Class Field Theory
Lectures by Frank Calegari

Typed by Andrea Bourque

Fall 2025

Preface

There will be some gaps in explanation, either due to the lecturer's admission or my own lack of understanding. In particular, many "proofs" are sketches of proofs. Gaps due to my own misunderstanding will be indicated by three red question marks: ???. More generally, my own questions about the material will also be in red. Things like "**Question**" will be questions posed by the lecturer. Feel free to reach out to me with explanations.

Contents

1 Sep 29: Intro

1.1 Prereqs

The two more important prereqs are working knowledge of Galois theory and representation theory of finite groups. The less important prereqs are knowledge of the statements of core theorems in a first course of algebraic number theory, particularly Dirichlet's unit theorem and finiteness of class groups, as well as some homological algebra.

1.2 Galois Theory

Let L/K be a Galois extension with Galois group G. The **Galois correspondence** states that there is an inclusion-reversing bijection between fields L' with $K \subseteq L' \subseteq L$ (also called **subextensions** of L/K) and subgroups of G; explicitly, a subgroup $H \leq G$ gives the subextension L^H of fixed points of the H-action, and a subextension L' gives the subgroup $\mathrm{Gal}(L/L')$.

The action of G on L is K-linear, meaning L has the structure of a $K[G]$-module. Also, the unit group $\mathcal{O}_L^\times$ is stable under the G-action, so $\mathcal{O}_L^\times$ has a $\mathbb{Z}[G]$-module structure. We aim to answer the following questions:

Questions:

1. What is the structure of L as a $K[G]$-module?
2. What is the structure of $\mathcal{O}_L^\times$ as a $\mathbb{Z}[G]$-module?
3. What is the structure of $\mathcal{O}_L^\times \otimes_{\mathbb{Z}} \mathbb{C}$ as a $\mathbb{C}[G]$-module?

The first question has a nice answer:

Theorem 1.1 (Normal Basis Theorem)**.** *If L/K is a Galois extension with Galois group G, then $L \cong K[G]$ as a $K[G]$-module. Equivalently, there exists some $\theta \in L$, called a **normal basis element**, such that the set $\{g\theta \mid g \in G\}$ is a K-basis for L.*

Example 1.1. Suppose $[L : K] = 2$ and $\mathrm{char}(K) \neq 2$. Then $L = K(\sqrt{D})$ for some square free $D \in K$. Any $y \in L$ can be written in the form $y = a + b\sqrt{D}$ for $a, b \in K$. Then θ is a normal basis element iff y and $\overline{y} = a - b\sqrt{D}$ span L, which happens iff $ab \neq 0$.

We will prove 1.1 in a bit. First, we showcase a certain proof technique.

Theorem 1.2 (Cayley-Hamilton)**.** *Let $M \in M_n(R)$ be an n by n matrix with entries in a commutative ring R. Then $ch_M(M) = 0$, where $ch_M(x) = \det(xI - M) \in R[x]$ is the characteristic polynomial of M.*

Proof. We will make several reductions and then pass to a lemma.

1. We can reduce to the case where R is finitely generated by simply taking the subring S of R generated by the entries of M. Notably, $ch_M(x) \in S[x]$, so there will be no issue in replacing R by S.

2. Using a choice of generators for R, we get a surjection $\mathbb{Z}[x_1, \ldots, x_d] \twoheadrightarrow R$. We can lift M to a matrix M' over $\mathbb{Z}[x_1, \ldots, x_d]$ by making arbitrary choices for the preimages of the entries of M. The matrix $ch_{M'}(M')$ will map down to $ch_M(M)$, so it suffices to prove the theorem when $R = \mathbb{Z}[x_1, \ldots, x_d]$.

3. We can embed into $\mathbb{Q}(x_1, \ldots, x_d)$, and better yet, an algebraic closure thereof.

To conclude the proof from here, we use the following lemma.

