

Galois Theory

Patrick Oare

These are currently my lecture recap notes from Math 250A at UC Berkeley. I will eventually write them up into a more legible set of notes.

Unless otherwise specified, let L/K be a Galois extension with Galois group G .

1 11/7 (Galois Extensions, Fundamental Theorem)

- **Definitions:** An extension L/K is called **Galois** if it is normal and separable. We define the **Galois group** of the extension L/K to be $Gal(L/K) := Aut(L/K) = \{\sigma \in Aut(L) : \forall k \in K, \sigma(k) = k\}$, i.e. $Gal(L/K)$ is the group of all automorphisms of L that fix K . If $\alpha \in L$, the **conjugates** of α under $Gal(L/K)$ are the set $\{\sigma(\alpha) : \sigma \in Gal(L/K)\}$.

- **Galois Extensions:**

Theorem 1

For a finite extension L/K , the following are equivalent. Let $G = Gal(L/K)$.

1. L is the splitting field of a separable polynomial over K .
2. L/K is Galois.
3. $[L : K] = |G|$.
4. $K = L^G$ is the fixed field of in L by G .

Some of these are easy: $i \implies ii$ and $iii \implies iv$. For $ii \implies iii$, suppose L/K is Galois. Let M be the algebraic closure of K . We have $\leq n = [L : K]$ maps $L \rightarrow M$ extending $id|_K$. But, L/K separable implies we have n such maps. For if $L = K(\alpha)$, then the minimal polynomial of α is separable and so has n distinct roots, so we have exactly n maps, and if $L = K(\alpha_1, \dots, \alpha_n)$, then we proceed as in the proof above to get n maps. But, L/K normal implies the image of any map $L \rightarrow M$ lies in L (as then L is a splitting field and uniquely determined), which gives us n homomorphisms extending the identity on K , so $[L : K] = |G|$.

For $iv \implies ii$, let $\alpha \in L$. Look at all conjugates of α by G , and call them $\alpha_1, \dots, \alpha_n$ ($\alpha_1 := \alpha$). Let $f(x) := \prod_{i=1}^n (x - \alpha_i)$. f is fixed by G (as in applying any $\sigma \in G$ we may reindex the product), so f has coefficients in $L^G = K$, and f is the minimal polynomial of α over K (really, take f to be a product over distinct conjugates of α).

L is. So, for any element in L , the minimal polynomial over K is separable and has all its roots in L . Now, take a basis $\omega_1, \dots, \omega_k$ of L/K , and let $p_i(x)$ be the minimal polynomial of ω_i over K . Then, take all repeated factors out of $\prod_{i=1}^k p_i(x)$, and call it g . This makes this a separable polynomial, and then L is the splitting field of g .

- **Minimal Polynomials under Galois Conjugates:** Let $\alpha \in L$ have minimal polynomial $p \in K[X]$. Then, any conjugate of α by G has minimal polynomial $p(x)$ as well.

- **Examples of Galois Extensions:**

1. $\mathbb{Q}(\sqrt[3]{2}, \omega)$ for $\omega := \exp(2\pi i/3)$. This is the splitting field of $x^3 - 2$ over $\mathbb{Q}$ and has Galois group S_3 .
2. $\mathbb{C}/\mathbb{R}$ is Galois with Galois group $\mathbb{Z}/2\mathbb{Z}$ —the nontrivial element is complex conjugation.
3. $\mathbb{F}_{16}/\mathbb{F}_2$ is the splitting field of $x^{16} - x$ over $\mathbb{F}_2$, and we have already shown this is separable. Let ϕ be the Frobenius element of $\mathbb{F}_{16}$, i.e. $\phi(x) = x^2$. Then $\text{Gal}(\mathbb{F}_{16}/\mathbb{F}_2) \cong \mathbb{Z}/4\mathbb{Z}$, and generated by ϕ .

- **Galois Groups of Finite Fields:** Let $q = p^n$ for $n \geq 1$. Then, the extension $\mathbb{F}_q/\mathbb{F}_p$ is Galois, and:

$$\text{Gal}(\mathbb{F}_q/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$$

That it is Galois follows because $\mathbb{F}_q$ is the splitting field of separable $x^q - x$ over $\mathbb{F}_p$. The Galois group is generated by the **Frobenius element** (the Frobenius element for an extension of finite fields L/K is $x \mapsto x^{|K|}$),

$$\phi(x) := x^{\text{char}(\mathbb{F}_q)} = x^p$$

The order of ϕ is n , as clearly if $m < n$ then $\phi^m \neq \text{id}$, but $\phi^n(a) = a^{n^p} = a^q = a$ and so $|\phi| = n$. But, $|\text{Gal}(\mathbb{F}_q/\mathbb{F}_p)| = [\mathbb{F}_q/\mathbb{F}_p] = n$, and so in fact $\text{Gal}(\mathbb{F}_q/\mathbb{F}_p) = \langle \phi \rangle$.

- **Fundamental Theorem of Galois Theory:** Let M/K be a Galois extension with $G = \text{Gal}(M/K)$. We have a bijection between the intermediate extensions L with $K \leq L \leq M$ and the subgroups $H \leq G$ given by sending L to:

$$L \mapsto \text{Gal}(M/L)$$

where $\text{Gal}(M/L)$ is the group of $\sigma \in G$ fixing L . The inverse of this sends H to:

$$H \mapsto M^H$$

which is all elements in M fixed by H . This bijection **reverses inclusions**, so bigger subfields correspond to smaller subgroups.

2 11 / 9 (Computing Galois Groups, Examples)

- **Seventh root of unity:** Let $\xi := \exp(2\pi i/7)$ be the 7th root of unity. Recall $\xi^7 - 1 = (\xi - 1)(\xi^6 + \xi^5 + \xi^4 + \xi^3 + \xi^2 + \xi + 1) = (\xi - 1)\Phi_7(\xi) = 0$, so obviously $\Phi_7(\xi) = 0$ and is irreducible. We know the roots of Φ_7 , so:

$$\Phi_7(x) = \sum_{i=0}^6 x^i = (x - \xi)(x - \xi^2) \dots (x - \xi^6)$$

and therefore the extension is Galois with degree 6. Let $G := \text{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$, so $|G| = 6$. Note that for $\sigma \in G$, σ is completely determined by its action on ξ since all roots are powers of ξ . σ may send ξ to other root of $\Phi_7(x)$, so $\sigma(\xi) = \xi^m$ for $m = 1, 2, \dots, 6$. Thus we have found the 6 elements of the Galois group, and we find $G \cong (\mathbb{Z}/7\mathbb{Z})^*$.

