The Grunwald–Wang Theorem

Hari Senthilkumar

Abstract

The Grunwald–Wang theorem is a local-to-global theorem in algebraic number theory. The theorem is about whether local cyclic extensions of number fields can be patched together into one global cyclic extension with the expected degree. Grunwald originally claimed that the answer was always yes, but Wang found a rare and important exception caused by powers of 2. This paper builds up to the theorem through things liek cyclic extensions and the Chebotarev density theorem.

1 The Local-to-Global Problem

A recurring question in number theory is whether solving a problem locally everywhere implies solving it globally. For example, suppose an element $a \in \mathbb{Q}^\times$ is an n-th power in every p-adic field $\mathbb{Q}_p$. Must a already be an n-th power in $\mathbb{Q}$? More generally, suppose we prescribe cyclic extensions over finitely many completions of a number field. Can we find one global cyclic extension that produces exactly those local extensions?

The Grunwald–Wang theorem answers this question. In nearly all cases, local cyclic data can be realized globally. The only obstruction occurs in a special 2-primary situation. This makes the theorem especially interesting: it is not a vague failure of local-to-global reasoning, but a very precise failure caused by the arithmetic of 2-power roots of unity.

Definition 1.1. *A **number field** is a finite extension $K/\mathbb{Q}$. Its elements behave like algebraic numbers, and its arithmetic generalizes the arithmetic of rational numbers.*

Definition 1.2. *A **place** v of a number field K is an equivalence class of absolute values on K. There are two main types:*

- ***finite places**, which come from prime ideals of the ring of integers of K;*
- ***infinite places**, which come from embeddings of K into $\mathbb{R}$ or $\mathbb{C}$.*

The completion of K at v is denoted K_v. For example, when $K = \mathbb{Q}$ and v corresponds to a prime p, the completion is the p-adic field $\mathbb{Q}_p$.

The phrase 'local" means 'after passing to K_v for some place v." The phrase 'global" means 'over the original number field K." Thus the Grunwald–Wang theorem compares arithmetic over K with arithmetic over its completions K_v.

2 Local Fields and Local Powers

The completions K_v are local fields. These fields are simpler than number fields in some ways because their elements can be measured by a single valuation.

Definition 2.1. *A **nonarchimedean local field** is a field complete with respect to a discrete valuation and having finite residue field. Examples include $\mathbb{Q}_p$ and finite extensions of $\mathbb{Q}_p$.*

If K_v is a nonarchimedean local field, then it has a valuation ring $\mathcal{O}_v$, a maximal ideal $\mathfrak{m}_v$, a residue field $\kappa_v = \mathcal{O}_v/\mathfrak{m}_v$, and a uniformizer π_v. Every nonzero element of K_v can be written uniquely as $[\ \mathrm{x}{=}\mathrm{u}\pi_v^r,]where\mathrm{u} \in \mathcal{O}_v^\times$ is a unit and $r \in \mathbb{Z}$. Therefore, asking whether x is an n-th power has two parts: the valuation r must be divisible by n, and the unit u must be an n-th power unit.

The most important tool for passing from the residue field to the local field is Hensel's lemma.

Theorem 2.2 (Hensel's lemma)**.** *Let F be a complete nonarchimedean field with valuation ring $\mathcal{O}$ and maximal ideal $\mathfrak{m}$. Suppose $f(X) \in \mathcal{O}[X]$. If $\overline{a} \in \mathcal{O}/\mathfrak{m}$ is a simple root of $\overline{f}(X)$, then $\overline{a}$ lifts to a root $a \in \mathcal{O}$ of $f(X)$.*

In practical terms, Hensel's lemma says that a simple solution modulo a prime often lifts to an actual p-adic solution.

Proposition 2.3. *Let p be a prime and let $n \geq 1$ with $p \nmid n$. If $u \in \mathbb{Z}_p^\times$ satisfies $[\ u{\equiv}\ 1 \pmod p,]thenuisann{-}thpowerin Z_p^\times$.*

Proof. Consider $f(X) = X^n - u$. Since $u \equiv 1 \pmod p$, we have $[\ \mathrm{f(1)}{=}\mathrm{1\text{-}u}{\equiv}\ 0 \pmod p.]Also, [f'(1) = n,]whichisnonzeromodulopbecausep \nmid n$. Therefore 1 is a simple root modulo p, so Hensel's lemma lifts it to a root $\alpha \in \mathbb{Z}_p$ satisfying $\alpha^n = u$. □

This local lifting principle is one reason local fields are manageable. The difficulty in the Grunwald–Wang theorem does not come from the local fields individually; it comes from trying to make several local conditions compatible with one global object.

