Ramification Constraints and the Class Field Property in Cyclic Extensions

Naina Praveen

Feb 2026

These notes are from the fourth lecture I gave at the London Number Theory Study group in 2026 on Global Class Field Theory. These notes follow §5.2-6.1 from Akshay Venkatesh's notes on "Global Class Field Theory, after Hilbert and Furtwängler".

1 Introduction

Let's go back to the start. Let k be a number field and K/k be a finite abelian extension. In Lecture 1, we defined a class field as an extension where the equality

$$[c : NC] = [K : k]$$

holds. We previously proved the inequality $[c : NC] \leq [K : k]$ using zeta functions and densities for any abelian extension. This analytic proof holds for any cyclic extension, regardless of ramification. In this lecture, we prove the reverse inequality (in the unramified case; the ramified case is treated in §7).

However, counting the norm group NC is difficult. Thus, in Lectures 2 and 3, we translated the problem from counting ideals to counting units, which are easier to understand. Specifically, we established that the "capitulation kernel"[1]

$$\ker : c \longrightarrow C \cong \frac{\text{norm 1 units in } U}{U^{1-\sigma}} := \frac{U^{N=1}}{U^{1-\sigma}}. \tag{1}$$

Using this isomorphism, we showed in Lecture 1 that

$$\frac{\#(\ker : c \longrightarrow C)}{[u : NU]} = [K : k],$$

where K/k was cyclic unramified of prime degree ℓ (and $\zeta_\ell \notin K$). In Lecture 2, we showed that

$$\frac{[\text{Norm 1 units of } U\text{: } U^{1-\sigma}]}{[u : NU]} = [K : k]. \tag{2}$$

[1] Capitulation derives from the Latin *caput* (head), evolving to *capitulum* (chapter heading) and the verb *capitulare* (to distinguish by chapters). This came into English as *capitulation*, originally meaning "drawing up into chapters." Turns out that in the 1600's, what people were most busy drawing up into chapters were articles of surrender, leading to the definition of "yielding on stipulated terms", from where get the modern definition "to comply/concede".

The ratio in (2) holds for any cyclic extension, regardless of finite ramification. We will use this to quantify how the capitulation kernel changes when ramification is introduced and see that this imposes certain constraints — specifically, that some ramified extensions cannot exist if the base units are too "large" (this non-existence result will force us to use specific "auxiliary primes" in the Existence Theorem in §7). Lastly, we prove the equality $[c : NC] = [K : k]$ for unramified extensions where $\#c = \ell = [K : k]$, using (2) to calculate the size of the "ambiguous classes" (C^σ).

2 §5.2 Consequences of Ramification

For reference, we use the following version of Hilbert 90:

Theorem 2.1 (Hilbert's 90)**.** *Let K/k be a cyclic Galois extension with Galois group $G = \langle\sigma\rangle$. If an element $\beta \in K^\times$ has norm $N_{K/k}(\beta) = 1$, then there exists an element $\alpha \in K^\times$ such that:*

$$\beta = \alpha^{1-\sigma} = \frac{\alpha}{\sigma(\alpha)}.$$

Notation. For any ramified prime $\mathfrak{p}$ in k, the ideal $\widetilde{\mathfrak{p}}$ is defined as the product of the prime ideals of K lying above $\mathfrak{p}$:

$$\widetilde{\mathfrak{p}} := \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}.$$

This is a σ-fixed ideal in K (though not necessarily in k).

We prove the following proposition:

Proposition 2.2. *Let K/k be a cyclic extension of number fields of degree $m = [K : k]$ and Galois group $\langle\sigma\rangle$. Assume K/k is unramified at all archimedean places but allow ramification at a finite set of primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ of k with ramification indices $e_1, \ldots, e_s$ respectively. Then the following equality holds:*

$$\frac{\#(\ker(c \to C)) \cdot \prod_{i=1}^{s} e_i}{m} = \#X \cdot [u : NU], \tag{3}$$

where X is the subgroup of the relative class group $\overline{C} = C/im(c)$ spanned by various σ-fixed classes $\widetilde{\mathfrak{p}}_1, \ldots, \widetilde{\mathfrak{p}}_s$ arising from ramified primes.

One may ask why the set X is defined in the relative class group and not just C. The reason this makes sense is because when we were dealing with unramified extension, σ-fixed ideals only came from k. However, if the extension is ramified, then there are other σ-fixed classes (like $\widetilde{\mathfrak{p}}$) that are σ-fixed, but aren't extended form k. By passing to the relative class group, we are trying to capture these new σ-fixed ideals. Heuristically, this formula makes sense because when there is ramification, norms can only be e^{th} powers, which restricts the size of NU, increasing the index $[u : NU]$. We would like this index to grow like $\prod_i e_i$, however, as the unit group is fairly rigid, there are fractional ideals that are like $1/e^{th}$ powers that are no longer principal because there aren't enough units, and X capture precisely this phenomenon.