We can use this to determine the subfields of the extension— As $(\mathbb{Z}/7\mathbb{Z})^*$ is cyclic of order 6, we have unique nontrivial subgroups of orders 2 and 3— these are $H := \{1, 2, 4\}$ and $J := \{1, 6\}$ (note G is generated by 3). We find $\mathbb{Q}(\xi)^H$ — this will be a degree 2 extension of $\mathbb{Q}$. An obvious element is given by taking any element and summing its conjugates which are in the subgroup. In this case, we take $a := \sigma(\xi) + \sigma^2(\xi) + \sigma^4(\xi) = \xi + \xi^2 + \xi^4$, which will be fixed under H . Note that $a^2 + a + 2 = 0$, so:

$$a = \frac{-1 + \sqrt{-7}}{2} \implies \mathbb{Q}(a) = \mathbb{Q}(\sqrt{-7})$$

and so our fixed field is $\mathbb{Q}(\sqrt{-7})$. For the degree 3 subfield over $\mathbb{Q}$, we take $b := \xi + \xi^6$ and find that the subfield is $\mathbb{Q}(\cos(2\pi/7))$.

- **Roots of unity:** In general, if ξ_n is a primitive n th root of unity, then:

$$\text{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$$

If $\gcd(n, m) = 1$, then:

$$\mathbb{Q}(\xi_n) \cap \mathbb{Q}(\xi_m) = \mathbb{Q}$$

- **Normal Extensions vs. Subgroups:** Let L/F be a Galois extension. Recall that if K is an intermediate field, then L/K is Galois (as L is a splitting field of $f(x) \in F[X] \subset K[X]$). Let $G = \text{Gal}(L/F)$, and let $H = \text{Gal}(L/K) \leq G$. Then, $H \trianglelefteq G$ iff K/F is a normal extension. If this is the case, then K/F is Galois (as it is separable since L/F is separable), and:

$$\text{Gal}(K/F) \cong G/H$$

This isomorphism follows because we can define a map $G \rightarrow \text{Gal}(K/F)$, $\sigma \mapsto \sigma|_K$, which has kernel H .

- **Determining Galois groups by reduction modulo p :** Let p be prime, $f \in \mathbb{Z}[X]$ monic with Galois group G . If $\bar{f}(x) := f(x) \pmod{p}$ has Galois group $\bar{G}$, then:

$$\bar{G} \hookrightarrow G$$

and so we may identify elements of $\bar{G}$ as elements of G . Combining these with the fact that $G \leq S_n$ is powerful; it is easy to find a combination of cycles which are in $\bar{G}$, and we may put it together to show they generate a certain unique subgroup of S_n .

In general, if we have a degree n irreducible polynomial, the Galois group acts transitively on these n roots. By orbit-stabilizer, this means that $|G\alpha| = n = (G : G_\alpha) \implies n$ divides $|G|$. If this is a degree p irreducible polynomial, then the Galois group of the polynomial contains a p -cycle. Since p divides $|G|$, this implies G has an element of order p by Cauchy, which is a p -cycle. This is helpful: <http://www.math.uconn.edu/~kconrad/blurbs/galoistheory/galoisaspermgp.pdf>

- **Condition for $G = S_p$:** Let f be irreducible in $\mathbb{Q}[X]$ with $\deg(f) = p$ prime. If f has precisely two non-real roots in $\mathbb{C}$, then the Galois group of f is S_p .

For suppose this is the case. Then G acts transitively on the p -roots of f , and hence contains a p -cycle by above. But since f has precisely two nonreal roots, these are complex conjugates of one another, and so complex conjugation induces an automorphism of the splitting field fixing $\mathbb{Q}$. Since S_p is generated by a p -cycle and a transposition, we are done.

- **Finding an extension with a given Galois group:** Let G be a finite group. Then, we may find an extension L/K with Galois group G . We first consider $G = S_n$. Take $L = \mathbb{Q}(x_1, \dots, x_n)$. S_n acts on L by permuting the variables $x_1, \dots, x_n$, and so we may put $K = L^G$. K will be the set of symmetric functions in n variables over $\mathbb{Q}$. One can show that **if G is a finite group acting on a field L , then L/L^G is Galois with $G = \text{Gal}(L/L^G)$** , so this implies $\text{Gal}(L/K) = G$.
- **Ex:** Galois group of $x^5 - 4x + 2$. This is irreducible by Eisenstein at $p = 2$, and hence 5 divides the order of the Galois group, so it contains a 5-cycle. One can draw the graph to verify it has 2 complex roots, and so the Galois group must contain complex conjugation, a transposition. But any transposition along with a p -cycle generate S_p , so the Galois group is S_5 . We can do a similar thing for any prime p , so for any prime p , we can find an extension $L/\mathbb{Q}$ with $\text{Gal}(L/\mathbb{Q}) = S_p$.

3 11/14 (Cyclic Extensions)

- **3rd degree polynomials:** Let $f(x) = x^3 + ax^2 + bx + c \in K[X]$ be an irreducible and separable polynomial. Recall the discriminant of the polynomial, if α_i are the roots, is:

$$\Delta^2 = \prod_{i < j} (\alpha_i - \alpha_j)^2$$

Let G be the Galois group of $f(x)$. 3 divides $|G|$ as G acts transitively on the roots, so since $G \leq S_3$, either $G \cong \mathbb{Z}/3\mathbb{Z}$ or $G \cong S_3$. Note that if we examine Δ , this is invariant under elements of A_3 and changes sign under elements of $S_3 \setminus A_3$. Thus, if the Galois group is A_3 , Δ is invariant under the action G and lies in the base field. If $G \cong S_3$, then any $\sigma \in S_3 \setminus A_3$ maps $\Delta \mapsto -\Delta$, so Δ is **not** in the base field. Thus, **if Δ^2 has a**

square root in the base field, $G = A_3$. If Δ^2 has no square root in the base field, then $G = S_3$. Note if $a = 0$, then:

$$\Delta^2 = -4b^3 - 27c^2$$

- **Fundamental Theorem of Algebra:** $\mathbb{C}$ is algebraically closed.

Proof. We use the following facts about $\mathbb{C}$ and $\mathbb{R}$:

1. $\text{char}(\mathbb{R}) = 0$.
2. Any polynomial in $\mathbb{R}$ of odd degree has a real root (can use IVT).
3. $[\mathbb{C} : \mathbb{R}] = 2$, and every element of $\mathbb{C}$ has a square root in $\mathbb{C}$.

Let L be a finite extension of $\mathbb{C}$ — we will show that $L = \mathbb{C}$. Since $\text{char}(\mathbb{C}) = 0$, $L/\mathbb{C}$ is separable, and we can assume that $L/\mathbb{R}$ is Galois (just make it normal by making it a splitting field), so set $G = \text{Gal}(L/\mathbb{R})$. By fact *ii*, $\mathbb{R}$ has no algebraic extensions of odd degree, for we there are no irreducible polynomials of odd degree (can just strip off the real root), which implies that G has no subgroups of odd index > 1 . Let $H = \text{Gal}(L/\mathbb{C})$, so $(G : H) = 2$. But $\mathbb{C}$ has no quadratic extensions by *iii*, so H has no subgroups of index 2. Let S be a 2-Sylow of G (the order of G is its index with 1 and hence is even). Then S has odd index ($|S| = p^\alpha$ with p not dividing $|G|/p^\alpha$), so $S = G$ as G has no subgroups of odd index other than G itself. Thus, $G = S$ has order 2^n for some $n \implies |H| = 2^{n-1}$. If $n - 1 > 0$, then H would have a subgroup of index 2, which we have shown is not possible, so $n - 1 = 0 \implies n = 1 \implies |G| = 2 \implies \mathbb{C}$ is algebraically closed. □

- **Lemma:** Suppose V is a vector space over an infinite field K . Then, V is not the union of a finite number of proper subspaces.
- **Theorem:** If L/K is a finite separable extension, then $L = K(\alpha)$, $\alpha \in L$ is a primitive extension.