3 Cyclic Extensions, Roots of Unity, and Kummer Theory

The Grunwald–Wang theorem is usually stated using cyclic field extensions.

Definition 3.1. *A finite extension L/K is **Galois** if it has enough automorphisms to reflect all of its algebraic symmetries. Its automorphism group is denoted* $\mathrm{Gal}(L/K)$.

Definition 3.2. *A finite Galois extension L/K is called **cyclic** if its Galois group* $\mathrm{Gal}(L/K)$ *is a cyclic group. For example, a cyclic extension of degree n has Galois group isomorphic to $\mathbb{Z}/n\mathbb{Z}$.*

Definition 3.3. *A **biquadratic extension** is a Galois extension L/K whose Galois group is $[$* $\mathrm{Gal}(L/K) \cong \mathbb{Z}/2\mathbb{Z}{\times}\mathbb{Z}/2\mathbb{Z}.]Equivalently, itisusuallyobtainedbyadjoiningtwoindependentsquareroots$: $[L = K(\sqrt{a}, \sqrt{b}).]Abiquadraticextensionhasdegree4, butitisnotcyclic.$

Roots of unity control many cyclic extensions.

Definition 3.4. *For an integer $n \geq 1$, let $[\ \mu_n = \zeta \in \overline{K}^\times : \zeta^n = 1]bethegroupofn{-}throotsofunity. A**primitive** n-t whose powers generate all of μ_n.*

The relevant bridge between powers and cyclic extensions is Kummer theory.

Theorem 3.5 (Kummer theory, simplified form)**.** *Let F be a field whose characteristic does not divide n, and suppose F contains a primitive n-th root of unity. Then cyclic extensions of F of degree dividing n are closely related to adjoining n-th roots: [$F(\sqrt[n]{a})/F$.]In this setting, questions about cyclic extensions can*

This is the first major reason the Grunwald–Wang theorem can be studied through n-th powers. If a field contains enough roots of unity, then cyclic extensions of exponent dividing n are built by adjoining n-th roots.

4 Chebotarev Density and the Clean Case

The next tool is the Chebotarev density theorem. We only need one consequence of it, but it is important to understand what it says.

Definition 4.1. *Let L/K be a finite Galois extension of number fields. A prime of K is said to* ***split completely*** *in L if, after factoring it in the ring of integers of L, it breaks into the largest possible number of distinct primes. Intuitively, such a prime looks as simple as possible inside the extension L.*

Theorem 4.2 (Chebotarev density theorem, simplified form)**.** *Let L/K be a finite Galois extension. The primes of K are distributed among the conjugacy classes of* $\mathrm{Gal}(L/K)$*. In particular, the set of primes that split completely in L has density [$1_{\overline{[L:K].]Therefore, if almost all primes of}}$ K split completely in L, then [L:K]=1, s*

This theorem gives a clean proof of the local-to-global statement when the base field already contains the relevant roots of unity.

Theorem 4.3. *Let K be a number field containing a primitive n-th root of unity. If $a \in K^\times$ is an n-th power in K_v for all but finitely many places v, then a is an n-th power in K.*

Proof. Choose $\beta \in \overline{K}$ with $\beta^n = a$. Since K contains the n-th roots of unity, the polynomial [$\mathrm{X}^n - a$]*splits completely over* $\mathrm{K}(\beta)$.

Now suppose a is an n-th power in K_v for all but finitely many v. Then $X^n - a$ has a root in K_v for almost all v. Because the roots differ only by multiplying by n-th roots of unity already contained in K, the polynomial actually splits completely locally for almost all v. Thus almost all places split completely in $K(\beta)/K$.

By Chebotarev density, a nontrivial extension cannot have almost all primes split completely. Therefore $K(\beta) = K$, so $\beta \in K$ and $a = \beta^n \in K^{\times n}$. □

This proof explains the main idea behind the theorem: local n-th power information forces splitting behavior in a Kummer extension, and Chebotarev density then forces the extension to be trivial. The Grunwald–Wang theorem is harder because K may not contain the necessary roots of unity, especially the relevant powers of 2.