Lemma 1.1. *Let K be an infinite field, and let $P \in K[x_1, \ldots, x_d]$. Then TFAE:*

1. *$P \neq 0$.*
2. *If L/K is any field extension, then $P \in L[x_i]$ is not 0.*
3. *There exist elements $a_i \in K$ such that $P(a_i) \neq 0$.*
4. *If L/K, there exist elements $a_i \in L$ such that $P(a_i) \neq 0$.*

Proof. It is clear that 1 is equivalent to 2, and that 3 implies 4 implies 1. Then it suffices to show that 1 implies 3. Assume $P \neq 0$. We induct on d. For $d = 1$, $P \in K[x]$ has only finitely many roots, while K itself is infinite, so there must be some $a \in K$ with $P(a) \neq 0$. For $d > 1$, we can write P as a polynomial in one variable over the field $L = K(x_1, \ldots, x_{d-1})$. Certainly L is infinite, so by the base case there is some $a_d \in L$ with $P(x_1, \ldots, x_{d-1}, a_d) \neq 0$ in L. By clearing denominators, we obtain a nonzero polynomial $Q \in K[x_1, \ldots, x_{d-1}]$, equal to $P(y_1, \ldots, y_d)$ for some $y_1, \ldots, y_d \in K[x_1, \ldots, x_{d-1}]$. By induction, there are some $a_1, \ldots, a_{d-1}$ such that $Q(a_i) \neq 0$. Using $x_i = a_i$ then gives values b_i for the y_i, so that $0 \neq Q(a_i) = P(b_i)$, as desired.

To finish the proof of Theorem 1.2 using this lemma, we (???)(something about $\mathbb{C}$ and Jordan normal forms?).

Before proving the normal basis theorem (1.1), we require a useful lemma.

Lemma 1.2 (Independence of Characters)**.** *Let Δ be an abelian group with distinct characters $\chi_1, \ldots, \chi_d : \Delta \to F^\times$ for some field F. If there are $c_i \in F$ such that $\sum_i c_i \chi_i = 0$, then all $c_i = 0$.*

Proof. Assume the c_i are not all 0. Relabeling if necessary, assume $c_d \neq 0$. Since the characters are distinct, there is some $\delta_0 \in \Delta$ such that $\chi_1(\delta_0) \neq \chi_d(\delta_0)$. We

then have two equations that hold for all $\delta \in \Delta$:

$$0 = \sum_i c_i \chi_i(\delta_0 \delta) = \sum_i c_i \chi_i(\delta_0)\chi_i(\delta),$$
$$0 = \chi_1(\delta_0) \sum_i c_i \chi_i(\delta) = \sum_i c_i \chi_1(\delta_0)\chi_i(\delta).$$

Subtracting these equations gives a new linear dependence equation: $\sum c_i' \chi_i = 0$, where $c_i' = c_i(\chi_i(\delta_0) - \chi_1(\delta_0))$. By the choice of δ_0, $c_d' \neq 0$ and $c_1' = 0$. In effect, we have removed χ_1 from our list of characters and obtained a new non-trivial dependence equation. We may repeat until we obtain $c\chi_d = 0$ for $c \neq 0$, at which point we have a contradiction. Thus, the original c_i must have all been 0.

We now prove the normal basis theorem (1.1).

Proof. For all $x \in L$, there are $a_g \in K$ indexed over $g \in G$ so that $\sum_g a_g gx = 0$; for instance, we can choose $a_g = 0$ for all g. We want to find x for which there is no choice of these a_g where not all $a_g = 0$. The previous equation implies that $\sum_g a_g h^{-1} gx = 0$ for all h, so we obtain a matrix equation $M\vec{a} = 0$, where $M = [h^{-1}gx]_{h,g}$ and $\vec{a} = (a_g)_g$. Note that M has nothing to do with a, so if we show that there is a choice of x for which M is invertible, we will be done.

As an aside, an explicit example with $L = K(\sqrt{D})$ and $x = a + b\sqrt{D}$ is $M = \begin{pmatrix} x & \overline{x} \\ \overline{x} & x \end{pmatrix}$, where $\overline{x} = a - b\sqrt{D}$.

Now, fix a basis $e_1, \ldots, e_d$ for L/K. Write $x = \sum_i x_i e_i$. Then M becomes $[\sum_i x_i h^{-1} g e_i]_{h,g}$.

