precisely* the injectivity of

$$\prod_{\mathfrak{p}\in S} {K_{\mathfrak{p}}}^{\times}/\left({K_{\mathfrak{p}}}^{\times}\right)^n \longrightarrow C_K/C_K^n. \tag{2.2}$$

We claim that the kernel of (2.2) is a quotient of the kernel $Ш_S^1(K, \mu_n)$ of the map

$$K^{\times}/\left(K^{\times}\right)^n \longrightarrow \prod_{\mathfrak{p}\notin S} {K_{\mathfrak{p}}}^{\times}/\left({K_{\mathfrak{p}}}^{\times}\right)^n \tag{2.3}$$

which contains the local-to-global information on n-th powers in K outside of the local information at S. To see this, consider the following commutative exact diagram (where I_K is the idèle group of K):

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K^{\times} & \longrightarrow & I_K & \longrightarrow & C_K & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle t^n} & & \downarrow{\scriptstyle t^n} & & \downarrow{\scriptstyle t^n} & & \\ 1 & \longrightarrow & K^{\times} & \longrightarrow & I_K & \longrightarrow & C_K & \longrightarrow & 1 \end{array}$$

from which we get the exact cokernel sequence in a commutative diagram

$$\begin{array}{ccccccccc} & & K^{\times}/\left(K^{\times}\right)^n & & \longrightarrow & & I_K/I_K^n & \longrightarrow & C_K/C_K^n & \longrightarrow & 1 \\ & & \downarrow & & & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \prod_{\mathfrak{p}\notin S} {K_{\mathfrak{p}}}^{\times}/\left({K_{\mathfrak{p}}}^{\times}\right)^n & \longrightarrow & \prod_{\mathfrak{p}\notin S} {K_{\mathfrak{p}}}^{\times}/\left({K_{\mathfrak{p}}}^{\times}\right)^n & \longrightarrow & 1 & & & & \end{array}$$

This yields an exact sequence of kernels of the vertical maps

$$Ш_S^1(K, \mu_n) \longrightarrow \prod_{\mathfrak{p}\in S} {K_{\mathfrak{p}}}^{\times}/\left({K_{\mathfrak{p}}}^{\times}\right)^n \longrightarrow C_K/C_K^n,$$

giving the kernel of (2.3) as a quotient of $Ш^1_S(K, \mu_n)$ (with some extra work, one can show that they are actually equal [9, Chapter 6]).

In effect, $Ш^1_S(K, \mu_n)$ encodes the obstruction for the local-to-global principle for n-th roots in K outside of the local information at S. By the discussion above, $Ш^1_S(K, \mu_n)$ also captures the surjectivity of (2.1), thus tying Theorem 2.2.1 back to Question 1.1.1. In this setting, we have a second version of the Grunwald–Wang Theorem [1, Chapter X, Theorem 1]:

Theorem 2.2.2. *Let K be a number field and S a finite set of places of K. Fix $n \in \mathbf{N}$. Let $P(n, S) := \{x \in K : x \in K_\mathfrak{p}^n \text{ for all } \mathfrak{p} \notin S\}$. Then $P(n, S) = K^n$ except in the special case given in Theorem 2.2.1, in which case $P(n, S) = K^n \cup (2 + \eta_m)^{n/2} K^n$:*

Write $n = 2^e r$ where $e := \mathrm{ord}_2(n) \geq 0$ and r is odd. The proof of the Grunwald–Wang theorem separately considers whether $K(\zeta_{2^e})/K$ is cyclic or not. In the cyclic case (such as whenever $e \leq 2$), the subfields of $K(\zeta_{2^e})/K$ are easier to work with in a sense, and so one can show that $P(n, S) = K^n$ with careful consideration.

The non-cyclic case is more delicate, and is characterized by the fact that $K(\zeta_{2^{m+1}})/K$ has three quadratic subextensions $K(i), K(\eta_{m+1})$, and $K(i\eta_{m+1})$. Note that if there exists $a \in P(n, S) \backslash K^n$ then $a \in K^r$ and $a \in P(2^e, S)$, so $a \notin K^{2^e}$. In a sense, the failure of "Grunwald's theorem" occurs specifically within the 2-power cyclotomic extensions K.

In fact, the "special case" in the Grunwald–Wang theorem arises from essentially the same counter-example even when K is any number field. The global extension $K(\zeta_{2^{m+1}})/K$ induces a local extension of $K_\mathfrak{p}$ of degree at most 2 for each $\mathfrak{p} \notin S_0$. For each $\mathfrak{p} \notin S_0$, one of $\{-1, 2+\eta_m, -2-\eta_m\}$ is a square in $K_\mathfrak{p}$ by definition of S_0, but each have $(2+\eta_m)^{n/2}$ as their n-th power. Thus, $(2+\eta_m)^{n/2}$ is an n-th power in $K_\mathfrak{p}$ for each $\mathfrak{p} \notin S_0$ but is only an $n/2$-th power globally. Thus, the kernel of (2.3) is order 2 in $K^\times / (K^\times)^n$ in the "special case." It is important to note that the failure *only occurs up to a factor of* 2.