Let M be a finite Galois extension containing L . Then there are finitely many intermediate extensions of M/K as these correspond with subgroups of the Galois group, and as $L \leq M$ there are only finitely many intermediate extensions of L/K . Each of these finitely many extensions is a vector space over K , and so if K is infinite, then L is not the union of all of the finitely many subextensions by the above lemma, so some $\alpha \in L$ is not in any smaller extension of K , and thus $L = K(\alpha)$. If K is finite, then $\implies L$ is finite, so $L^* = \langle \alpha \rangle$ and $L = K(\alpha)$.

- **Purely inseparable extension:** An example of this is $\mathbb{F}_p(t, u)/\mathbb{F}_p(t^p, u^p)$. This has degree p^2 , and every element of $\mathbb{F}_p(t, u)$ generates an extension of degree p or 1. This implies this extension is not primitive as no element generates an extension of degree p^2 , and in fact this extension has an infinite number of subextensions.

- **Theorem:** Suppose that L/K is a Galois extension such that:

1. $\text{Gal}(L/K) \cong \mathbb{Z}/p\mathbb{Z}$.
2. K contains all the p th roots of unity.
3. $\text{char}(K) \neq p$.

Then $L = K(\sqrt[p]{a})$ for some $a \in K$.

Proof. To prove this, let σ be a generator of the Galois group. We look at the eigenvectors of σ as a linear transformation. Since σ generates the Galois group, $\sigma^p = 1$, so its eigenvalues are all the p th roots of unity and are in K . Pick any $v \in L$. Then the element:

$$v + \xi\sigma v + (\xi\sigma)^2 v^2 + (\xi\sigma)^3 v^3 + \dots + (\xi\sigma)^{p-1} v$$

has eigenvalue ξ^{-1} , and similarly $v + \xi^2\sigma v + (\xi^2\sigma)^2 v^2 + \dots$ has eigenvalue ξ^{-2} , and so on. But v is the average of these as $1 + \xi + \xi^2 + \dots + \xi^{p-2} = 0$, so the eigenspaces sum to the entire space, and therefore:

$$L = \bigoplus_{i=0}^{p-1} E_i$$

where E_i is the eigenspace of σ with eigenvalue ξ^i —each eigenspace is one dimensional. Now, pick w to be any eigenvector of σ with $\sigma w = \xi w$, so $w \notin K$ as σ does not fix w . Then $\sigma w^p = \xi^p w^p = w^p$, so $w^p \in K$, and if we put $a = w^p$ then $L = K(w) = K(\sqrt[p]{a})$ as w has order p under multiplication by ξ , so the elements $\{\sigma^i(w)\}$ span each eigenspace and therefore generate L . □

- **Artin-Schrier Equation:** The above proof breaks down if $\text{char}(K) = p$. Suppose $\text{Gal}(L/K) = \langle \sigma \rangle$. Then L cannot be of the form $K(\sqrt[p]{a})$ as $x^p - a$ is inseparable, so its splitting field is not a Galois extension. Now, since $|\sigma| = p$, we have $\sigma^p = 1 \implies (\sigma - 1)^p = 0$ by the Frobenius endomorphism, so $\sigma - 1$ is a nilpotent operator. Suppose v is a rank 2 generalized eigenvector, so $(\sigma - 1)^2 v = 0 \implies \sigma(\sigma - 1)v = (\sigma - 1)v \implies (\sigma - 1)v \in K$ as it is fixed by a generator of the Galois group. Thus, $\sigma v - v = a, a \in K$, and replacing v with v/a gives $\sigma v - v = 1 \implies \sigma v = v + 1$, so $\sigma v^p = v^p + 1$. Combining these, we have that $\sigma(v^p - v) = v^p - v \in K$ as σ fixes it, so v is a root of the **Artin-Schrier Equation**:

$$x^p - x - b = 0 \quad (b \in K)$$

This is the analog of $x^p - b = 0$ for characteristic p . Note that the polynomial $f(x) = x^p - x - b$ is separable in characteristic p for any $b \in K$ as it has derivative -1 , so its splitting field is Galois. If v is any root, then we see by inspection that $v + 1$ is a root, so the distinct roots are $v, v + 1, \dots, v + (p - 1)$. Thus, $K(v)$ is Galois, and $\text{Gal}(K(v)/K) = \{\sigma : v \mapsto v + i, i \in \mathbb{Z}/p\mathbb{Z}\}$. Thus the Galois group of this equation is either trivial or is $\mathbb{Z}/\mathbb{Z}$. **If $x^p - x - b$ is irreducible in characteristic p , its Galois group is $\mathbb{Z}/p\mathbb{Z}$.** If not, it splits into linear factors over K and its Galois group is trivial.

4 11/16 (Solvability, Cyclotomic Polynomials)

- A **cyclic (abelian)** extension is a Galois extension L/K whose Galois group is cyclic (abelian).
- We say a polynomial equation is **solvable by radicals** if its roots can be expressed using only field operations and n th roots, or in characteristic p if it can also be expressed in roots of the Artin-Schrier equation. Equivalently, a field extension L/K is **solvable by radicals** if there is a tower of field extensions:

$$K = K_0 \leq K_1 \leq K_2 \leq \dots \leq K_n = L$$

such that for each i , there is $a_i \in K_i$ such that:

$$K_{i+1} = K_i(\sqrt[k_i]{a_i})$$

- A group G is **solvable** if it admits a cyclic tower. This is equivalent to the group admitting an abelian tower, as any abelian tower may be refined to a cyclic one.
- A polynomial $f(x) \in K[X]$ is **solvable by radicals** iff its Galois group G is **solvable** (assuming the base field K contains all the relevant roots of unity).

Proof. Suppose that $f(x)$ is solvable in radicals with the tower $K_0 \leq K_1 \leq \dots \leq K_n = L$. We look at the Galois groups $G_0 \geq G_1 \geq \dots \geq G_n = \{1\}$. Then $K_{i+1} = K_i(\sqrt[k_i]{a_i})$ and so the extension K_{i+1}/K_i is Galois as the base field contains all the k_i th roots of unity. Thus, K_{i+1}/K_i is normal, so $G_{i+1} \trianglelefteq G_i$. We have already shown that if we have all the roots of unity, a radical extension has a cyclic Galois group, so $\text{Gal}(K_{i+1}/K_i) = G_i/G_{i+1}$ is cyclic, so the group G has a cyclic tower and is solvable. Conversely, suppose G is solvable with tower $G_0 \geq G_1 \geq \dots \geq G_n$. Each G_i/G_{i+1} is cyclic and so the extension K_{i+1}/K_i is either cyclic or generated by the Artin-Schrier polynomial (if the characteristic is p), and so the equation is solvable in radicals. □

All polynomials of degree ≤ 4 are solvable in radicals because the group S_4 admits a cyclic tower $\{1\} \trianglelefteq V_4 \trianglelefteq A_4 \trianglelefteq S_4$, and any subgroup of a solvable group is solvable.