We will first treat the case where K is infinite, so that we can use Lemma 1.1. To that end, we want to find a specialization of the x_i to $\eta_i \in L$ such that $\sum_i \eta_i e_i = 1$ and $\sum_i \eta_i g e_i = 0$ for $g \neq 1 \in G$. We can do this by showing $A = [ge_i]_{i,g}$ is invertible. A is invertible iff its transpose is invertible iff its transpose is injective. So, suppose we have $c_g \in L$ with $\sum_g c_g g e_i = 0$ for all i. Since the e_i are a basis for L, this means that $\sum_g c_g gx = 0$ for all $x \in L$, and thus that $\sum_g c_g g = 0$ as functions on L. But each g is a character of $L^\times$, so by linear independence of characters (Lemma 1.2), we have that all $c_g = 0$. Thus A is invertible and we can find the η_i. The ability to find η_i implies that the polynomial defining $\det(M)$ can be specialized to be 1, which is in particular not 0. Therefore, by Lemma 1.1, we can find a specialization of the x_i in K that makes $\det(M) \neq 0$, so that $x = \sum x_i e_i$ is a normal basis element.

Now we treat the case where $K = \mathbb{F}_q$ is a finite field. Then $L = \mathbb{F}_{q^d}$, and $G = \mathbb{Z}/d\mathbb{Z}$ is generated by the q-power Frobenius $\Phi : x \mapsto x^q$. In particular, the group ring $K[G]$ is isomorphic to $K[x]/(x^d - 1)$, with the isomorphism sending Φ to x. In particular, we have a map $K[x] \twoheadrightarrow K[G]$, so that any $K[G]$-module,

like L, can be considered a $K[x]$-module, where x acts by Φ. This allows us to use the structure theorem for f.g. modules over a PID; $L \cong \bigoplus_{i=1}^{n} K[x]/(a_i)$, where we can arrange the $a_i \in K[x]$ to satisfy a_{i+1} is a multiple of a_i. Since $[L : K] = d < \infty$, we must have $a_n \neq 0$, since otherwise L would have a subspace isomorphic to $K[x]$, which is infinite dimensional over K. Since $a_n \neq 0$ and it is a multiple of all other a_i, the other a_i cannot be 0. We may assume the a_i are not constants, since $K[x]$ modulo a non-zero constant is 0. Each subspace $K[x]/(a_i)$ has K-dimension equal to $\deg a_i$, so $d = [L : K] = \sum_i \deg a_i$.

Now, suppose L is not cyclic as a $K[x]$-module, so that $n > 1$ above. Then $\deg a_n < d$. We also know that a_n annihilates L, since it annihilates each $K[x]/(a_i)$ by virtue of $a_i | a_n$. What this means is that if $a_n = \sum_{j=0}^{d-1} c_j x^j$, then $\sum_{j=0}^{d-1} c_j \Phi^j(y) = 0$ for all $y \in L$. In other words, $\sum_j c_j \Phi^j = 0$ as functions on L. We noted that $a_n \neq 0$, so the c_j are not all 0. But the Φ^j are distinct characters of $L^\times$, so we obtain a contradiction by independence of characters (Lemma 1.2).

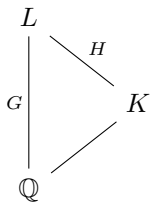
So now we are in the case that $L \cong K[x]/(a)$ as $K[x]$-modules for some degree d polynomial a. Suppose $a = \sum_{j=0}^{d} c_j x^j$. Then by similar reasoning as above, we have $\sum_j c_j \Phi^j = 0$ as functions on L. But notice that, since Φ is an order d generator for G, we have $\Phi^d = 1$, so $\sum_j c_j \Phi^j = c_0 + c_d + \sum_{j=1}^{d-1} c_j \Phi^j = 0$. This is another linear dependence equation of the characters $1, \Phi, \ldots, \Phi^{d-1}$, so we must have $c_j = 0$ for $0 < j < d$ and $c_0 = -c_d$. In other words, up to scalar, $a = x^d - 1$. Therefore, $L \cong K[x]/(x^d - 1)$ as $K[x]$-modules, say with an isomorphism $f : L \to K[x]/(x^d - 1)$. Let $y = f^{-1}(1)$. Then the set $\{gy \mid g \in G\}$ is the set $\{\Phi^j y \mid 0 \leq j < d\}$, which under the isomorphism f corresponds to the set $\{x^j \cdot 1 \mid 0 <= j < d\}$. This set is certainly a basis for $K[x]/(x^d - 1)$, so $\{gy \mid g \in G\}$ is a basis for L. Thus, y is a normal basis element as desired.