When $K = \mathbf{Q}$, the characterization of the non-cyclic case $\mathbf{Q}(\zeta_m)/\mathbf{Q}$ is precisely when m is divisible by 8 due to the fact that $\mathbf{Q}(\zeta_8)$ has three quadratic subextensions $\mathbf{Q}(i), \mathbf{Q}(\sqrt{2})$, and $\mathbf{Q}(\sqrt{-2})$ (related to Example 2.1.3). Here is a corollary to the Grunwald–Wang theorem:

Corollary 2.2.3. *Let $a \in \mathbf{Q}$ and $n \in \mathbf{N}$. Then a is an n-th power in $\mathbf{Q}_p$ for all but finitely many primes $p \in \mathbf{Q}$ if and only if either:*

1. *a is an n-th power in $\mathbf{Q}$, or*
2. *n is divisible by 8 and $a = 2^{n/2} b^n$ for some $b \in \mathbf{Q}$.*

With Corollary 2.2.3 and the observation that $X^8 - 16 \mid X^n - 2^{n/2}$ in $\mathbf{Q}[x]$ for any integer $n \geq 8$, we see that the counter-examples to "Grunwald's theorem" over $\mathbf{Q}$ all effectively arise from Example 2.1.3. related to Question 1.1.4.

Chapter 3

Isomorphism Question for Radical Extensions

If the m-th roots of unity are not in k, the symbol $k(\sqrt[m]{\alpha})$ has no well-defined meaning and a careless use of it may lead to mistakes.

–Emil Artin and John Tate [1, Chapter IX, Section 1]

3.1 First Steps

In this chapter, we aim to analyze Question 1.1.4 which was originally posed over $\mathbf{Q}$ by Ewan Delanoy on MathOverFlow in 2014 [4] and is restated here in more natural generality.

Question 3.1.1. *Let K be a field of characteristic 0 and let $a, b \in K^\times$ such that $X^n - a$ and $X^n - b$ are irreducible over K for some $n \in \mathbf{N}$. Assume that a root of each generate K-isomorphic degree-n extensions. Is b^j/a necessarily an n-th power in K for some integer j coprime to n?*

When K contains a primitive n-th root of unity, the answer is affirmative by Kummer theory (Proposition 3.2.3). When K does not contain a primitive n-th root of unity, we can sometimes deduce an affirmative answer to Question 1.1.4 by reducing to the $K(\zeta_n)$-case when $X^n - a$ and $X^n - b$ *remain irreducible* over $K(\zeta_n)$. Indeed, for such cases (admittedly quite special), it is sufficient to show that whenever $z \in K^\times$ is an n-th power in $K(\zeta_n)$ then z is an n-th power in K. In other words, it is sufficient that the map

$$\phi : K^\times / \left(K^\times\right)^n \longrightarrow K(\zeta_n)^\times / \left(K(\zeta_n)^\times\right)^n$$

be injective when lifting to $K(\zeta_n)$ preserves irreducibility.

The irreducibility of $X^n - a$ and $X^n - b$ over $K(\zeta_n)$ is automatic whenever ϕ is injective as a consequence of the following irreducibility criterion from [8, Chapter VI, Theorem 9.1]:

Theorem 3.1.2. *Let K be a field of characteristic 0. For $n > 1$ and $a \in K^\times$, $X^n - a$ is irreducible over K if and only if a is not a p-th power in K for all primes p dividing n and, when n is divisible by 4, $a \notin -4(K^\times)^4$.*

Remark 3.1.3. To see that the condition of Theorem 3.1.2 that $a \notin -4(K^\times)^4$ is necessary, suppose that $n = 4m$ and $a = -4c^4$ with $m \in \mathbf{Z}$ and $c \in K^\times$. Then $X^n - a$ is reducible over K because

$$X^{4m} + 4c^4 = (X^{2m} + 2cX^m + 2c^2)(X^{2m} - 2cX^m + 2c^2).$$

Let us now see the relevance of Theorem 3.1.2. This says that $X^n - a$ is irreducible over $K(\zeta_n)$ if and only if $a \notin K(\zeta_n)^p$ for all primes p dividing n and, when n is divisible by 4, $a \notin -4(K(\zeta_n)^\times)^4$. Likewise, via the *given* irreducibility of $X^n - a$ over K, we know that $a \notin K^p$ for all primes p dividing n and, when n is divisible by 4, that $a \notin -4(K^\times)^4$. By the injectivity of ϕ, $a \notin K(\zeta_n)^p$ for each p dividing n and $a \notin -4(K(\zeta_n)^\times)^4$. Therefore, $X^n - a$ is irreducible over $K(\zeta_n)$ and likewise for $X^n - b$ through the same argument.

