Abstract Algebra. Math 6320. Bertram/Utah 2022-23.
Group Characters and more Galois Theory

We will prove the following foundational result of Galois Theory.

Theorem. Let F/K be a splitting field for a separable polynomial $f(x) \in K[x]$ and let $G = \text{Gal}(F/K)$ be the Galois group of the splitting field. Then:

(a) For each subgroup $H \subset G$, the intermediate "fixed field" of H:

$$F^H := \{\alpha \in F \mid h(\alpha) = \alpha \text{ for all } h \in H\} \text{ satisfies } \text{Gal}(F/F^H) = H$$

(b) If $E \subset F$ is an intermediate field, then $F^{\text{Gal}(F/E)} = E$ (inverting (a)).

(c) The subgroup H in (a) is normal if and only if F^H/K is a splitting field.

That is, fixed fields (and Galois groups) determine a bijections:

$$\{\text{subgroups of } G\} \leftrightarrow \{\text{intermediate fields } K \subset E \subset F\} \text{ and}$$

$$\{\text{normal subgroups of } G\} \leftrightarrow \{\text{intermediate splitting fields}\}$$

To get to this Theorem, we'll use a new idea.

Characters

Let G be a group and K be a field.

Definition. A *character* of G in K is a group homomorphism $\chi : E \to K^*$.

Remark. Each character satisfies $\chi(ghg^{-1}h^{-1}) = \chi(g)\chi(h)\chi(g)^{-1}\chi(h^{-1}) = 1 \in K^*$ since K^* is abelian. So each character factors through the abelian quotient by the commutator subgroup:

$$\chi : G \to G/[G,G] \to K^*$$

and these "one-dimensional" characters are therefore a feature of abelian groups.

A character of $\mathbb{Z}$ is determined by the choice of an element $\alpha = \chi(1) \in K^*$ with:

$$\chi(d) = \alpha^d \text{ for all } d \in \mathbb{Z}$$

and a character of $C_n = \mathbb{Z}/n\mathbb{Z}$ is similarly the choice of an nth root of unity in K.

A character is, in particular, a (non-zero) vector in the vector space:

$$\text{Fun}(G, K) = \{f : G \to K\}$$

and characters $\chi_1, ..., \chi_n$ are *independent* if they are linearly independent functions,

$$\text{i.e. if } \sum_{i=1}^{n} c_i\chi_i(g) = 0 \text{ for all } g \in G \text{ if and only if } c_1 = \cdots = c_n = 0 \text{ in } K$$

When $|G| < \infty$, we may choose a basis $e_g \in \text{Fun}(G, K)$ (of non-characters!) by:

$$e_g(g) = 1 \text{ and } e_g(h) = 0 \text{ otherwise}$$

and in terms of this basis, $\chi_i = \sum_{g \in G} \chi_i(g)e_g$.

Somewhat surprisingly, we have the following:

Proposition 1. Every set of distinct characters (of any group) is independent.

Proof. We will prove this by induction on the number of characters.

Let $\chi_1, ..., \chi_n : G \to K^*$ be distinct characters with $n \geq 2$, and suppose:

$$c_1\chi_1 + \cdots + c_n\chi_n = 0 \text{ is a linear relation}$$

Then for each fixed $h \in G$ and all $g \in G$, we have the identity:

$$c_1\chi_1(h)\chi_1(g) + \cdots + c_n\chi_n(h)\chi_n(g) = c_1\chi_1(gh) + \cdots + c_n\chi_n(gh) = 0$$

and subtracting this from:

$$c_1\chi_n(h)\chi_1(g) + \cdots + c_n\chi_n(h)\chi_1(g) = \chi_n(h)\left(c_1\chi_1(g) + \cdots + c_n\chi_n(g)\right) = 0$$

we get linear relations among the first $n-1$ characters (one for each value of h):

$$c_1\left(\chi_n(h) - \chi_1(h)\right)\chi_1 + \cdots + c_{n-1}\left(\chi_n(h) - \chi_{n-1}(h)\right)\chi_{n-1} = 0$$

which implies (by the inductive assumption) that:

$$c_i(\chi_n(h) - \chi_i(h)) = 0 \text{ for all } i = 1, ..., n-1 \text{ and all } h$$

But $\chi_i \neq \chi_n$ for $i < n$, so $\chi_i(h) \neq \chi_n(h)$ for some h (possibly depending on i), from which it follows that $c_1, ..., c_{n-1} = 0$ and then $c_n = 0$ as well. $\square$