- **Cyclotomic Polynomials:** The n th roots of unity are the roots of $x^n - 1$ over $\mathbb{Q}$. We call a n th root of unity ξ_n **primitive** if $\forall d|n, d < n$, ξ_n is not a d th root of unity. We define the n th cyclotomic polynomial to be:

$$\Phi_n(x) := \prod_{\xi_n} (x - \xi_n)$$

The cyclotomic polynomials all have coefficients in $\mathbb{Z}$, and have degree $\phi(n)$, where ϕ is Euler's totient function. To compute $\Phi_n(x)$, we divide $x^n - 1$ by all the cyclotomic polynomials less than n dividing n . For an example of this, see notes.

- $\Phi_n(x)$ is irreducible over $\mathbb{Q}$ with Galois group $(\mathbb{Z}/n\mathbb{Z})^*$
- **Example:** Suppose $n \in \mathbb{Z}$. Then there are infinitely many primes $p > 0$ such that $p \equiv 1 \pmod n$.

TODO proof.

- **Theorem:** Given a finite abelian group G , there is an abelian extension $K/\mathbb{Q}$ such that $\text{Gal}(K/\mathbb{Q}) = G$.

Put $G = (\mathbb{Z}/n_1\mathbb{Z}) \times (\mathbb{Z}/n_2\mathbb{Z}) \times \dots \times (\mathbb{Z}/n_k\mathbb{Z})$ with each n_i coprime. By above, we can choose distinct primes p_i such that $p_i \equiv 1 \pmod{n_i}$. Then $\mathbb{Z}/n_i\mathbb{Z}$ is a quotient of $(\mathbb{Z}/p_i\mathbb{Z})^*$ as it is cyclic of order $p_i - 1$ and $n_i | p_i - 1$, so G is a quotient of $(\mathbb{Z}/p_1\mathbb{Z})^* \times (\mathbb{Z}/p_2\mathbb{Z})^* \times \dots \times (\mathbb{Z}/p_k\mathbb{Z})^* \cong (\mathbb{Z}/p_1p_2\dots p_k\mathbb{Z})^*$ by the Chinese remainder theorem. But the group $(\mathbb{Z}/p_1p_2\dots p_k\mathbb{Z})^*$ is the Galois group of $\Phi_{p_1\dots p_k}(x)$, and so G is a quotient of a Galois group and hence a Galois group.

- **Kronecker-Weber-Hilbert Theorem:** If $K/\mathbb{Q}$ is Galois with $\text{Gal}(K/\mathbb{Q})$ abelian, then K is contained in a cyclotomic extension of $\mathbb{Q}$, i.e. $K \leq \mathbb{Q}(\xi)$ for some primitive n th root of unity ξ .
- **Wedderburn's Theorem:** Any finite division algebra is a field.

Recall any group G is a union of its conjugacy classes, and the order of a conjugacy class is the index of its stabilizer, i.e. $|Gx| = (G : G_x)$ for $G_x := \{g \in G : gxg^{-1} = x\}$. Let L be a finite division algebra with center K . We induct on the size of the division algebra. K is obviously a field, so $K = \mathbb{F}_q$ for some prime power q , and L is a K -vector space of dimension n for some n . Look at $G = K^*$ with $|G| = q - 1$. Suppose $a \in G$. The stabilizer of a in L under conjugation is a subalgebra of L and therefore a K -vector space, so the size is q^k . This includes 0, so the size is really $q^k - 1$. By the class equation on L^* :

$$|L^*| = q^n - 1 = |Z(G)| + \sum_i (G : C_G(a_i)) = (q - 1) + \sum_i \frac{q^n - 1}{q^{k_i} - 1}$$

with each $k_i < n$. Note that $q^n - 1$ and $\frac{q^n - 1}{q^{k_i} - 1}$ are divisible by $\Phi_n(q)$ as $k_i | n$, so this implies $q - 1$ is divisible by $\Phi_n(q)$ as well and thus $\Phi_n(q) = \prod_{i \in (\mathbb{Z}/n\mathbb{Z})^*} (q - \xi_i) \leq q - 1$. But $|q - \xi| > |q - 1|$ unless $\xi = 1$, so this implies $n = 1$ and thus $L = K$.

5 11/21 (Norm and Trace)

- **Definitions:** Let l/K be a finite extension, and choose some $a \in L$. The map $m_a : L \rightarrow L, x \mapsto ax$ is a linear transformation of L as a K -vector space. We define the **trace** and the **norm** of a to be:

$$\begin{aligned} \text{tr} : L &\rightarrow K & \text{tr}(a) &:= \text{tr}(m_a) \\ N : L^* &\rightarrow K^* & N(a) &:= \det(m_a) \end{aligned}$$

The norm and the trace are homomorphisms, i.e. $N(ab) = N(a)N(b)$ and $tr(a + b) = tr(a) + tr(b)$.

- **Norm, Trace as Galois conjugates:** Suppose $L = K(a)$. Then a is the root of an irreducible $p(x) := x^n + b_{n-1}x^{n-1} + \dots + b_0 = 0$, and we can pick a basis of L/K to be $\{1, a, a^2, \dots, a^{n-1}\}$, and the matrix of a in this basis is upper triangular except for the last column (i.e. must express a^n in terms of this basis to get last column). We note the trace of this matrix is just $-b_{n-1}$ and its determinant is $\pm b_0$. If the roots of $p(x)$ are $a_1, \dots, a_n$ with $a = a_1$, then $b_{n-1} = \sum_i a_i$ and $b_0 = \pm \prod_i a_i$. This gives us a formula for the trace and norm, as we note that the Galois group acts transitively on the roots. If L/K is Galois and $G = Gal(L/K)$, this gives the following formula for the norm and trace of $a \in L$:

$$tr(a) = \sum_{\sigma \in G} \sigma a$$

$$N(a) = \prod_{\sigma \in G} \sigma a$$

- **Algebraic integers:** An **algebraic integer** α is any number which is the root of a monic polynomial in $\mathbb{Z}[X]$. For example, $\omega := \exp(2\pi i/3)$ is an algebraic integer because it is a root of $\Phi_3(x) = x^2 + x + 1 = 0$. Algebraic integers form a ring under the usual addition and multiplication.

Theorem: Let $L/\mathbb{Q}$ be a finite extension, and $\alpha \in L$. TFAE:

1. α is an algebraic integer.
2. We can find a finitely generated $\mathbb{Z}$ -module A in L such that $\alpha A \subset A$ (note Borchers says we may also pick A such that $L = span_{\mathbb{Q}}(A)$, but I'm not sure if this is the case).