Proof. We prove the proposition by establishing the following exact sequence:

$$0 \to \ker(c \to C) \xrightarrow{\alpha} \frac{U^{N=1}}{U^{1-\sigma}} \xrightarrow{\beta} \prod(\mathbb{Z}/e_i) \xrightarrow{\gamma} X \to 0$$

- *Definition of α:* Take a class $[\mathfrak{a}]$ in the kernel. This means $\mathfrak{a}$ is an ideal in k, but in K, it becomes principal, i.e., $\mathfrak{a}\mathcal{O}_K = (Y)$. Since $\mathfrak{a}$ is in k, it is σ-fixed. Thus $(Y)^\sigma = (Y)$. This implies $Y^\sigma = Y \cdot u^{-1}$ for some unit u. Rearranging gives $u = Y^{1-\sigma}$. This implies that $N(u) = N(Y^{1-\sigma}) = 1$, and so we define $\alpha([\mathfrak{a}]) = [u]$.

- *Definition of β:* Take a class $[u] \in U^{N=1}/U^{1-\sigma}$. As $N(u) = 1$, by Hilbert 90, there exists $Y \in K^\times$ such that $u = Y^{1-\sigma}$. For each ramified prime $\mathfrak{p}_i$, pick any prime $\mathfrak{P}$ over it and compute $v_i := v_{\mathfrak{P}_i}(Y)$ (note that because $\widetilde{\mathfrak{p}}$ is σ-fixed, any prime $\mathfrak{P} \mid \mathfrak{p}_i$ yields the same valuation). Set $\beta([u]) = (v_1 \mod e_i, \ldots, v_s \mod e_s)$.

- *Definition of γ:* Take a tuple $(a_1, \ldots, a_s)$ and assign it to the class of the ideal I, where $I = \prod_i \widetilde{\mathfrak{p}}_i^{a_i}$.

We now establish exactness.

◇ *Injectivity of α:* To show injectivity, suppose $\alpha([\mathfrak{a}]) = 1$ in the quotient group. This means the unit $u = Y^{1-\sigma}$ is of the form $\epsilon^{1-\sigma}$ for some $\epsilon \in U_K$. Then $Y^{1-\sigma} = \epsilon^{1-\sigma}$, which yields

$$(Y\epsilon^{-1})^{1-\sigma} = 1 \implies \sigma(Y\epsilon^{-1}) = Y\epsilon^{-1}.$$

Since $\gamma = Y\epsilon^{-1}$ is fixed by σ, it must lie in the base field k. So $\alpha = \gamma\epsilon$ with $\gamma \in k$, and thus

$$\mathfrak{a}\mathcal{O}_K = (Y) = (\gamma\epsilon) = (\gamma)\mathcal{O}_K$$

(since ϵ is a unit, it doesn't change the ideal). Since ideals extend uniquely from k, this implies $\mathfrak{a} = (\gamma)$. Because $\mathfrak{a}$ is generated by an element in k, it is principal in the class group c. Thus $[\mathfrak{a}] = 1$.

◇ *$im(\alpha) = ker(\beta)$:* We first show $\mathrm{im}(\alpha) \subseteq \ker(\beta)$. Let $x = \alpha([\mathfrak{a}])$ for some $\mathfrak{a}$ in $\ker(c \to C)$. Then $\mathfrak{a}\mathcal{O}_K = (Y)$ for some $Y \in K$, so $\alpha([\mathfrak{a}]) = [Y^{1-\sigma}]$. We compute $\beta(x)$:

$$\begin{aligned}(Y) = \mathfrak{a}\mathcal{O}_K &= \prod \mathfrak{p}^{n_\mathfrak{p}}\mathcal{O}_K \\ &= \prod_{\text{ramified primes}} \widetilde{\mathfrak{p}}_i^{e_i \cdot n_\mathfrak{p}} \cdot \prod(\ldots).\end{aligned}$$

Since each power of $\widetilde{\mathfrak{p}}_i$ is divisible by e_i, it maps to 0 in $\prod \mathbb{Z}/e_i\mathbb{Z}$.

Conversely, let $\beta([u]) = 0$. As $u \in U^{N=1}$, Hilbert 90 implies $u = Y^{1-\sigma}$. Since $[u]$ is in the kernel of β, the valuation of Y is divisible by e_i at every ramified prime $\mathfrak{p}_i$. Further, as u is a unit, $(1) = (u) = (Y^{1-\sigma}) \implies (Y) = (Y)^\sigma$. We claim this means Y is extended from k.