Example. Consider n characters of $\mathbb{Z}$ in K given by $\chi_i(1) = x_i$ for distinct $x_i \in K^*$. Then the truncated character vectors $\chi_i(0)e_0 + ... + \chi_i(n-1)e_{n-1}$ are columns of:

$$V(x_1, ..., x_n) = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_n \\ x_1^2 & x_2^2 & \cdots & x_n^2 \\ & & \vdots & \\ x_1^{n-1} & x_2^{n-1} & \cdots & x_n^{n-1} \end{bmatrix}$$

the Vandermonde matrix with (nonzero!) determinant $D = \prod_{1 \leq i < j \leq n}(x_j - x_i)$. This independently verifies that any finite set of characters of $\mathbb{Z}$ is independent.

If we take, instead, the n characters of C_n in $\mathbb{C}$ with $\chi_i(1) = \omega^i$, we get:

$$D = \prod_{0 \leq i < j < n} (\omega^j - \omega^i) \in \mathbb{Q}(\omega)$$

as the determinant of the Vandermonde. This can be computed! From:

$$f(x) = x^n - 1 = \prod_{i=0}^{n-1}(x - \omega^i) \text{ we get } nx^{n-1} = f'(x) = \sum_{i=0}^{n-1}\prod_{i \neq j}(x - \omega^i)$$

and in particular, $n(\omega^j)^{n-1} = \prod_{i \neq j}(\omega^j - \omega^i)$. Thus the product satisfies:

$$n^n \cdot \omega^{(n-1)\binom{n}{2}} = \prod_{j=0}^{n-1} n(\omega^{j(n-1)}) = \prod_{i \neq j}(\omega^j - \omega^i) = (-1)^{\binom{n}{2}}D^2$$

so that in particular, if n is odd:

$$D = \pm\sqrt{(-1)^{\binom{n}{2}}n^n} \in \mathbb{Q}(\omega_n)$$

and as a consequence, $\sqrt{(-1)^{\binom{n}{2}}n} \in \mathbb{Q}(\omega_n)$, generating an intermediate "quadratic" field (as long as $(-1)^{\binom{n}{2}}n$ is not a perfect square) corresponding to a subgroup of the Galois group of order $\phi(n)/2$. This "explains" the appearances of $\sqrt{-3}$, $\sqrt{5}$ and $\sqrt{-7}$ in the fields $\mathbb{Q}(\omega_3), \mathbb{Q}(\omega_5)$ and $\mathbb{Q}(\omega_7)$, respectively.

Corollary. If G is an abelian group with $|G| = n$, then G has at most n characters with values in a field K and exactly n characters with values in $\mathbb{C}$.

Proof. $\mathrm{Fun}(G, K)$ has dimension n as a vector space over K, so there are at most n distinct characters by the Proposition. Letting $G = \prod C_{n_i}$ be a product of cyclic groups with generators g_i and $\prod n_i = n$, then setting each g_i to an n_ith root of unity in $\mathbb{C}$ determines a distinct character, and there are n of them. $\square$

Now let F/K be a splitting field for a separable $f(x) \in K[x]$, and consider:

$$\sigma : F \to F \text{ for } \sigma \in \mathrm{Gal}(F/K)$$

Then in particular σ is a character of the group F^* in the field F. Thus any finite collection of distinct elements of the Galois group is independent, and we have:

Corollary. The fixed field F^S of a subset $S = \{\sigma_1, ..., \sigma_m\} \subset \mathrm{Gal}(F/K)$ satisfies

$$[F : F^S] \geq m$$

with equality if S is a subgroup of the Galois group.

Proof. Let $\alpha_1, ..., \alpha_r \in F$ be a basis for F as a vector space over F^S.

If $[F : F^S] = r < m$, then the r equations in m unknowns:

$$(*_j) \quad \sigma_1(\alpha_j)x_1 + \cdots + \sigma_m(\alpha_j)x_m = 0$$

have a common non-zero solution $(c_1, ..., c_m)$ with $c_i \in F$ so $\sum_{i=1}^r c_i\sigma_i(\alpha_j) = 0$ for all basis vectors α_j.

But then $\sum_{i=1}^n c_i\sigma_i(\alpha) = 0$ for **all** $\alpha = \sum a_i\alpha_i \in F$ (with $a_i \in F^S$) since each $\sigma_i \in \mathrm{Gal}(F/K)$ is a field automorphism of F (fixing F^S). This violates the independence of the *characters* σ_i of F^* in F and so by the Proposition, $r \geq m$.