To prove $i \implies ii$, just take $A = span_{\mathbb{Z}}\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$, where n is the degree of the minimal polynomial of α . Then evidently this is a finitely generated $\mathbb{Z}$ -module which satisfies $\alpha A \subset A$ as α^n is a linear combination of its lower powers. For the converse, view α as a linear map $T : x \mapsto \alpha x \in End(A)$. α is obviously an eigenvalue of this, so $char_T(\alpha) = 0$, and $char_T(x) \in \mathbb{Z}[X]$ as we are working over $\mathbb{Z}$, so α is an algebraic integer.

- **Quadratic Fields:** Suppose N is squarefree and $L = \mathbb{Q}(\sqrt{N})$ — we will determine the algebraic integers in L . The obvious examples are $m + n\sqrt{N}$, since $\sqrt{N}$ is an algebraic integer and they form a ring. The key here is that if α is an algebraic integer, then so are $tr(\alpha)$ and $N(\alpha)$, as $\sigma\alpha$ will be an algebraic integer since it will satisfy the same polynomial as α . Since algebraic integers form a ring, $tr(\alpha)$ and $N(\alpha)$ will be algebraic integers, and will be in $\mathbb{Z}$ because the only degree 1 algebraic integers over $\mathbb{Q}$ are elements of $\mathbb{Z}$. We pick a basis $\beta := \{1, \sqrt{N}\}$ of $L/\mathbb{Q}$, and compute the trace and norm of $m + n\sqrt{N}$. Let $T_{m,n}$ be the linear transformation $x \mapsto (m + n\sqrt{N})x$. Then:

$$[T_{m,n}]_{\beta} = \begin{pmatrix} m & nN \\ n & m \end{pmatrix}$$

We see that, for $m + n\sqrt{N} \in L$:

$$\begin{aligned} N(m + n\sqrt{N}) &= \det(T_{m,n}) = m^2 - n^2N \\ \text{tr}(m + n\sqrt{N}) &= \text{tr}(T_{m,n}) = 2m \end{aligned}$$

Since the trace and norm are in $\mathbb{Z}$, this implies that either $m \in \mathbb{Z}$ or $m \in \mathbb{Z} + \frac{1}{2}$. If $m \in \mathbb{Z}$, then $n^2N \in \mathbb{Z}$, so $n \in \mathbb{Z}$ as N is squarefree (for if $n = \frac{c}{d}$ with $\gcd(c, d) = 1$, then $c^2N = d^2k \implies d^2|N \implies d = 1$). This therefore reduces to the first case of $m + n\sqrt{N}$ for $m, n \in \mathbb{Z}$. Suppose $m \in \mathbb{Z} + \frac{1}{2}$. Then $m^2 = k + \frac{1}{4} \implies \frac{1}{4} - n^2N \in \mathbb{Z} \implies (2n)^2N \equiv 1 \pmod{4}$. For $N \equiv 2, 4 \pmod{4}$ this has no solutions, and for $N \equiv 1 \pmod{4}$ this has solutions $2n$ odd. Thus, the algebraic integers of $\mathbb{Q}(\sqrt{N})$ are:

$$\begin{cases} \mathbb{Z}[\sqrt{N}] & n \equiv 2, 3 \pmod{4} \\ \mathbb{Z}[\frac{1+\sqrt{N}}{2}] & n \equiv 1 \pmod{4} \end{cases}$$

- **Theorem (Artin):** Let G be a group or monoid, and K a field. A **character** of G with values in K is a homomorphism $\chi : G \rightarrow K^*$. If $\chi_1, \dots, \chi_n$ are distinct characters, then they are linearly independent, i.e. $\forall g \in G \ a_1\chi_1(g) + \dots + a_n\chi_n(g) = 0$ implies $a_1 = \dots = a_n = 0$.
- **Trace as a bilinear form:** The trace gives us a bilinear form $(\cdot, \cdot) : L \times L \rightarrow K$ given by:

$$(a, b) := \text{tr}(ab)$$

i.e. this form is linear in each argument. We say a bilinear form is **degenerate** if the map $b \mapsto (a \mapsto (a, b))$ is not an isomorphism of L with its dual space. Equivalently, a bilinear form is degenerate if there is a nonzero $x \in L$ such that $\forall y \in L, (x, y) = 0$, so this form is degenerate if $\text{tr}(a) = 0$ for every $a \in L$. For example, take $L = \mathbb{F}_p(t)$ and $K = \mathbb{F}_p(t^p)$. Then $\text{tr} : L \rightarrow K$ is identically zero on L because every element of L has minimal polynomial of the form $x^p - a$, $a \in \mathbb{F}_p(t^p)$ and so the coefficient on x^{p-1} , which is the trace, is 0.

We note that **for separable extensions, the trace is not identically 0**, so $(\cdot, \cdot)$ is nondegenerate. In characteristic 0, this is easy as $\text{tr}(1) = \sum_{\sigma \in G} \sigma(1) = |G| = [L : K] \neq 0$.

For any Galois extension L/K , the form $(\cdot, \cdot)$ is nondegenerate (equivalently, the trace does not vanish completely on L). This is because $\text{tr}(a) = \sigma_1(a) + \dots + \sigma_n(a)$, and we may view each $\sigma \in \text{Gal}(L/K)$ as a character $L^* \rightarrow L^*$. So, if the trace vanishes for every element of L , then this contradicts Artin's theorem on independence of characters, and thus the trace is not identically zero.

- **Discriminant of a Field Extension:** Let L/K be a field extension. We define the **discriminant** of L/K to be the discriminant of the bilinear form $(a, b) = \text{tr}(ab)$ on L as a K -vector space. If $a_1, \dots, a_n$ is a basis for L/K , then this is:

$$\text{Disc}_{L/K}(a_1, \dots, a_n) = \det \begin{pmatrix} (a_1, a_1) & (a_1, a_2) & \cdots \\ (a_2, a_1) & (a_2, a_2) & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix}$$

Note the discriminant is not independent of basis: if $b_1, \dots, b_n$ is another basis and $b_i = \sum_j A_{ij}a_j$, then:

$$Disc_{L/K}(a_1, \dots, a_n) = \det(A)^2 Disc_{L/K}(b_1, \dots, b_n)$$

However, it is defined up to multiplication by a square, and thus $Disc_{L/K} \in K^*/K^{*2}$

Suppose $L = K(a)$ is Galois. Let $p(x)$ be the minimal polynomial of a in $K[X]$, and pick the basis $\{1, a, a^2, \dots, a^{n-1}\}$ of L/K . Then the traces reduce to $tr(a^k) = \sum_{\sigma \in G} \sigma a^k$, and we may plug these in so simplify the discriminant to the product of two Vandermonde determinants. This ends up simplifying to:

$$Disc_{L/K}(1, a, \dots, a^{n-1}) = \prod_{i < j} (\sigma_i a - \sigma_j a)^2 = \Delta^2$$

where Δ^2 is the discriminant of the polynomial $p(x)$.

Discriminant applications: Which of the following fields are isomorphic?