2 Oct 3 25

Came in 9 mins late.

Let $L/\mathbb{Q}$ be Galois with Galois group G. Let $\Sigma_L = \mathrm{Hom}(L, \mathbb{C})$. G acts on Σ_L by $g\sigma = \sigma \circ g^{-1}$.

Σ_L up to complex conj. in bijection with $G/\langle c \rangle$.



We want to understand the relationship between $c \in G$ corresponding to $\sigma \in \Sigma_L$ and Σ_K. There is a surjective map $\Sigma_L \twoheadrightarrow \Sigma_K$ given by restriction to K. Elements $\sigma, g\sigma$ map to the same thing iff $g \in H$. Similarly $g_1\sigma$ and $g_2\sigma$ map to the same thing iff $g_1^{-1} = g_2^{-1}h$ for some $h \in H$, which means that the fibers of the map $\Sigma_L \to \Sigma_K$ are right cosets of H.

How many embeddings in Σ_K are real? How many are complex? Can write this in terms of cosets...

Can map $L^\times \to \prod_{\nu \text{ cplx}} \mathbb{C}^\times \xrightarrow{\log|\cdot|} \prod \mathbb{R}$. G acts on the rightmost set by permutation, corresponding to the action of G on $G/\langle c\rangle$. We can express this as $\mathbb{R}[G/\langle c\rangle]$ or $\mathrm{Ind}_{\langle c\rangle}^G \mathbb{R}$. If we restrict to units, we get $\mathcal{O}_L^\times \otimes \mathbb{R} \to \mathrm{Ind}_{\langle c\rangle}^G \mathbb{R} = \mathbb{R}^{[G:\langle c\rangle]}$. Since units have norm one, this map lands in the subspace whose coordinates sum to 0. In particular, letting d be the rank of $\mathcal{O}_L^\times$, we find $d = [G : \langle c\rangle] - 1$. Denoting by $\mathbb{R}$ the trivial representation in $\mathbb{R}^{[G:\langle c\rangle]}$, sitting in the diagonal of vectors with equal coordinates, we obtain an isomorphism of G-modules $\mathcal{O}_L^\times \otimes R \cong (\mathrm{Ind}_{\langle c\rangle}^G \mathbb{R})/\mathbb{R}$. For example, if L is totally real, we get $\mathcal{O}_L^\times \otimes \mathbb{R} \cong \mathbb{R}[G]/\mathbb{R}$. Otherwise (or in any case?), we also obtain $\mathcal{O}_L^\times \otimes \mathbb{C} \cong (\mathrm{Ind}_{\langle c\rangle}^G \mathbb{C})/\mathbb{C}$.

What is the multiplicity of a G-irrep V in $\mathcal{O}_L^\times \otimes \mathbb{C}$? It is $\dim \mathrm{Hom}_G(V, \mathcal{O}_L^\times \otimes \mathbb{C}) = \dim \mathrm{Hom}_G(V, \mathrm{Ind}_{\langle c\rangle}^G) - \dim \mathrm{Hom}_G(V, \mathbb{C})$. The subtracted term is 1 if V is trivial and 0 otherwise. The other term can be rewritten with Frobenius reciprocity as $\dim \mathrm{Hom}_{\langle c\rangle}(V, \mathbb{C}) = \dim(V|c = 1)$.

Example 2.1. Let $G \cong \mathbb{Z}/3$. There are three irreducible characters over $\mathbb{C}$, called $1, \chi, \chi^2$. They are all defined over $K = \mathbb{Q}(\zeta_3)$. You can look at χ as a 2-dimensional representation over $\mathbb{Q}$, by taking a basis $1, \zeta_3$. for $K/\mathbb{Q}$.