Thus, for a given K and n, it is sufficient for ϕ to be injective for Question 1.1.4 to have an affirmative answer. The kernel of ϕ is controlled by Galois cohomology groups, as we shall see in Section 3.2. In Section 3.3, we determine precisely when ϕ is injective. When n is a power of an odd prime p, or when n is a power of 2 with $i \in K$, we will show that the relevant Galois cohomology groups are trivial. However, injectivity when n is odd depends on certain congruence conditions on its prime factors and fails in most cases when n is even due to the non-cyclicity of 2-power cyclotomic extensions, as we shall see in Proposition 3.3.3.

Due to the role of the 2-power cyclotomic extensions, it is more feasible to understand Question 1.1.4 when K and $\mathbf{Q}(\zeta_n)$ have trivial intersection. In this setting, there are examples for which Question 1.1.4 has a negative answer due to the existence of distinct quadratic subextensions of $K(\alpha)/K$, reminiscent (yet somehow not as an instance) of the Grunwald–Wang theorem. As we shall sketch in Section 3.4, a direct algebraic argument given by Brian Conrad [3] determines that when $K \cap \mathbf{Q}(\zeta_n) = \mathbf{Q}$, the answer is affirmative precisely away from two explicit classes of counter-examples that occur when $8 \mid n$ (requiring $16 \mid n$ for the second class).

Altogether, the steps from Kummer theory, Section 3.3, and Section 3.4 demonstrate the following result:

Theorem 3.1.4. *Let K be a field of characteristic 0 and choose an integer $n > 1$. Let $a, b \in K^\times$ be such that $X^n - a$ and $X^n - b$ are irreducible over K and a single root of each generate K-isomorphic degree-n extensions.*

Then b^j/a is an n-th power in K for some positive integer j coprime to n if any of the following hold:

1. $K \cap \mathbf{Q}(\zeta_n) = K$,
2. $\mathbf{Q} \subsetneq K \cap \mathbf{Q}(\zeta_n) \subsetneq K$ *and either:*
   (a) n *is odd and for each prime* $p \mid n$, *either* $\mu_p(K) = 1$ *or* $q \not\equiv 1 \pmod{p}$ *for every other prime* $q \mid n$,
   (b) n *is a power of* 2 *and* $i \in K$,
3. $K \cap \mathbf{Q}(\zeta_n) = \mathbf{Q}$ *and either:*
   (a) $8 \nmid n$,
   (b) *one of* $-a$ *or* $-b$ *is not a square in* K.

Remark 3.1.5. The arguments used to prove these statements are generally algebraic in nature, so we may relax the statements to allow K to be a field of characteristic not dividing some integer n. We restrict our attention to the characteristic 0 case since it is the motivating case of interest and avoids distracting hypotheses and notation.

Case (1) of Theorem 3.1.4 amounts to Proposition 3.2.3 from Kummer theory. Both parts of Case (2) follows from applying Proposition 3.3.3 to reduce to Case (1): since $X^n - a$ and $X^n - b$ remain irreducible over $K(\zeta_n)$ because the map $K^\times / (K^\times)^n \longrightarrow K(\zeta_n)^\times / (K(\zeta_n)^\times)^n$ is injective, we may apply Proposition 3.2.3. Case (3) is discussed as Theorem 3.4.5 below.

Remark 3.1.6. The conditions in Case (2a) of Theorem 3.1.4 are much wider in scope for odd n than the restrictive hypothesis "$K \cap \mathbf{Q}(\zeta_n) = \mathbf{Q}$" in Case (3). It would be good to find some analogous condition for $n \in 8\mathbf{Z}$ allowing $K \cap \mathbf{Q}(\zeta_n) \neq \mathbf{Q}$, but this seems rather difficult.

3.2 Kummer Theory Preliminaries

First, let us recall the necessary basic results from Kummer theory. We can study the structure of n-th powers in a field K with characteristic 0 using the following classic theorem first proven by Ernst Kummer in 1861 and given in its more general form by Emmy Noether in 1933 (although the result is named after David Hilbert for reporting it in his *Zahlbericht* [7, Theorem 90]).

Theorem 3.2.1 (Hilbert's Theorem 90 [2, Chapter V, Proposition 3])**.** *If* L/K *is a Galois extension of fields, then* $H^1(L/K, L^\times)$ *is trivial.*

This yields the following useful result.

Corollary 3.2.2. *Fix* $n \in \mathbf{N}$. *Let* K *be any field of characteristic* 0 *and let* $\overline{K}$ *be a separable closure, with* $G_K := \mathrm{Gal}(\overline{K}/K)$. *Then* $K^\times / (K^\times)^n \cong H^1(\overline{K}/K, \mu_n)$ *naturally in* K, *where* μ_n *denotes the* n*-th roots of unity in* $\overline{K}$.

