Global Class Field Theory Study Group

Talk 2: Hilbert's Theorem 94 and the Capitulation Kernel

Edwina Aylward

January 21, 2026

1 Introduction

This is the second talk of the Global Class Field Theory Study Group. The material for today covers Sections 3 and 4 of Venkatesh's lecture notes. Section 3 discusses the broad strategies that will be implemented throughout the notes to prove the various elements of class field theory. Section 4 proves a fundamental result: that when a number field k has class number $c_k = 1$, it admits no non-trivial unramified abelian extensions.

For this talk, I will cover Section 4 first. We will run through the proof regarding unramified extensions, which, while technically involved, is quite elementary in its logic. I will conclude by discussing the ideas in Section 3.

(I'm doing this for a few reasons. I didn't want to chop §4 at a point, so doing it first ensures we finish it. Also §3 is kinda hand wavy).

Remark: Whenever I say ideal, I will mean a non-zero fractional ideal. Also, all my norms are relative norms.

2 §4: Unramified Extensions and Class Number One

The goal of §4 is to show that for a number field k, if there exists a cyclic unramified ℓ-extension K/k (ℓ prime), then C_k must be divisible by ℓ. We proceed by showing that the **capitulation kernel** $\ker(i_k)$, where $i_k : C_k \to C_K$ is the ideal class extension map, is non-trivial.

2.1 §4.1: Ideals and Units

If a class $[\mathfrak{a}] \in \ker(i_k)$, then its extension to K is principal, so $\mathfrak{a}\mathcal{O}_K = (y)$ for some $y \in K^\times$. Since $\mathfrak{a}$ originates in the base field k, the ideal (y) must be fixed under the Galois action $\langle\sigma\rangle = \mathrm{Gal}(K/k)$. Therefore:

$$(y)^\sigma = (y) \implies (y)(y^\sigma)^{-1} = \mathcal{O}_K = (y^{1-\sigma})$$

This implies that $y^{1-\sigma}$ is a unit of $K^\times$ of norm 1.

Conversely, by Hilbert Theorem 90, if $\theta \in K^\times$ is a unit of norm 1, then $\theta = y^{1-\sigma}$ for some $y \in K^\times$. Then $(y)^\sigma = (y)$, meaning (y) is necessarily extended from k.

(In fact, every σ-fixed ideal is extended from k because K/k is unramified. We can see this through the factorization:

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_\mathfrak{p}}, \quad n_\mathfrak{p} = n_{\sigma(\mathfrak{p})}$$

For $\mathfrak{P} \cap \mathcal{O}_k = \mathfrak{p}$, the primes above $\mathfrak{p}$ form a single $\langle\sigma\rangle$ orbit. Thus, the ideal factors as $\mathfrak{p} \cdot \mathcal{O}_K = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}$, and all such primes must factor into $\mathfrak{a}$ with equal exponents.)

Note that (y) is the extension of a principal ideal of k if and only if $y \in k^* U_K$, which is equivalent to saying θ is the image of a unit of K under $1-\sigma$, i.e., $\theta \in (1-\sigma)U_K$. We thus have an isomorphism:

$$(*) \quad \ker(C_k \to C_K) \cong \frac{\{\text{norm 1 units of } U_K\}}{(1-\sigma)U_K}$$

defined by the mapping $(\mathfrak{a} \mapsto (y)\mathcal{O}_K) \longmapsto y^{1-\sigma}$. To show $c_k > 1$, we must show that $(1-\sigma)U_K \subsetneq \{\text{norm 1 units of } U_K\}$, meaning Hilbert 90 fails for units.

2.2 §4.2: Reduction to the Relative Unit Group

We prove the RHS of $(*)$ is non-trivial assuming $\zeta_\ell \notin k$ (so excluding $\ell = 2$). Let the relative unit group be $\bar{U}_K := U_K/U_k$. The norm map $N : U_K \to U_k$ induces $\bar{N} : \bar{U}_K \to U_k/U_k^\ell$. The quotient map induces a surjection:

$$(**) \quad \frac{\text{norm 1 units of } U_K}{(1-\sigma)U_K} \longrightarrow \frac{\text{norm 1 elements of } \bar{U}_K}{(1-\sigma)\bar{U}_K}$$

This map is also injective: if $x \in U_K$ is in the kernel, then $x = z^{1-\sigma}y$ for $z, y \in U_K$, and $N(x) = 1 = N(y) = y^\ell \implies y = 1$ as $\zeta_\ell \notin k$. The right-hand side of $(**)$ has size:

$$(\star) \quad \frac{[\bar{U}_K : (1-\sigma)\bar{U}_K]}{\#\text{image } \bar{N}}$$

The image size can also be expressed as:

$$\#\text{image } \bar{N} = \frac{\#(U_k/U_k^\ell)}{[U_k/U_k^\ell : \bar{N}\bar{U}_K]} = \frac{\#(U_k/U_k^\ell)}{[U_k : NU_K]}$$

Since $\zeta_\ell \notin k$, Dirichlet's Unit Theorem gives $\#(U_k/U_k^\ell) = \ell^{r_\infty - 1}$ where r_∞ is the number of Archimedean places.