Lemma 2.3. *Every σ-fixed ideal is extended from k if and only if its valuation at ramified primes is divisible by e_i.*

Proof. Every ramified prime extended from k is raised to the power e, so its valuation is divisible by e. Conversely, suppose an ideal J is σ-fixed and has valuations over ramified

primes divisible by e_i. The exponents in the factorisation of J over any fixed prime $\mathfrak{p}$ are identical (as it is σ-fixed), say k_i. As $e \mid k_i$ (so $k_i = e_i m_i$), we have

$$\begin{aligned} J &= \prod_{\mathfrak{P}|\mathfrak{p}_i,\text{ramified}} (\mathfrak{P}\cdots)^{k_1}\cdots(\mathfrak{P}'\cdots)^{k_s} \cdot \prod_{\mathfrak{P}|\mathfrak{p},\text{unramified}} (\mathfrak{Q}\cdots)(\mathfrak{Q}'\cdots) \\ &= \prod_{\mathfrak{p},\text{ ramified}} \mathfrak{p}^m \cdot \mathfrak{p}^{m'}\cdots \prod_{\mathfrak{p},\text{ unramified}} \mathfrak{q}^{v_{\mathfrak{Q}}}\cdot \mathfrak{q}'^{v_{\mathfrak{Q}'}}\cdots \\ &= (\mathfrak{p}^m \mathfrak{p}'^{m'}\cdots \mathfrak{q}^v \mathfrak{q}'^{v'}\cdots)\mathcal{O}_K \end{aligned}$$

which extends from k. □

The Lemma implies $(Y) = \mathfrak{a}\mathcal{O}_K$ for some $\mathfrak{a} \subset k$. Since $\mathfrak{a}$ extends to a principal ideal (Y), the class $[\mathfrak{a}]$ is in $\ker(c \to C)$, implying $\alpha([\mathfrak{a}]) = [Y^{1-\sigma}] = [u]$.

- *$im(\beta) = ker(\alpha)$:* Let $a = (a_1, \ldots, a_s) \in \prod_i (\mathbb{Z}/e_i\mathbb{Z})$. $a \in \ker(\gamma)$ if and only if $J = \prod \widetilde{\mathfrak{p}}^{a_i}$ is trivial in $C/\mathrm{im}(c)$. For $[J] = 1$ in $C/\mathrm{im}(c)$, J must differ from a principal ideal (Y) by a factor extended from the base field k, i.e., $(Y) = J \cdot \mathfrak{a}\mathcal{O}_K$. Since J is a product of σ-fixed $\widetilde{\mathfrak{p}}_i$ and $\mathfrak{a}\mathcal{O}_K$ is σ-fixed (extended from k), we have $(Y)^\sigma = (Y)$, implying $Y^{1-\sigma} = u$ is a unit. The equation $(Y) = J \cdot \mathfrak{a}\mathcal{O}_K$ holds if and only if their valuations match at every prime. Focusing on ramified primes:

$$\begin{aligned} v_{\mathfrak{P}_i}(Y) &= v_{\mathfrak{P}_i}(J) + v_{\mathfrak{P}_i}(\mathfrak{a}\mathcal{O}_K) \\ &= a_i + 0 \mod e_i \\ &= a_i \mod e_i \end{aligned}$$

This is true if and only if $\beta([u]) = (a_1, \ldots, a_s)$, so $a \in \mathrm{im}(\beta)$.

With exactness proved, we use the first isomorphism theorem to get

$$\#(\ker(c \to C)) \cdot \prod_i e_i = [K : k] \cdot [u : NU] \cdot \#X,$$

where we use (2) to substitute $\#U^{N=1}/U^{1-\sigma} = [K : k] \cdot [u : NU]$. □

Application:

We see that (3) constrains the types of abelian extensions we can build.

Suppose $k = \mathbb{Q}(\sqrt{2})$. As this is a PID, it has class number 1. Thus, $\#\ker(c \to C) = 1$. Suppose, for the sake of contradiction, that we wish to build a cubic abelian extension ramified only at a single prime $\mathfrak{p} = (3 - \sqrt{2})$. This requires $e = 3$. The LHS of (3) is $1 \cdot 3/3 = 1$. First, we check for local obstructions. As $N(\mathfrak{p}) = 7 \equiv 1 \mod e$. the residue field contains cube roots of unit, and so by Hensel's, the local field $k_\mathfrak{p}$ also contains cube roots of unity. So theoretically, we should be able to build a polynomial $x^3 - \pi$ (where π is a uniformiser) whose splitting field is cyclic and totally ramified.