Now if S is a group and $[F : F^S] > m$, let $\alpha_1, ..., \alpha_{m+1}$ be independent vectors in F as a vector space over F^S and consider the m equations:

$$(\dagger_i) \quad \sigma_i(\alpha_1)y_1 + \cdots + \sigma_i(\alpha_{m+1})y_{m+1} = 0 \text{ in } m+1 \text{ variables}$$

As above, this system of equations has a common non-zero solution $(b_1, ..., b_{m+1})$ with $b_j \in F$. Among all such solutions, we choose one with the smallest number of non-zero entries and reorder the α_j (if necessary) so $(b_1, ..., b_s, 0, ..., 0)$ is a minimal solution, with $b_1, ..., b_s \neq 0$, and dividing through by b_s, we may assume $b_s = 1$.

Since S is a group, we have $\mathrm{id}_F \in S$, and so among these equations we have:

$$\sum \mathrm{id}_F(\alpha_j)b_j = \sum b_j\alpha_j = 0$$

from which we conclude that at least one of the b_j is outside of the fixed field F^S (otherwise the α_j would be linearly dependent vectors). Reordering again if needed, we may assume $b_1 \notin F^S$. Thus there is some $\sigma \in S$ so that $\sigma(b_1) \neq b_1$, and then:

$$0 = \sigma(\sum_{j=1}^s \sigma_i(\alpha_i)b_i) = \sum_{j=1}^s (\sigma \circ \sigma_i)(\alpha_j) \cdot \sigma(b_j)$$

for all σ_i. But because S is a group, the $\sigma \circ \sigma_i$ are simply a reordering of the elements of S, and so the equation above gives another solution:

$$(\sigma(b_1), ..., \sigma(b_s), 0, ..., 0) \text{ with } \sigma(b_s) = \sigma(1) = 1 \text{ and } \sigma(b_1) \neq b_1$$

so subtracting one solution from the other gives a solution with fewer non-zero entries, and a contradiction to the assumption that $[F : F^S] > m$. $\square$

Corollary. If $H_1, H_2 \subset \text{Gal}(F/K)$ are subgroups with $F^{H_1} = F^{H_2}$, then $H_1 = H_2$.

Proof. Let $E = F^{H_1} = F^{H_2}$. By the previous Corollary, $|H_1| = |H_2| = [F : E]$. Moreover, if $H_1 \neq H_2$, then there is an $h \in H_1$ that is not in H_2. But then by the Corollary:

$$[F : F^{H_2 \cup \{h\}}] > |H_2| = [F : E]$$

so h does not fix some element of E, giving a contradiction. $\square$

We may now prove parts (a) and (b) of the Theorem at the top of this section.

(a) Recall that $G = \text{Gal}(F/K)$ has order equal to $[F : K]$. It follows that

$$F^G = K$$

since $K \subset F^G$ and $|G| = [F : F^G]$ from the second Corollary.

We may apply this to any subgroup $H \subset G$ with fixed field F^H to get:

$$F^H = F^{\text{Gal}(\text{F}/\text{F}^{\text{H}})}$$

(letting F^H play the role of K), and then from the last Corollary, $H = \text{Gal}(F/F^H)$.

(b) Starting with an intermediate field $E \subset F$, we have:

$$E \subset F^{\text{Gal}(F/E)}$$

and $[F : F^{\text{Gal}(F/E)}] = |\text{Gal}(F/E)| = [F : E]$, so we must have equality!

Now for the third part of the Theorem, notice that conjugating subgroups of the Galois group has the effect of moving from one intermediate field to another:

$$H \subset G = \text{Gal}(F/K) \text{ with } F^H = E \subset F \text{ and } \ g \in G \text{ give}$$

$$gHg^{-1} \subset G \text{ with } F^{gHg^{-1}} = gE \subset F$$

and so $H \subset G$ is a normal subgroup if and only if $E = gE$ for all $g \in G$. So we need to show that every subfield $E \subset F$ fixed by the Galois group is a splitting field.

Proposition 2. Let K be an infinite field, and let F/K be a splitting field of a separable polynomial $f(x) \in K[x]$. Then:

(a) F/K is separable as a field extension.

(b) For each $\beta \in F$ with associated irreducible polynomial $h(x)$, the field F contains **all** the roots of $h(x)$. Thus, F contains a splitting field E/K of $h(x)$.

(c) Every subfield of F fixed by the Galois group of F/K is a splitting field.