2.3 §4.3: Galois Module Structure

The upshot of passing to $\bar{U}_K$ is that it is a module of $\mathcal{O} = \mathbb{Z}[\sigma]/(1 + \sigma + \cdots + \sigma^{\ell-1})$. The map $\sigma \mapsto \zeta_\ell$ identifies $\mathcal{O}$ with $\mathbb{Z}[\zeta_\ell]$. Thus $\mathcal{O}$ is a Dedekind domain, and $1 - \sigma \in \mathcal{O}$ generates the unique prime ideal $\mathfrak{l}$ above ℓ. By the structure theorem:

$$\bar{U_K} \cong \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_r \oplus \mathcal{O}/\mathfrak{b}_1 \oplus \cdots \oplus \mathcal{O}/\mathfrak{b}_s$$

where $\mathfrak{a}_i, \mathfrak{b}_j$ are non-zero fractional ideals. Calculating ranks: $rk(U_k) = r_\infty - 1$ and $rk(U_K) = [K : k]r_\infty - 1 = \ell r_\infty - 1$ (as K/k is unramified). This implies $rk(\bar{U}) = (\ell - 1)r_\infty$. Since $rk(\mathcal{O}) = \ell - 1$, we must have $r = r_\infty$.

$\bar{U}_K$ has no ℓ-torsion. Indeed, if $y \in U_K \setminus U_k$ satisfied $y^\ell \in k$, then $T^\ell - y^\ell \in k[T]$ is irreducible and K/k is Galois, so K contains all roots $\implies \zeta_\ell \in K \implies \zeta_\ell \in k$ (by degree considerations), a contradiction. It follows that $(1 - \sigma)$ and $\mathfrak{b}_j$ are coprime, so:

$$\frac{\bar{U}_K}{(1-\sigma)\bar{U}_K} \cong \bigoplus_{i=1}^{r_\infty} \mathfrak{a}_i/(1-\sigma)\mathfrak{a}_i \cong \bigoplus_{i=1}^{r_\infty} \mathcal{O}/\mathfrak{l} \cong (\mathbb{F}_\ell)^{r_\infty} \implies [\bar{U}_K : (1-\sigma)\bar{U}_K] = \ell^{r_\infty}$$

Thus, $(\star) > 1$, proving the capitulation kernel is non-trivial.

2.4 Conclusion

Corollary (Hilbert Theorem 94): If there exists a cyclic unramified extension K/k of prime degree ℓ, then the class number of k is divisible by ℓ.

We have shown, in the context of the above corollary, that

$$\frac{[\text{norm 1 units of } U_K : (1-\sigma)U_K]}{[U_k : NU_K]} = \ell$$

implying $\#\ker(C_k \to C_K) = [U_k : NU_K] \cdot \ell$. Note that it is the unit showcasing the failure of Hilbert's theorem 90 that gives us an element of this kernel of order ℓ.

This formula showcases that the fewer the units that are norms, the more ideal classes that capitulate. The formula also holds when K/k is a cyclic unramified extension of composite degree, as proved in §5 (with ℓ replaced by $[K\colon k]$).

Example 2.1. Let $k = \mathbb{Q}(\sqrt{-5})$ and $K = \mathbb{Q}(i, \sqrt{5})$. The extension K/k is a cyclic unramified extension of degree 2. Let $\langle\sigma\rangle = \mathrm{Gal}(K/k)$, where σ is the automorphism fixing $i\sqrt{5}$ and mapping $i \mapsto -i$ and $\sqrt{5} \mapsto -\sqrt{5}$.

The ideal $\mathfrak{p} = (2, 1+\sqrt{-5})$ is non-principal in $\mathcal{O}_k$. However, its extension to K becomes principal:

$$\mathfrak{p}\mathcal{O}_K = (2, 1 + i\sqrt{5})\mathcal{O}_K = (1 + i)\mathcal{O}_K.$$

Let $y = 1 + i$. Then $y^{1-\sigma} = i$. Thus, i is a unit in U_K with relative norm 1. However, i is not contained in $(1-\sigma)U_K$. That is, there exists no unit $u \in U_K$ such that $u/\sigma(u) = i$. This demonstrates that Hilbert's Theorem 90 fails for units in this extension.

3 §3: The general strategy

Let K/k be a finite abelian extension. We saw last week that

$$[C_k : N_k^K C_K] \leq [K : k].$$

This inequality bounds the size of $N_k^K C_K$ from below. We want to also bound it from above.

Idea of strategy

Suppose K/k is cyclic with Galois group generated by σ. Then

$$(1-\sigma)C_K = \{[a][a^\sigma]^{-1} \mid [a] \in C_K\}$$

satisfies $N_k^K((1-\sigma)C_K) = 1$.

$\therefore$ Showing $(1-\sigma)C_K$ is large controls $N_k^K C_K$ from above.

Since $C_K/C_K^\sigma \xrightarrow{\sim} (1-\sigma)C_K$, we can equivalently show that C_K^σ is small.

Thus we will be interested in analysing C_K^σ, and will end up with formulae of the shape

$$\frac{\#C_k^* \cdot \prod \text{ramif. indices}}{[K : k]} = \#(C_K^\sigma)^* \times \text{index of norms in } u_k^*$$

where $C_k^*, (C_K^\sigma)^*, u_k^*$ are variants on C_k, C_K^σ, u_k.

The aim of establishing such formulae is to shift the burden of proving that not too many ideal classes are norms, to showing that not too many elements are norms.

We established a simple version of this shape already.