5 The Grunwald Problem

We can now state the problem that Grunwald tried to solve.

Definition 5.1. *Let K be a number field, let S be a finite set of places of K, and let $n \geq 1$. Define [K(n,S)=a∈ $K^\times$: $a \in K_v^{\times n}$ for every $v \notin S$.]Thus K(n,S)consistsofglobalelementsthatbecomelocaln−thpowersout*

If local information perfectly determined global information, then we would always have [K(n,S)=$K^{\times n}$.]*Thatis, if a is an n−th power locally almost everywhere, then a should be an n−th power globally. Grunwal*

There is also an equivalent extension version.

Definition 5.2. *Let S be a finite set of places of K. To prescribe **local cyclic data** means that for each $v \in S$, we choose a cyclic extension [L_v/K_v.]TheGrunwaldproblemaskswhetherthereisaglobalcyclicextensio S, the extension L/K produces the prescribed local extension L_v/K_v.*

The power version and the cyclic extension version are connected by Kummer theory and class field theory. For the purposes of this paper, the important point is this: the same rare 2-primary obstruction appears in both versions.

6 The Special 2-Primary Case

The exceptional case is caused by 2-power roots of unity. We now define it carefully.

Let ζ_{2^s} be a primitive 2^s-th root of unity. For $s \geq 2$, define [$\eta_s = \zeta_{2^s} + \zeta_{2^s}^{-1}$.]*Thiselementliesinthemaximalrealsu* For example, [$\eta_2 = \zeta_4 + \zeta_4^{-1} = i + (-i) = 0,$]*and*[$\eta_3 = \zeta_8 + \zeta_8^{-1} = \sqrt{2}$.]

Definition 6.1. *Let K be a number field. Define s_K to be the largest integer $s \geq 2$ such that [$Q(\eta_s) \subseteq K$.]Equivalently,Kcontainstherealpartofthe 2^s-th cyclotomic field, but not necessarily the next one.*

Definition 6.2. *A **2-adic place** of K is a place lying above the rational prime 2. Let S_K be the set of 2-adic places v of K for which [$K_v(\zeta_{2^{s_K+1}})/K_v$]isbiquadratic.*

The word "biquadratic" is the key. If the relevant 2-power cyclotomic extension is cyclic, then the usual local-to-global principle survives. If it is biquadratic, then Wang's obstruction can appear.

Definition 6.3. *The triple (K, S, n) is in the **special case** if:*

1. *$K(\zeta_{2^{s_K+1}})/K$ is biquadratic;*
2. *2^{s_K+1} divides n;*
3. *the finite set S contains every place in S_K.*

The condition $2^{s_K+1} \mid n$ says that n is divisible by a sufficiently high power of 2. Thus the exceptional case never occurs for odd n.

7 The Grunwald–Wang Theorem

We can now state the theorem in its n-th power form.

Theorem 7.1 (Grunwald–Wang theorem, n-th power form)**.** *Let K be a number field, let S be a finite set of places of K, and let $n \geq 1$.*

1. *If (K, S, n) is not in the special case, then [K(n,S)=$K^{\times n}$.]Inotherwords, everyelementofKthatisann−thpow*

"‘

2. *If (K, S, n) is in the special case, then there is exactly one extra obstruction class:*

$$K(n, S)/K^{\times n} \cong \mathbb{Z}/2\mathbb{Z}.$$

A representative of the nontrivial class is

$$a_{K,n} = (2 + \eta_{s_K})^{n/2}.$$

Thus

$$K(n, S) = K^{\times n} \sqcup a_{K,n} K^{\times n}.$$

‘‘

The theorem says that the local-to-global principle for n-th powers is almost always true. When it fails, it fails in the smallest possible way: there is one extra class, and it has order 2.

The cyclic extension version says the same thing in different language.

Theorem 7.2 (Grunwald–Wang theorem, cyclic extension form)**.** *Let K be a number field, let S be a finite set of places, and suppose that for each $v \in S$ we are given a cyclic extension L_v/K_v whose degree divides n. Outside the special case, there exists a cyclic extension L/K of degree dividing n whose completion at every $v \in S$ matches the prescribed local extension. In the special case, one may need to allow degree dividing $2n$ instead of degree dividing n.*

This is the corrected version of Grunwald’s original claim. Grunwald’s theorem missed the special 2-primary exception. Wang’s work identified exactly when and why the correction is necessary.