In fact for representations of finite groups over $\mathbb{C}$, we can always define over a number field. There is a moduli space perspective on this; a purely transcendental representation must correspond to some deformation, and then the deformation corresponds to a non-split extension. By semisimplicity, this cannot happen.

If W is a representation of $\mathbb{Q}[G]$, then $W \otimes_{\mathbb{Q}} K$ is a representation of $\mathbb{Q}[G]$ isomorphic to $W^{[K:\mathbb{Q}]}$.

Lemma 2.1. *If W, V are reps of G over a number field K and if $W \otimes_K \mathbb{C} \cong V \otimes_K \mathbb{C}$, then $V \cong W$.*

How close is $\mathcal{O}_L^\times$ to $\mathrm{Ind}_{\langle c\rangle}^G \mathbb{Z}$? Similarly, if L/K Galois, how close is $\mathcal{O}_L$ to $\mathcal{O}_K[G]$?

Example 2.2. Let $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{D})$. Let $\theta = a + b\sqrt{D}$ with $ab \neq 0$. We have $L \cong \mathbb{Q}[\mathbb{Z}/2]$. Integrally, the question is whether $\mathcal{O}_L = \mathbb{Z}\theta \oplus \mathbb{Z}\overline{\theta}$.

If $L = \mathbb{Q}(\sqrt{-3})$, we can pick $\theta = \frac{1+\sqrt{-3}}{2}$. If $L = \mathbb{Q}(\sqrt{-1})$, there is no choice of θ.

In general, if $\Delta_D \equiv 1 \mod 4$, then we can find θ. But if $\Delta_D \equiv 0 \mod 4$, then we cannot find θ. However, we can get an index 2 subgroup.

In general we can do things after inverting finitely many primes.

3 6 Oct 25

Integral versions (or failures thereof) of the NBT.

Example 3.1. $[K : \mathbb{Q}] = 2$. Then $\mathcal{O}_K = \mathbb{Z}[\frac{\Delta_K + \sqrt{\Delta_K}}{2}]$, where Δ_K is the discriminant of K. Direct computation shows that $\mathcal{O}_K \cong \mathbb{Z}[G]$, where $G = \mathbb{Z}/2$ is the Galois group, iff $(\Delta_K, 2) = 1$.

In general, $K \cong \mathbb{Q}[G]$ gives two integral results: $\mathbb{Z}[1/S][G] \cong \mathcal{O}_K[1/S]$ for some finite set S of primes, and a finite index inclusion $\mathcal{O}_K \hookrightarrow \mathbb{Z}[G]$ (and the other way around).

Questions: What restrictions are there on the image? Is the index of the image controlled/bounded in some way, e.g. by something only depending on $|G|$?
We ask these questions for any M sitting inside $\mathbb{Z}[G]$ with finite index and satisfying $M \otimes \mathbb{Q} \cong \mathbb{Q}[G]$. Can we find another embedding $M \hookrightarrow \mathbb{Z}[G]$ with a controlled index?

Another perspective: if $M \cong \mathbb{Z}^{|G|}$ is a G-module, then this corresponds to a group homomorphism $\rho : G \to GL_n\mathbb{Z}$, where $n = |G|$. If $M \otimes \mathbb{Q} \cong \mathbb{Q}^n$, then we further impose $G \xrightarrow{\rho} GL_n\mathbb{Z} \hookrightarrow GL_n\mathbb{Q}$ is the regular representation. This essentially means we are looking at ρ up to conjugation.

Example 3.2. If $G = \mathbb{Z}/2$, $M \cong \mathbb{Z}^2$, then $G \curvearrowright M \otimes \mathbb{Q}$ is conjugate to the map sending the generator σ to $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Since this matrix has entries in $\mathbb{Z}$, we can interpret this over $\mathbb{Z}$, i.e. by taking $M = \mathbb{Z}[i]$ with σ acting by conjugation. If we take the permutation module over $\mathbb{Z}$, i.e. where σ acts by $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, then this is not isomorphic to the other module over $\mathbb{Z}[G]$. We can see that they are different e.g. by quotienting by the multiples of 2. (clean up this example) The question is now: are there any others?