Proof. Observe that we have the short exact sequence

$$1 \longrightarrow \mu_n \longrightarrow \overline{K}^\times \xrightarrow{t^n} \overline{K}^\times \longrightarrow 1.$$

The induced long exact sequence of cohomology, combined with the fact that $H^1\left(G_K, \overline{K}^\times\right) = 0$ due to Theorem 3.2.1, yields the exact sequence

$$\left(\overline{K}^\times\right)^{G_K} \xrightarrow{t^n} \left(\overline{K}^\times\right)^{G_K} \longrightarrow H^1\left(\overline{K}/K, \mu_n\right) \longrightarrow 0.$$

Since G_K fixes precisely K, we have that $\left(\overline{K}^\times\right)^{G_K} = K^\times$. Therefore, we see that $K^\times/\left(K^\times\right)^n \cong H^1\left(\overline{K}/K, \mu_n\right)$ as desired. The naturality in K is clear by design. □

When we allow K to contain the n-th roots of unity, then G_K acts trivially on μ_n and so $K^\times/\left(K^\times\right)^n \cong H^1(G_K, \mu_n) \cong \mathrm{Hom}(G_K, \mu_n)$ (the cocycles are continuous so the homomorphisms have open kernel). Any $\phi \in \mathrm{Hom}(G_K, \mu_n)$ determines a cyclic Galois extension E/K of degree d dividing n (via $\ker\phi$ and the Galois correspondence) along with a *specified* isomorphism $\mathrm{Gal}(E/K) \cong \mu_d$. Any two such isomorphisms are related through the action of $(\mathbf{Z}/n\mathbf{Z})^\times \twoheadrightarrow (\mathbf{Z}/d\mathbf{Z})^\times$, and $\ker\phi^k = \ker\phi$ for any k coprime to n, so each cyclic subgroup of $K^\times/\left(K^\times\right)^n$ uniquely determines a cyclic extension of K. Conversely, a cyclic extension L of K of degree d dividing n admits an isomorphism from $\mathrm{Gal}(L/K)$ onto $\mu_d \subset \mu_n$.

By the hypothesis of Question 1.1.4, $X^n - a$ and $X^n - b$ generate K-isomorphic degree n extensions. Thus, a and b must generate the *same* subgroup of $K^\times/\left(K^\times\right)^n$ when K contains the n-th roots of unity, so one obtains:

Proposition 3.2.3. *In the setting of Question 1.1.4, b^j/a is an n-th power in K for some positive integer j coprime to n if K contains the n-th roots of unity.*

3.3 Lifting to Cyclotomic Extensions

To obtain an affirmative answer to Question 1.1.4 for a specified K, by Proposition 3.2.3 and the discussion early in Section 3.1 that it suffices that the map

$$\phi : K^\times/\left(K^\times\right)^n \longrightarrow K(\zeta_n)^\times/\left(K(\zeta_n)^\times\right)^n$$

is injective. Such injectivity holds if $H^1\big(K(\zeta_n)/K, \mu_n\big)$ is trivial, due to Corollary 3.2.2 applied to K and $K(\zeta_n)$ and the inflation-restriction sequence for H^1. In this section, we consider the case that K contains only m-th roots of unity where m is a proper divisor of n. First, we show that $H^1\big(K(\zeta_n)/K, \mu_n\big) = 1$ when $m = p^e$ and $n = p^f$ for $e < f$ with the additional stipulation that $2 \leq e$

when $p = 2$ (i.e. $i \in K$). Then, we will build up to more general m and n under suitable hypotheses on the prime factors of n and m. Throughout what follows, K is a field of characteristic 0.

Lemma 3.3.1. *Fix $f \geq 0$ and let p^e be the order of $\mu_{p^f}(K)$. Let $L := K(\zeta_{p^f})$. Then $H^i(L/K, \mu_{p^f})$ is trivial for all $i > 0$ if either p is odd or $e \geq 2$.*

Remark 3.3.2. The proof of Lemma 3.3.1 requires $e \geq 2$ when $p = 2$ because $\mathrm{Gal}(L/K)$ may not be cyclic otherwise.

Proof. Observe that whenever p is odd or $e \geq 2$, L is a *cyclic* Galois extension of K of degree $\varphi(p^f)/\varphi(p^e)$ (so p^{f-e} when $e > 0$). Furthermore, when $e > 0$ (with $e \geq 2$ when $p = 2$), $\sigma : \zeta_{p^f} \mapsto \zeta_{p^f}^{1+p^e}$ is a generator of $\mathrm{Gal}(L/K)$. If $e = 0$ (so $p > 2$) then let $\sigma : \zeta_{p^f} \mapsto \zeta_{p^f}^{\ell}$ with $\ell \in (\mathbf{Z}/p^f\mathbf{Z})^\times$ be a generator of $\mathrm{Gal}(L/K)$. Thus, $H^i(L/K, \mu_{p^f})$ is isomorphic to the Tate cohomology group $\widehat{H}^{-1}(L/K, \mu_{p^f})$ when $i > 0$ is odd and to $\widehat{H}^0(L/K, \mu_{p^f})$ when $i > 0$ is even. Let $\Delta(x) := \sigma(x)/x$. Recall from the definition of $\widehat{H}^{-1}$ and $\widehat{H}^0$ for cyclic groups that

$$\widehat{H}^{-1}(L/K, \mu_{p^f}) = \frac{\ker N_{L/K}\big|_{\mu_{p^f}}}{\Delta(\mu_{p^f})}$$
$$\widehat{H}^{0}(L/K, \mu_{p^f}) = \frac{\ker \Delta\big|_{\mu_{p^f}}}{N_{L/K}(\mu_{p^f})}.$$