8 Wang’s Counterexample over $\mathbb{Q}$

The most famous example occurs over $K = \mathbb{Q}$ with $n = 8$.

For $K = \mathbb{Q}$, we have

$$s_{\mathbb{Q}} = 2,$$

because

$$\eta_2 = 0 \in \mathbb{Q},$$

but

$$\eta_3 = \sqrt{2} \notin \mathbb{Q}.$$

The relevant exceptional element is therefore

$$a_{\mathbb{Q},8} = (2 + \eta_2)^{8/2} = 2^4 = 16.$$

Example 8.1 (Wang’s counterexample)**.** *The rational number* 16 *is an eighth power in $\mathbb{Q}_p$ for every odd prime p, but it is not an eighth power in $\mathbb{Q}$ and not an eighth power in $\mathbb{Q}_2$.*

Proof. First, 16 is not an eighth power in $\mathbb{Q}$. Indeed, if $x^8 = 16 = 2^4$ for some $x \in \mathbb{Q}^\times$, then comparing the exponent of 2 on both sides would require an integer multiple of 8 to equal 4, which is impossible.

The same valuation argument shows that 16 is not an eighth power in $\mathbb{Q}_2$. If $x^8 = 16$, then

$$v_2(x^8) = 8v_2(x)$$

would have to equal

$$v_2(16) = 4,$$

which is impossible because 4 is not divisible by 8.

Now let p be an odd prime. We show that 16 is an eighth power in $\mathbb{Q}_p$. It is enough to show that 16 is an eighth power modulo p, because Hensel's lemma then lifts the solution to $\mathbb{Z}_p$.

The group $\mathbb{F}_p^\times$ is cyclic of order $p-1$. In a cyclic group of order m, an element b is an eighth power if and only if

$$b^{m/\gcd(8,m)} = 1.$$

Here $b = 16 = 2^4$ and $m = p-1$. Let $g = \gcd(8, p-1)$. If $g = 2$ or $g = 4$, then

$$16^{(p-1)/g} = 2^{4(p-1)/g}$$

is automatically 1 modulo p because the exponent is a multiple of $p-1$. If $g = 8$, then $p \equiv 1 \pmod 8$. In this case 2 is a quadratic residue modulo p, so

$$2^{(p-1)/2} \equiv 1 \pmod p.$$

Thus

$$16^{(p-1)/8} = 2^{(p-1)/2} \equiv 1 \pmod p.$$

So 16 is an eighth power modulo every odd prime p. Since the derivative of $X^8 - 16$ at a nonzero root is not divisible by p, Hensel's lemma lifts the root to $\mathbb{Q}_p$.

Therefore 16 is an eighth power locally at every odd prime, but not globally and not at 2. This is exactly the kind of exception described by the Grunwald–Wang theorem. □

This example explains why the set S matters. If S contains the place 2, then 16 is an eighth power in $\mathbb{Q}_p$ for every $p \notin S$, but it is not an eighth power in $\mathbb{Q}$. Thus

$$16 \in \mathbb{Q}(8, S),$$

but

$$16 \notin \mathbb{Q}^{\times 8}$$

References

[1] E. Artin and J. Tate, *Class Field Theory*, AMS Chelsea Publishing, Providence, RI, 2009.

[2] W. Grunwald, "Ein allgemeines Existenztheorem für algebraische Zahlkörper," *Journal für die reine und angewandte Mathematik* 169 (1933), 103–107.

[3] J. S. Milne, *Class Field Theory*, online lecture notes.

[4] J. Neukirch, *Algebraic Number Theory*, Springer, Berlin, 1999.

[5] J.-P. Serre, *Local Fields*, Graduate Texts in Mathematics 67, Springer, New York, 1979.

[6] S. Wang, "A Counter-Example to Grunwald's Theorem," *Annals of Mathematics* 49 (1948), 1008–1009.

[7] S. Wang, "On Grunwald's Theorem," *Annals of Mathematics* 51 (1950), 471–484.

[8] B. Conrad, *Lifting Global Representations with Local Properties*, Appendix A, 2011.

[9] R. Zhang, *The Grunwald–Wang Theorem and Isomorphic Radical Extensions: Why 2 is the Evil Prime*, undergraduate honors thesis, Stanford University, 2017.