1. $\mathbb{L} = \mathbb{Q}[X]/(x^3 + x + 1), Disc(L/\mathbb{Q}) = -31.$
2. $\mathbb{L} = \mathbb{Q}[X]/(x^3 + x - 1), Disc(L/\mathbb{Q}) = -31$
3. $\mathbb{L} = \mathbb{Q}[X]/(x^3 - x + 1), Disc(L/\mathbb{Q}) = -23$

The first two have equal discriminants and are thus isomorphic; it is possible for two non-isomorphic extensions to have the same discriminant, but this is quite rare. Note that -23 and -31 are not equal modulo a square as $\frac{-31}{-23}$ is not a square in $\mathbb{Q}$, so these discriminants are not equal.

Another example is that of finding algebraic integers in $L = \mathbb{Q}(\alpha)$ with $\alpha^3 + \alpha + 1 = 0$. The discriminant of the basis $\{1, \alpha, \alpha^2\}$ in this extension is -31 . Let A be the $\mathbb{Z}$ -linear span of this basis, and let B be all algebraic integers in L . Clearly $A \subset B$ as α is an algebraic integer, and we wish to show $A = B$. If X is the change of basis from A to B , then $Disc_{L/\mathbb{Q}}(B) = \det(X)^2 Disc_{L/\mathbb{Q}}(A)$, and $\det(X) = |B/A|$. Since -31 is square-free, $\det(X)^2 = 1$, so $|B/A| = 1 \implies A = B$. This generalizes to any square-free discriminant, so if the discriminant is square-free we can easily identify the ring of algebraic integers in $L/\mathbb{Q}$.

- **Theorem:** If L/K is a finite Galois extension of finite fields, then $N : L^* \rightarrow K^*$ and $tr : L \rightarrow K$ are surjective.

Essentially, take $q = |K|$ and $n = [L : K]$. Then $Gal(L/K) = \langle F \rangle$ where $F : x \mapsto x^q$ is the Frobenius element, so:

$$N(a) = \prod_{i=0}^{n-1} F^i(a) = a \cdot a^q \cdot a^{q^2} \cdot \dots \cdot a^{q^{n-1}} = a^{\frac{q^n-1}{q-1}}$$

As the polynomial $x^{\frac{q^n-1}{q-1}} - 1$ has degree $\frac{q^n-1}{q-1}$, it has $\leq \frac{q^n-1}{q-1}$ roots and therefore $|ker(N)| \leq \frac{q^n-1}{q-1}$. The order of L^* is $q^n - 1$, and since $L^*/ker(N) \cong im(N)$, we

have:

$$q^n - 1 = |L^*| = |\text{im}(N)| \times |\ker(N)| \leq \frac{q^{n-1}}{q-1} |\text{im}(N)| \implies q-1 \leq |\text{im}(N)|$$

which implies that $\text{im}(N) = K^*$ as this is the order of K^* .

6 11/28 (Solving Equations, Galois Cohomology)

- **Lemma:** This is a simple and useful lemma that we will use often in this lecture. Suppose G is a finite group acting on a K -vector space V . Let $g \in G$ have order n . Then, for any $v \in V$, the vector:

$$w := \sum_{i=0}^{n-1} g^i(v)$$

is fixed under the action of g , i.e. $g(w) = w$.

Proof.

$$g(w) = g\left(\sum_{i=0}^{n-1} g^i(v)\right) = \sum_{i=1}^n g^i(v) = g^n(v) + \sum_{i=1}^{n-1} g^i(v) = v + \sum_{i=1}^{n-1} g^i(v) = \sum_{i=1}^n g^i(v) = w$$

□

- **Hilbert's Theorem 90:** Suppose L/K is a cyclic Galois extension with generator σ and degree $n = [L : K]$. Then:

$$N(a) = 1 \iff a = \frac{b}{\sigma b}$$

for some $b \in L^*$.

Proof. If $a = \frac{b}{\sigma b}$, then we have $N(a) = 1$ because $N(\sigma b) = N(b)$ by reindexing the finite sum over the group. Conversely, suppose $N(a) = 1$. We wish to find a fixed vector $b \in L^*$ under the linear map $a\sigma$, i.e. a vector b with $a\sigma b = b$. By the above lemma, if $a\sigma$ has finite order, we may just average over it acting on an arbitrary $v \in L$ to find b . Note that $(a\sigma)^2(v) = a\sigma(a\sigma(v)) = a\sigma(a)\sigma^2(v)$, and in general:

$$(a\sigma)^i = a\sigma(a)\sigma^2(a)\dots\sigma^{i-1}(a)\sigma^i$$

Then since $\sigma^n = \text{id}$, $(a\sigma)^n = a\sigma(a)\sigma^2(a)\dots\sigma^{n-1}(a)\sigma^n = \prod_{i=0}^{n-1} \sigma^i(a) = N(a) = 1$, so $a\sigma$ has finite order. Thus we may take an arbitrary $\theta \in L$ and find a fixed vector to be:

$$b = \sum_{i \in \mathbb{Z}/n\mathbb{Z}} (a\sigma)^i(\theta)$$

We must show that θ can be picked to make b nonzero, and then we will be done. This follows from independence of the characters $\{1, \sigma, \dots, \sigma^{n-1}\}$, as we have $b = (c_0\sigma^0 + c_1\sigma + \dots + c_{n-1}\sigma^{n-1})\theta$ for $c_i = a\sigma(a)\sigma^2(a)\dots\sigma^{i-1}(a) \in L$, so if b was identically 0 for every $\theta \in L$, this would contradict Artin's theorem.

□

- **Remember relations between roots:** Suppose $f(x)$ is separable with degree n and roots $\alpha_1, \dots, \alpha_n$. Then recall:

$$f(x) = \prod_{i=1}^n (x - \alpha_i) = x^n - e_1x^{n-1} + e_2x^{n-2} + \dots$$

where $e_1 = \sum_{i=1}^n \alpha_i$, ..., are the elementary symmetric functions in variables α_i . In particular, this allows one to easily determine $\sum_{i=1}^n \alpha_i$ and $\prod_{i=1}^n \alpha_i$ by looking at the coefficient on the x^{n-1} term and the constant term.