We claim that both $\ker N_{L/K}\big|_{\mu_{p^f}}$ and $\Delta(\mu_{p^f})$ are equal to $\mu_{p^{f-e}}$, so $\widehat{H}^{-1}(L/K, \mu_{p^f})$ is trivial. If $e = 0$, $N_{L/K}(x) \in \mu_{p^f}(K) = \mu_{p^e}(K) = \{1\}$ for any $x \in \mu_{p^f}$, so $\ker N_{L/K}\big|_{\mu_{p^f}} = \mu_{p^f}$ when $e = 0$. Also notice that when $e = 0$, $\Delta(x) = x^{\ell-1}$ is an automorphism of μ_{p^f} since $\ell - 1 \in (\mathbf{Z}/p^f\mathbf{Z})^\times$ (as $l \not\equiv 1 \pmod p$ due to ℓ being a generator of $(\mathbf{Z}/p^f\mathbf{Z})^\times$ and hence of $(\mathbf{Z}/p\mathbf{Z})^\times$ when $f > 0$), so $\Delta(\mu_{p^f}) = \mu_{p^f}$ when $e = 0$.

Now suppose $e > 0$. For $x \in \mu_{p^f}$, we have

$$\begin{aligned} N_{L/K}(x) &= \prod_{\tau \in \mathrm{Gal}(L/K)} \tau(x) \\ &= \prod_{j \in \mathbf{Z}/p^{f-e}\mathbf{Z}} \sigma^j(x) \\ &= \prod_{j \in \mathbf{Z}/p^{f-e}\mathbf{Z}} x^{1+jp^e} \\ &= x^{p^{f-e} + \frac{(p^{f-e}-1)p^f}{2}}. \end{aligned} \tag{3.1}$$

If p is odd then $\frac{(p^{f-e}-1)p^f}{2} \equiv 0 \pmod{p^f}$, so $N_{L/K}(x) = x^{p^{f-e}}$ for $x \in \mu_{p^f}$ and hence $x \in \ker N_{L/K}\big|_{\mu_{p^f}}$ if and only if $x^{p^{f-e}} = 1$ when p is odd. Therefore, $\ker N_{L/K}\big|_{\mu_{p^f}} = \mu_{p^{f-e}}$ when p

is odd (and $e > 0$). If $p = 2$ and $e \geq 2$, then

$$2^{f-e} + \frac{(2^{f-e} - 1)2^f}{2} = 2^{f-e}(1 + 2^{f-1} - 2^{e-1}).$$

Therefore, for any $x \in \mu_{2^f}$ we have $N_{L/K}(x) = x^{2^{f-e}(1+2^{f-1}-2^{e-1})}$. Since $1 + 2^{f-1} - 2^{e-1}$ is odd (as $e \geq 2$), $x \in \ker N_{L/K}\big|_{\mu_{2^f}}$ if and only if $x^{2^{f-e}} = 1$. Hence $\ker N_{L/K}\big|_{\mu_{2^f}} = \mu_{2^{f-e}}$. We see directly (when $e > 0$) that

$$\Delta(\mu_{p^f}) = \{\sigma(x)/x : x \in \mu_{p^f}\} = \{x^{p^e} : x \in \mu_{p^f}\} = \mu_{p^{f-e}},$$

so $\widehat{H}^{-1}(L/K, \mu_{p^f}) = 1$ always.

Similarly, we claim that both $\ker \Delta|_{\mu_{p^f}}$ and $N_{L/K}(\mu_{p^f})$ are equal to μ_{p^e}, so $\widehat{H}^0(L/K, \mu_{p^f})$ is trivial. Clearly $\ker \Delta|_{\mu_{p^f}} = \{x \in \mu_{p^f} : \sigma(x) = x\} = \mu_{p^f}(K) = \mu_{p^e}$ by definition of e. When $e = 0$, we saw above that $N_{L/K}(x) = 1$ for all $x \in \mu_{p^f}$. To see that $N_{L/K}(\mu_{p^f}) = \mu_{p^e}$ when $e > 0$, if $p = 2$ we use (3.1) and that $1 + 2^{f-1} - 2^{e-1}$ is odd, whereas for $p > 2$ we use that $N_{L/K}(x) = x^{p^{f-e}}$ as seen already (when $e > 0$). Thus, $\widehat{H}^0(L/k, \mu_{p^f}) = 1$. □

Now let us consider general $n \in \mathbf{N}$ and $m \mid n$ such that n/m has the same odd prime factors as n. Due to the issue with the cyclicity of 2-power cyclotomic fields, we also require that if n is divisible by 4 then m is divisible by 4.