Let us see why such a global extension is impossible. Using (3), we compute $[u : NU]$. For $\mathbb{Q}(\sqrt{2})$, the unit group is generated by -1 and $\epsilon = 1 + \sqrt{2}$. Thus $u = \{\pm\epsilon^n\}$. To compute $[u : NU]$, we check if ϵ is a global norm.

If $\epsilon \in N(K^\times)$, it must be a local norm at every completion (since $N_{L/K}(x) = \prod_{\mathfrak{P}|\mathfrak{p}} N_{L_\mathfrak{P}/K_\mathfrak{p}}(x)$). Since $\mathfrak{p} = (3-\sqrt{2})$ is totally ramified in K/k with $e = 3$, the Galois group acts trivially on the residue field $\mathcal{O}_K/\mathfrak{P} \cong \mathcal{O}_k/\mathfrak{p}$. Consequently, the local norm map is $N(y) = y \cdot y \cdot y = y^3 \mod \mathfrak{p}$. Thus, for ϵ to be a local norm at $\mathfrak{p}$, it must be a perfect cube modulo $\mathfrak{p}$.

As $(3-\sqrt{2})(3+\sqrt{2}) = 7$, $\mathcal{O}_k/\mathfrak{p} \cong \mathbb{F}_7$, where $\sqrt{2} \equiv 3$. Then, $\epsilon = 1+\sqrt{2} \equiv 1+3 \equiv 4 \mod 7$. However, the only cubes in $\mathbb{F}_7$ are $\{1, 6\}$. Therefore ϵ is not a local norm modulo $\mathfrak{p}$ and thus not a global norm. This means $NU \subset u$, with the units mapping surjectively onto $\mathbb{F}_7$ (as powers of $\epsilon \mod \mathfrak{p}$ cover the units). So, $[u : NU] = \#(\mathbb{F}_7^\times/\{\text{cubes}\}) = 6/2 = 3$. Substituting this into (3) yields a contradiction.

3 §6.1 Unramified extensions are class fields (when $\#c = \ell = [K : k]$)

Theorem 3.1. *Let $\#c = \ell = [K : k]$. Then every unramified extension is a class field.*

Proof. From (2), we have $\#\ker(c \to C) = \ell \cdot [u : NU]$. As ℓ is prime and the RHS is a multiple of ℓ, it must be that $\ker(c \to C) = c$, the zero map. Thus $[u : NU] = 1$.

To show $[c : NC] = \ell$, we must show NC is trivial. We use the fact that the norm map kills anything of the form $Y^{1-\sigma}$. Let $f : C \to C$ send I to $I^{1-\sigma}$, i.e., $I = I^\sigma$. If the kernel is zero, f is injective; as C is finite, f is bijective. Let C^σ be the set of ideal *classes* in C fixed by σ (so $[I]^\sigma = [I]$, which is not the same as $I^\sigma = I$). If we show C^σ is trivial, we show that every class is of the form $I^{1-\sigma}$, implying NC is trivial.

Pick $[I] \in C^\sigma$. Then $I^{1-\sigma} = (\theta)$ for some $\theta \in K$. We wish to move from ideal classes to ideals using Hilbert 90. Taking norms:

$$(N(\theta)) = (N(I^{1-\sigma})) = (1).$$

Since $N(\theta)$ generates the trivial ideal, it must be a unit. It is not necessarily 1, so we cannot apply Hilbert 90 immediately. However, as $[u : NU] = 1$, all units are norms. This means that we can write $N(\theta) = N(\eta)$ for some unit $\eta \in K^\times$. Define

$$\theta' = \theta \cdot \eta^{-1}.$$

Then,

$$\begin{aligned} N(\theta') = N(\theta) \cdot N(\eta)^{-1} = 1, \\ \implies I^{1-\sigma} = (\theta') \quad \text{with } N(\theta') = 1. \end{aligned}$$

Hilbert 90 implies the existence of $\beta \in K^\times$ such that $\theta' = \beta^{1-\sigma}$, so $I^{1-\sigma} = (\beta^{1-\sigma}) = (\beta)^{1-\sigma} \implies (I \cdot \beta^{-1})^{1-\sigma} = (1)$. Setting $J = I \cdot \beta^{-1}$, we see J and I belong to the same ideal class as they differ by a principal ideal. Since J is a σ-fixed ideal, it is extended from k. Thus $[I] = [J]$ comes from the class group c. Since $\ker(c \to C) = c$ is the zero map, $[I]$ is trivial. As $[I]$ was arbitrary, C^σ is trivial. □