$M = e_1\mathbb{Z} + e_2\mathbb{Z}$ generated by $\{e_1, \sigma e_1, e_2, \sigma e_2\}$. Contained with index at most 16 in $\{\}$ (bunch of fractions) and this is the diagonal rep over $\mathbb{Q}$.

Example 3.3. We now consider $G = \mathbb{Z}/p$. What are the conjugacy classes of matrices M in $GL_p\mathbb{Z}$ of order (dividing) p? Over $\mathbb{Q}$ we just have the super diagonal matrix. Can split $\mathbb{Q}^p$ into $\mathbb{Q}$ where M acts trivially, and $\mathbb{Q}^{p-1}$ where

M acts by $M^{p-1} + \cdots + I$. The polynomials $x - 1, x^{p-1} + \cdots + 1$ have gcd p, so there is an index issue when we do this over $\mathbb{Z}$.

If M acts on $\mathbb{Z}^{p-1}$ by $(x^p - 1)/(x - 1)$, we get a module over $R = \mathbb{Z}[x]/((x^p - 1)/(x - 1)) = \mathbb{Z}[\zeta_p]$, and this module tensored with $\mathbb{Q}$ is $R \otimes \mathbb{Q}$. Then what we are looking at is ideal classes of $\mathbb{Z}[\zeta_p]$.

Theorem 3.1 (Jordan-Zassenhan)**.** *Let G be finite group and let n be a positive integer. There are only finitely many representations $\rho : G \to GL_n\mathbb{Z}$ up to conjugation in $GL_n\mathbb{Z}$.*

By the above work, this theorem implies the finiteness of the class group for $\mathbb{Q}(\zeta_p)$.

Alternate questions: When is $\mathcal{O}_{K,p} \cong \mathbb{Z}_{(p)}[G]$? When is $\mathcal{O}_K/p \cong \mathbb{F}_p[G]$?

The answer to the second question is yes if p is inert and unramified.

Factor $p = \prod_{i=1}^r \mathfrak{p}_i^e$ in $\mathcal{O}_K$. Let $f = [\mathcal{O}_K/\mathfrak{p} : \mathbb{F}_p]$. Then $|G| = n = efr$. When is $\prod_i \mathcal{O}_K/\mathfrak{p}_i^e \cong \mathbb{F}_p[G]$? Given a prime $\mathfrak{p}$ over p, let $D = D_\mathfrak{p}$ be the stabilizer of $\mathfrak{p}$ in G. Then D acts on $\mathcal{O}_K/\mathfrak{p}^k$ for any k. We have $[G : D] = r$ by the orbit stabilizer theorem. All the primes over p are conjugate to $\mathfrak{p}$. Note that $\mathcal{O}_K/p = \prod \mathcal{O}_K/\mathfrak{p}_i^e = \mathrm{Ind}_D^G \mathcal{O}_K/\mathfrak{p}^e$.

Now, consider the local situation: we have a Galois extension $K_\mathfrak{p}/\mathbb{Q}_p$ with Galois group D. When is D acting on $\mathcal{O}_{K_\mathfrak{p}}/\mathfrak{p}^e$ isomorphic to $\mathbb{F}_p[D]$? The answer is not always. In the unramified case we get yes by the normal basis theorem.

If p is odd, consider $K = \mathbb{Q}(\sqrt{p^*})$, where $p^* = \pm p$ making the discriminant good. We have $\mathcal{O}_K/p \cong \mathbb{Z}_p[x]/(x^2 - p, p) \cong \mathbb{F}_p[x]/x^2$. Then ....

Now consider $K/\mathbb{Q}_p$ be Galois, totally ramified, with ramification index e coprime to p (called tame). What is the action of D on $\mathcal{O}_K/p$?

Theorem 3.2 (Noether)**.** *We have an integral normal basis theorem iff L/K is tamely ramified.*