Proposition 3.3.3. *Choose $n > 1$. Assume that $\mu_n(K) = \mu_m(K)$ for a proper divisor $m \mid n$ as above, so in particular if n is divisible by 4 then $i \in K$. Then*

$$\phi : K^\times / \left(K^\times\right)^n \longrightarrow K(\zeta_n)^\times / \left(K(\zeta_n)^\times\right)^n$$

is injective if for each prime $p \mid n$, either $\mu_p(K) = 1$ or $q \not\equiv 1 \pmod{p}$ for all other primes $q \mid n$.

Proof. Write $n = \prod_{i=1}^k p_i^{f_i}$ for distinct primes p_i and exponents $f_i \in \mathbf{N}$. Write $m = \prod_{i=1}^k p_i^{e_i}$ for non-negative $e_i \leq f_i$. Let $L := K(\zeta_n)$.

By Corollary 3.2.2, ϕ is identified with the kernel of the restriction map $H^1(K, \mu_n) \longrightarrow H^1(L, \mu_n)$, so $\ker \phi \cong H^1(L/K, \mu_n)$ by the inflation-restriction exact sequence. Furthermore, $\mu_n = \bigoplus_{i=1}^k \mu_{p_i^{f_i}}$, so

$$H^1(L/K, \mu_n) \cong \bigoplus_{i=1}^k H^1(L/K, \mu_{p_i^{f_i}}).$$

Hence, ϕ is injective if and only if $H^1(L/K, \mu_{p_i^{f_i}})$ is trivial for each $i \in \{1, \ldots, k\}$.

Fix an $i \in \{1, \ldots, k\}$. Then $m = p_i^{e_i} s$ and $n = p_i^{f_i} r$ with $r, s \in \mathbf{N}$ both coprime to p. Let $E := K(\zeta_{p_i^{f_i}})$, a Galois intermediate field of L/K, and let $N := \mathrm{Gal}(L/E) \lhd G := \mathrm{Gal}(L/K)$. The

low-degree spectral sequence for group cohomology gives an exact sequence

$$1 \longrightarrow H^1\Big(E/K, \mu_{p_i^{f_i}}^N\Big) \xrightarrow{\text{Inf}} H^1\Big(L/K, \mu_{p_i^{f_i}}\Big) \xrightarrow{\text{Res}} H^1\Big(L/E, \mu_{p_i^{f_i}}\Big)^{G/N} \longrightarrow H^2\Big(E/K, \mu_{p_i^{f_i}}^N\Big).$$

But by Lemma 3.3.1 for E/K (note that if $p_i = 2$, the condition that $i \in K$ when $4 \mid n$ forces $e_i \geq 2$),

$$H^1\Big(E/K, \mu_{p_i^{f_i}}\Big) = H^2\Big(E/K, \mu_{p_i^{f_i}}\Big) = 1.$$

Therefore, the restriction gives an isomorphism

$$H^1\Big(L/K, \mu_{p_i^{f_i}}\Big) \cong H^1\Big(L/E, \mu_{p_i^{f_i}}\Big)^{G/N},$$

and the latter H^1 is isomorphic to

$$\text{Hom}\Big(\text{Gal}(L/E), \mu_{p_i^{f_i}}\Big)^{G/N} = \text{Hom}\Big(\text{Gal}(L/E), \mu_{p_i^{f_i}}^{G/N}\Big) = \text{Hom}\Big(\text{Gal}(L/E), \mu_{p_i^{f_i}}(K)\Big),$$

and since $f_i > 0$ this is trivial if and only if either $\mu_{p_i}(K) = 1$ or $p_i \nmid [L : E]$ (as holds whenever $p_j \not\equiv 1 \pmod{p_i}$ for all $j \neq i$ since $L = E(\zeta_s)$ has E-degree dividing $\varphi(s)$).

Thus, ϕ is injective if for each $i \in \{1, \ldots, k\}$ either $\mu_{p_i}(K) = 1$ or $p_j \not\equiv 1 \pmod{p_i}$ for each $j \in \{1, \ldots, k\}$ with $j \neq i$. □

One of the consequences of Proposition 3.3.3 is that if K has a real embedding and n is odd, then Question 1.1.4 has an affirmative answer because $\mu_p(K) = 1$ for all primes p dividing n. Furthermore, if n is a power of 2 or if n is odd and $q \not\equiv 1 \pmod{p}$ for all distinct prime factors p, q of n, then we also have an affirmative answer to Question 1.1.4.

The proof of Proposition 3.3.3 informs us that the injectivity of ϕ fails whenever both $\mu_p \subset K$ and $p \mid \big[K(\zeta_n) : K\big(\zeta_{p^{\text{ord}_p(n)}}\big)\big]$ for any prime $p \mid n$. Therefore, a completely different approach to Question 1.1.4 is needed for this more difficult class of cases. Nevertheless, Proposition 3.3.3 yields Case (2) of Theorem 3.1.4.