- **Solving $x^3 + x + 1 = 0$:** Let L be the splitting field, and we will work over $\mathbb{Q}(\omega)$, for $\omega = \exp(2\pi i/3)$, a primitive 3rd root of unity. This has discriminant -31 which is not a square in $\mathbb{Q}(\omega)$, so $\text{Gal}(L/\mathbb{Q}) = S_3$. S_3 is solvable by the cyclic tower:

$$1 \trianglelefteq \mathbb{Z}/3\mathbb{Z} \trianglelefteq S_3$$

We may use the Galois correspondence to get the corresponding tower of fixed fields:

$$L \geq K \geq \mathbb{Q}(\omega)$$

The degree $[K : \mathbb{Q}(\omega)] = (S_3 : A_3) = 2$, and so $K/\mathbb{Q}(\omega)$ is a quadratic extension. Let the roots of f be $\alpha_1, \alpha_2, \alpha_3$, and let $\sigma = (123)$. S_3 acts on the roots by permuting them, and we want to find $K = L^{A_3}$, and $A_3 = \langle \sigma \rangle$. Note that $\Delta = \sqrt{-31} = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)$ is fixed by σ but not by transpositions, so $K = \mathbb{Q}(\omega)(\Delta) = \mathbb{Q}(\omega)(\sqrt{-31})$. Now, $[L : K] = 3$ so $\text{Gal}(L/K) \cong \mathbb{Z}/3\mathbb{Z}$, and since K contains all the 3rd roots of unity, this implies $L = K(\sqrt[3]{b})$ for some b . But (from the proof above with cyclic Galois group and ground field containing roots of unity) we have $\sqrt[3]{b} = w$ with $\sigma w = \omega w$. Note that for any $c \in L$, $c + \omega^{-1}\sigma(c) + \omega^{-2}\sigma^2(c)$ has eigenvalue ω under σ , and so we may take any linear combination like this. So, pick $c = \alpha_1$ and take $y := \alpha_1 + \omega^{-1}\sigma(\alpha_1) + \omega^{-2}\sigma^2(\alpha_1) = \alpha_1 + \omega^{-1}\alpha_2 + \omega^{-2}\alpha_3$, and so $L = K(y)$, and y is a cube root of an element of K . Similarly, let $z = \alpha_1 + \omega\alpha_2 + \omega^2\alpha_3$, which has eigenvalue $\omega^{-1} = \omega^2$. Furthermore, $0 = \alpha_1 + \alpha_2 + \alpha_3$ as the coefficient on x^2 is 0, and this has eigenvalue 1— if we can find y^3, z^3 , we can solve for the roots by linear algebra. We know both y^3 and z^3 are in K and therefore are fixed by σ . We can expand out $y^3 + z^3$ in terms of the α_i to get that $y^3 + z^3 = -27c$ and $y^3b^3 = -27b^3$, so y^3 and z^3 are roots of $x^2 + 27x - 27 = 0$, and we may solve for y^3, z^3 , then solve for y, z , and finally solve for the roots α_i .

- **Solving 4th degree polynomials:** TODO

- **Galois Cohomology:** Suppose G acts on a module M . We can define the **invariants** of M under G by:

$$M^G = \{m \in M : gm = m, \forall g \in G\}$$

This is the largest submodule of M upon which G acts trivially. We can define the dual notion to be the largest quotient of M upon which G acts trivially:

$$M_G = M / \{m - gm : g \in G, m \in M\}$$

Now, the functors $M \mapsto M^G$ and $M \mapsto M_G$ are **not exact**. They are both covariant functors, but $M \mapsto M^G$ is **left exact** and $M \mapsto M_G$ is **right exact**, i.e. if $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ is exact, then the following are as well:

$$0 \rightarrow A^G \rightarrow B^G \rightarrow C^G$$

$$A_G \rightarrow B_G \rightarrow C_G \rightarrow 0$$

We often want to know how these fail to be exact. Let $\mathbb{Z}G$ be the group ring of G over $\mathbb{Z}$. We note that:

$$M^G \cong \text{Hom}_{\mathbb{Z}G}(\mathbb{Z}, M)$$

by the bijection sending $m \in M^G$ to the map $\phi_m : z \mapsto zm$. Note we view $\mathbb{Z}$ is a $\mathbb{Z}G$ module with g acting trivially on $\mathbb{Z}$, i.e. $gz = z$. This will be a $\mathbb{Z}G$ homomorphism, as it clearly respects $+$ and $\phi_m((\sum_{g \in G} c_g g)z) = \phi_m(\sum_{g \in G} c_g z) = (\sum_{g \in G} c_g z)m = (\sum_{g \in G} c_g g)zm = (\sum_{g \in G} c_g g)\phi_m(z)$ as $gm = m$ for $m \in M^G$. So, we may view $\cdot^G$ as the functor $\text{Hom}_{\mathbb{Z}G}(\mathbb{Z}, \cdot)$, which we recall is not exact. The failure for this to be exact is controlled by the **Ext functor**, so we put $H^0(G, M) := M^G$ and:

$$H^i(G, M) := \text{Ext}_{\mathbb{Z}G}^i(\mathbb{Z}, M)$$

Similarly, we have:

$$M_G \cong \mathbb{Z} \otimes_{\mathbb{Z}G} M$$

and the failure for $\otimes$ to preserve exactness is measured by *Tor*. We then define $H_0(G, M) := M_G$, and:

$$H_i(G, M) := \text{Tor}_i^{\mathbb{Z}G}(\mathbb{Z}, M)$$

These are the **ith cohomology groups**. They measure how inexact a sequence is— for an exact sequence $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$, the sequence $0 \rightarrow H^0(A) \rightarrow H^0(B) \rightarrow H^0(C) \rightarrow H^1(A) \rightarrow H^1(B) \rightarrow H^1(C) \rightarrow H^2(A) \rightarrow \dots$ is exact.

7 11/30 (Galois Cohomology, Infinite Extensions)

- **Crossed Homomorphisms:** Let G act on an abelian group A by means of a homomorphism $G \rightarrow \text{Aut}(A)$ (for example, G a Galois group acting on a L^*). We define a **crossed homomorphism**, also called a **1-cocycle**, to be a map $G \rightarrow A$ with $\sigma \mapsto a_\sigma \in A$ satisfying:

$$a_{\sigma\tau} = a_\sigma + \sigma a_\tau$$

We may equivalently view a 1-cocycle as a family of elements $\{a_\sigma\}_{\sigma \in G}$ satisfying this relation. If $\{a_\sigma\}_{\sigma \in G}$ and $\{b_\sigma\}_{\sigma \in G}$ are 1-cocycles, then $\{a_\sigma + b_\sigma\}_{\sigma \in G}$ is also a 1-cocycle, and so 1-cocycles form a group, which we write as $Z^1(G, A)$. By a **principal crossed homomorphism**, also called a **1-coboundary**, we mean a 1-cocycle $\{a_\sigma\}_{\sigma \in G}$ such $\exists \beta \in A$ such that

$$a_\sigma = \beta - \sigma(\beta), \forall \sigma \in G$$

Note we use $\beta - \sigma\beta$ here, but we may use $\beta/\sigma\beta$ if the group law is multiplicative. These similarly form a group, which we write as $B^1(G, A)$. Lang's definition of the **first cohomology group** is:

$$H^1(G, A) := Z^1(G, A)/B^1(G, A)$$

- **Hilbert's Theorem 90, Generalized:** Let L/K be a Galois extension with $G = \text{Gal}(L/K)$. Then:

$$H^1(G, L^*) = \{1\}$$

and:

$$H^1(G, L) = \{0\}$$

Proof. We must show that every 1-cocycle is a 1-coboundary. Let $\{a_\sigma\}_{\sigma \in G}$ be a 1-cocycle. Note the map $a_\sigma \sigma : L \rightarrow L$ is a linear map on L , and so we get a map $\phi : G \rightarrow \text{End}(L), \sigma \rightarrow a_\sigma \sigma$. This is in fact a homomorphism: note that $(a_\sigma \sigma)(a_\tau \tau)(v) = a_\sigma \cdot \sigma(a_\tau \tau(v)) = a_\sigma \cdot \sigma(a_\tau) \sigma(\tau(v)) = (a_\sigma \sigma a_\tau \sigma \tau)(v)$, so $\phi(\sigma\tau) = a_{\sigma\tau} \sigma\tau = a_\sigma \sigma a_\tau \sigma \tau = (a_\sigma \sigma)(a_\tau \tau) = \phi(\sigma)\phi(\tau)$. Now, we wish to show there is a b that is fixed under this map $a_\sigma \sigma$, i.e. $a_\sigma \sigma b = b$. G still acts on L^* by the twisted action $\sigma \mapsto a_\sigma \sigma$ as this is a homomorphism, and so we can use our usual technique of averaging elements. That is, for each $v \in L^*$:

$$b := \sum_{\sigma \in G} a_\sigma \sigma(v)$$

is fixed under the action. But, the elements $a_\sigma \sigma$ are still characters on L^* , and so by linear independence of characters we may find a v making b nonzero, and thus $\forall \sigma \in G$, $a_\sigma = b/\sigma b$, and so $\{a_\sigma\}_{\sigma \in G}$ is a 1-coboundary. □

Note this is stronger than the earlier statement of the theorem. Suppose that G is cyclic and $G = \langle \sigma \rangle$. Then we may define $a_1 = 1, a_\sigma = a, a_{\sigma^2} = a\sigma(a) = a\sigma a, \dots, a_{\sigma^i} = a\sigma(a)\sigma^2(a)\dots\sigma^{i-1}(a)$. We have $a_{\sigma^n} = N(a)$, so if $N(a) = 1 \implies a_{\sigma^n} = 1$ and $\{a_{\sigma^i}\}$ is a 1-cocycle, which implies it is a 1-coboundary. Thus, there is some $b \in L^*$ with $a_{\sigma^i} = b/\sigma^i b$ for every i , and in particular for $i = 1$ this gives $a_\sigma = a = b/\sigma b$.

- **Normal Basis Theorem:** Let L/K be a Galois extension of degree n , and let $\text{Gal}(L/K) = \{\sigma_1, \dots, \sigma_n\}$. Then, there is an element $w \in L$ such that $\{\sigma_1 w, \dots, \sigma_n w\}$ form a basis of L/K .
- **Equivalence of H^1 Definitions:** **TODO**

- **Infinite Galois Extensions:** We define an **infinite Galois extension** to be an algebraic, normal, and separable extension. Let L/K be an infinite Galois extension. How can we compute $Gal(L/K)$? The idea is to look at all finite Galois subextensions L_i/K . We can induce a map from G into the inverse limit of this family, and this will end up being an isomorphism. So, if we let i range over finite normal subextensions L_i of L/K , then:

$$Gal(L/K) = \varprojlim_i Gal(L_i/K)$$

- **Example: Algebraic closure of $\mathbb{F}_p$:** Let $L = \bar{\mathbb{F}}_p$ be the algebraic closure of $K = \mathbb{F}_p$. Then:

$$L = \bigcup_{k \geq 1} \mathbb{F}_{p^k}$$

Recall that $Gal(\mathbb{F}_{p^k}/\mathbb{F}_p) \cong \mathbb{Z}/k\mathbb{Z}$, so we get:

$$Gal(\bar{\mathbb{F}}_p/\mathbb{F}_p) = \varprojlim_n \mathbb{Z}/n\mathbb{Z} \cong \prod_p \mathbb{Z}_p$$

where $\mathbb{Z}_p = \varprojlim_k \mathbb{Z}/p^k\mathbb{Z}$ is the p -adic integers.

This group $\varprojlim_n \mathbb{Z}/n\mathbb{Z}$ is called the **profinite completion** of $\mathbb{Z}$.

- **Profinite Groups:** A group is **profinite** if it is the inverse limit of a directed system of finite groups. The **profinite completion** of G is the group:

$$\varprojlim_i G/G_i \subset \prod_i G/G_i$$

where i ranges over all normal $G_i \trianglelefteq G$ with $(G : G_i)$ finite. We get a homomorphism $G \rightarrow \varprojlim_i G/G_i$, and the image of G is dense in the Krull topology.

- **The Krull Topology:** Recall that to give a set S the **discrete topology** means to let each subset of S be open. Given a collection $\{X_i\}_{i \in I}$ of topological spaces, we may give this the **product topology** by defining a base for the open sets of $\prod_i X_i$ to be the open sets of each X_i times X_j for all $j \neq i$. In other words, the open sets of $\prod_i X_i$ are:

$$\prod_i U_i$$

where U_i is open in X_i and $U_i \neq X_i$ for all but finitely many i .

- **Cyclotomic Extension of $\mathbb{Q}$:** We take

$$L = \bigcup_n \mathbb{Q}(\xi_n)$$

and $K = \mathbb{Q}$, where ξ_n is a primitive n th root. We have that $Gal(\mathbb{Q}(\xi_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$, so:

$$Gal(L/\mathbb{Q}) = \varprojlim_n (\mathbb{Z}/n\mathbb{Z})^* \cong \prod_p \mathbb{Z}_p^*$$

Kummer Theory: The problem is to find all abelian extensions of K , given that K has "enough" roots of unity. Let $\bar{K}$ be the separable algebraic closure of K , so the largest separable extension of K in the algebraic closure, and $\mu_n \subset \bar{K}^*$. We examine:

$$1 \rightarrow \mu_n \rightarrow \bar{K}^* \xrightarrow{x \mapsto x^n} \bar{K}^* \rightarrow 1$$

These groups are acted on by $G := \text{Gal}(\bar{K}/K)$, and we assume $\mu_n \subset K$. We look at the invariants under $\text{Gal}(\bar{K}/K)$. The invariants of $\bar{K}^*$ will be K^* as K is fixed, and μ_n is contained in K , and so will be invariant. Since $\cdot^G$ is left exact, we get:

$$1 \rightarrow \mu_n \rightarrow K^* \xrightarrow{x \mapsto x^n} K^* \rightarrow H^1(G, \mu_n) \rightarrow H^1(G, \bar{K}^*) \rightarrow \dots$$

By Hilbert's theorem 90, $H^1(G, \bar{K}^*) = 1$ is trivial, and $H^1(G, \mu_n) \cong \text{Hom}(G, \mu_n)$ because G acts trivially on μ_n , so we get the exact sequence:

$$K^* \xrightarrow{x \mapsto x^n} K^* \rightarrow \text{Hom}(G, \mu_n) \rightarrow 1$$

We have that $\text{Hom}(G, \mu_n) \cong K^*/(K^*)^n$, and the kernel of elements in $\text{Hom}(G, \mu_n)$ is the subgroups $H \trianglelefteq G$ with G/H cyclic of order n , which is the same as the cyclic Galois extensions L/K .