3.4 Disjointness from Cyclotomic Fields

We know that the approach in Section 3.3 reducing to the Kummer theory case fails if $8 \mid n$ and the 2-power cyclotomic extensions are not cyclic over K (this is why Proposition 3.3.3 provides an affirmative answer to Question 1.1.4 when n is a power of 2 and $i \in K$). At the opposite extreme of Kummer theory, we now consider the case $K \cap \mathbf{Q}(\zeta_n) = \mathbf{Q}$. In this setting, we can extract more information about the 2-power cyclotomic extensions and their subfields. In an unpublished note by Conrad [3], this case of Question 1.1.4 was answered completely. Here, we present a brief overview of the results. *For the remainder of this section, assume* $K \cap \mathbf{Q}(\zeta_n) = \mathbf{Q}$.

In the most interesting case $8 \mid n$ complications to Question 1.1.4 arise from non-cyclic 2-power cyclotomic field extensions (reminiscent of the Grunwald–Wang theorem). This phenomenon turns out to be related to whether there is more than one quadratic subextension of $K(\alpha)/K$ where $\alpha^n = a$. The uniqueness of such a subextension turns out to be a sufficient condition for an affirmative answer whenever n is even (though determining when such uniqueness holds in reasonable generality is a rather nontrivial matter, as we shall see).

It is obvious by degree reasons that there is a unique quadratic subextension of the degree-n extension $K(\alpha)/K$ when $\mathrm{ord}_2(n) = 1$, and with a bit more work one can show this uniqueness holds for any even n when $-a$ is not a square in K. This is optimal:

Lemma 3.4.1. *If n is divisible by 4 and $-a$ is a square in K, there are distinct quadratic subextensions of $K(\alpha)/K$.*

Proof. Note that -1 cannot be a square in K since $-a$ is a square in K but a is not (as n is even and $X^n - a$ is irreducible) Write $-a = h^2$ with $h \in K^\times$. Since $X^n - a = (X^{n/4})^4 + h^2$ is irreducible over K, neither $2h$ nor $-2h$ can be squares in K by Theorem 3.1.2. Since $(\alpha^{n/4})^4 = -h^2$, we see that $(\alpha^{n/4})^2 = \pm ih$. Since $\mp i = 2/(1 \pm i)^2$, we have for some pair of signs that

$$\alpha^{n/4} = \pm \frac{\sqrt{2h}}{1 \pm i},$$

and hence $K(i, \sqrt{2h}) = K(\alpha^{n/4})$, a quartic extension of K. Since neither -1 nor $2h$ are squares in K, this gives rise to quadratic subextensions $K(i)/K$ and $K(\sqrt{2h})/K$. Since $K(i, \sqrt{2h})/K$ is quartic, this forces $K(i)/K$ and $K(\sqrt{2h})/K$ to be distinct. □

Remark 3.4.2. The reasoning in [3] for why the presence of distinct quadratic subextensions of $K(\alpha)/K$ is an obstruction to an affirmative answer to Question 1.1.4 is reminiscent of how the existence of distinct quadratic subextensions of $K(\zeta_n)/K$ is an obstruction to an affirmative answer in the Grunwald–Wang theorem (Theorem 2.2.2) when $K(\zeta_{2^e})/K$ is non-cyclic, with 2^e the 2-part of n (and $8 \mid n$).

The situation is sometimes salvageable when *both* $-a$ and $-b$ are squares in K, by careful group-theoretic study of the subextensions of $K(\alpha)/K$ and $K(\beta)/K$ via considerations of their Galois closures. However, Conrad's analysis reveals that there are two classes of examples with *negative* answers to Question 1.1.4.

Example 3.4.3. Suppose n is divisible by 8 (so -1 and ± 2 are not squares in K, since $K \cap \mathbf{Q}(\zeta_8) = \mathbf{Q}$ and $\mathbf{Q}(\zeta_8) \supset \mathbf{Q}(i), \mathbf{Q}(\sqrt{2}), \mathbf{Q}(\sqrt{-2})$). Let $h \in K^\times$ be such that h is not a p-th power in K for any odd prime p dividing n and assume that all of $\pm h$ and $\pm 2h$ are not squares in K. Let $g := 2^{n/4}h$ (so $\pm g$ and $\pm 2g$ are not squares in K either). Define $a := -h^2$ and $b := -g^2 = 2^{n/2}a$.

By Theorem 3.1.2, $X^n - a$ and $X^n - b$ are irreducible over K. Note that $\alpha^{n/2}$ is a square root of $-h^2 = \alpha^n$, so $i \in K(\alpha)$. Letting $\beta = (1+i)\alpha$, we have that $\beta^n = 2^{n/2}\alpha^n = b$, so $K(\alpha) = K(\beta)$. One can show that b^j/a is not an n-th power in K for any j coprime to n [3, Example 2.3].

An example of this situation with $K = \mathbf{Q}$ is given by $X^8 + h^2$ and $X^8 + 16h^2$ for h any odd squarefree integer.

Example 3.4.4. Suppose n is divisible by 16. Let $h \in K^\times$ such that h is not a p-th power in K for any odd prime p dividing n. Let $g := 2^{n/8}h$. Define $a := -h^4$ and $b := -g^4 = 2^{n/2}a$ and let $e = \mathrm{ord}_2(n) \geq 4$.

If both $\pm h$ are not 2^{e-3}-th powers in K, then both $\pm h$ are at most 2^{e-4}-th powers in K; let f and f' be the maximal integers such that $h \in K^{2^f}$ and $h \in K^{2^{f'}}$. Then $h = s^{2^f}$ and $-h = (s')^{2^{f'}}$ for non-squares $s, s' \in K^\times$. If $f > 0$ then $h = (-s)^{2^f}$, so $-s$ is not a square in K by maximality of f. If $f' > 0$, then $h = -(s')^{2^{f'}}$ with $\pm s'$ both non-squares in K by the same argument. If $f = 0$ and $f' = 0$, then $-s = s'$ is not a square in K. Therefore, $h = \pm s^{2^f}$ for some sign, some $s \in K^\times$, and some integer $0 \leq f \leq e-4$ such that $\pm s$ are both non-squares in K. In this case, we make the *additional assumption* that neither of $\pm 2s$ are squares in K.

Since ± 2 are not squares in K, h^4 and g^4 cannot be written as $h^4 = 4k^4$ or $g^4 = 4\ell^4$ for $k, \ell \in K^\times$. Thus, by Theorem 3.1.2, $X^n - a$ and $X^n - b$ are irreducible over K. Note that $\alpha^{n/2} = \pm ih^2$, so $i \in K(\alpha)$. Letting $\beta = (1+i)\alpha$, we have that $\beta^n = 2^{n/2}\alpha^n = b$ and $K(\alpha) = K(\beta)$. One can show that b^j/a is not an n-th power in K for any j coprime to n [3, Example 2.4].

An example of this situation with $K = \mathbf{Q}$ is given by $X^{16} + h^4$ and $X^{16} + 256h^4$ for h any odd squarefree integer.

Somewhat surprisingly, given the intricate nature of the preceding two constructions, they are the *only* cases that provide negative answers to Question 1.1.4 when $K \cap \mathbf{Q}(\zeta_n) = \mathbf{Q}$:

Theorem 3.4.5. *In the setting of Question 1.1.4, if $K \cap \mathbf{Q}(\zeta_n) = \mathbf{Q}$ then b^j/a is an nth power for some positive integer j coprime to n if and only if a and b do not arise from the constructions in Example 3.4.3 and Example 3.4.4. In particular, the answer is affirmative if $8 \nmid n$ or if one of $-a$ or $-b$ is not a square in K.*

This is proved by a rather long induction on $\mathrm{ord}_2(n)$, the difficulty lying in navigating around the known counter-examples. For instance, if $\mathrm{ord}_2(n) \geq 4$ and $a = -h^2$ with one of $\pm h$ a square in K (so avoiding Example 3.4.3), the subextensions of $K(\alpha)/K$ with degree divisible by 8 turn out to be precisely $K(\alpha^m)$ for $m \mid n$ such that $8 \mid n/m$. Thus, such subextensions are uniquely determined by their degree over K and that enables one to apply an inductive process using $n/2$ and $K(\alpha^2)/K$ (taking much care to avoid Example 3.4.4!).

Bibliography

[1] Emil Artin and John Tate. *Class field theory*. W. A. Benjamin, Inc., New York-Amsterdam, 1968.

[2] John W.S. Cassels and Albrecht Fröhlich. *Algebraic Number Theory: Proceedings of an Instructional Conference Organized by the London Mathematical Society (a NATO Advanced Study Institute) with the Support of the International Mathematical Union*. London Mathematical Society, 2010.

[3] Brian Conrad. Unpublished note, 2011.

[4] Ewan Delanoy. Isomorphism problem for two radical extensions. MathOverflow. URL: https://mathoverflow.net/q/188165 (version: 2017-04-13).

[5] Wilhelm Grunwald. Ein allgemeines Existenztheorem für algebraische Zahlkörper. *J. Reine Angew. Math.*, 169:103–107, 1933.

[6] Helmut Hasse. Zum Existenzsatz von Grunwald in der Klassenkörpertheorie. *J. Reine Angew. Math.*, 188:40–64, 1950.

[7] David Hilbert. Die Theorie der algebraischen Zahlkörper. *Jahresber. Deutsch. Math.-Verein.*, 4:175–535, 1894/95.

[8] Serge Lang. *Algebra*. Graduate Texts in Mathematics. Springer New York, 2005.

[9] Martin Luedtke. The Grunwald–Wang Theorem. Part III Essay, University of Cambridge, May 2013.

[10] P. Roquette. *The Brauer-Hasse-Noether Theorem in Historical Perspective*. Schriften der Mathematisch-naturwissenschaftlichen Klasse. Springer Berlin Heidelberg, 2006.

[11] Shianghaw Wang. A counter-example to Grunwald's theorem. *Ann. of Math. (2)*, 49:1008–1009, 1948.

[12] Shianghaw Wang. On Grunwald's theorem. *Ann. of Math. (2)*, 51:471–484, 1950.

[13] George Whaples. Non-analytic class field theory and grunwalds theorem. *Duke Math. J.*, 9(3):455–473, 09 1942.