Proof. Note that (a) is automatic if K is a perfect field. Let's assume (a), putting off the case where K is imperfect. Then the roots of $h(x)$ contained in F are distinct. If G is the Galois group of F/K, then either $\beta = \beta_1 \in K$ and $h(x)$ is linear, or else $\beta_2 = g\beta_1 \neq \beta_1$ for some $g \in G$, which finds us another root.

If $h(x)$ has two roots $\beta_1, \beta_2 \in F$ that are permuted by every element of G, then

$$\beta_1 + \beta_2 \text{ and } \beta_1\beta_2 \text{ are both elements of } K$$

since they are fixed by every element of the Galois group! Thus:

$$(x - \beta_1)(x - \beta_2) = x^2 - (\beta_1 + \beta_2)x + \beta_1\beta_2 \in K[x]$$

is the (irreducible) polynomial $h(x)$. Thus if $h(x)$ has more roots, then elements of G cannot all permute the set $\{\beta_1, \beta_2\}$, and there must be a new root $g\beta_i = \beta_3$.

We may proceed in this way, noticing that if G permutes a set of known roots $\{\beta_1, ..., \beta_d\}$ then $h(x)$ is the product $\prod_{i=1}^d (x - \beta_i)$, otherwise there is another root of $h(x)$ obtained as $\beta_{i+1} = g\beta_i$ for one of the "known" roots. This gives (b).

For (c), let $K \subset E \subset F$ be a fixed subfield. Notice that there are only finitely many intermediate fields $K \subset L \subset F$ between K and F since there are only finitely many subgroups $H \subset G$ of the Galois group! Thus, there are only finitely many intermediate fields properly contained in E, and so if K is infinite, then there is an $\alpha \in E$ that is not in any proper subfield of E. Then, remarkably,

$$K(\alpha) = E$$

and in particular, E is the splitting field of the polynomial $g(x)$ associated to α. $\square$

In fact, the last thing said is so remarkable that it is spawns a theorem.

The Theorem of the Primitive Element. If $K \subset L$ is **any** finite, separable extension of an infinite field then there is a "primitive" element α so that $L = K(\alpha)$.

Proof. Let $L = K(\alpha_1, ..., \alpha_n)$ and let $f_1(x), ..., f_n(x) \in K[x]$ be (separable) irreducible polynomials for $\alpha_1, ..., \alpha_n$. Then L is a subfield of a splitting field F/K for $f(x) = \prod f_i(x)$. But F has finitely many subfields containing K, corresponding to the subgroups of the Galois group of F/K, and in particular L has only finitely many subfields containing K. These are sub-vector spaces, and a vector space over an infinite field cannot be covered by finitely many proper subspaces, so L contains an element α outside all the subfields, which tells us that $L = K(\alpha)$. $\square$

We've made assumptions in the proof of the Proposition that we should address.

- We assumed K was infinite in the proof of (c).
- We assumed K was perfect to avoid proving (a).

Finite Fields. When $K = \mathbb{F}_q$ is a finite field with $q = p^r$ elements, the Proposition and the Theorem of the Primitive Element are still true. Of course, these fields are perfect, so (a) is automatic. The field F is isomorphic to $\mathbb{F}_{q^d}$ for some d, and

$$\mathbb{F}_q \subset \mathbb{F}_{q^d} \text{ has a } \textit{cyclic} \text{ Galois group, isomorphic to } C_d$$

The finitely many intermediate fields:

$$\mathbb{F}_q \subset \mathbb{F}_{q^e} \subset \mathbb{F}_{q^d}$$

are the fixed fields of the subgroups $C_e \subset C_d$. They are all splitting fields, and the subgroups are all normal. As for the primitive element, we may take any of the generators of the cyclic group $\mathbb{F}_{q^d}^*$.

Turning back to (a) in the Proposition, we prove the more general:

Proposition 3. Let $K \subset L$ be a field extension. Then the elements $\alpha \in L$ that are (algebraic and) separable over K form an intermediate "separable extension"

$$K \subset L_{\text{sep}} \subset L$$

Proof. Let $0 \neq \alpha, \beta \in L$ be separable over K with associated polynomials $f(x), g(x) \in K[x]$. Then the polynomial $f(-x)$ has distinct roots $-\alpha_i$, where α_i are the roots of $f(x)$, so $-\alpha$ is also separable.

Similarly, $x^{\deg(f)} f(1/x)$ has distinct roots $1/\alpha_i$, so $1/\alpha$ is separable over K.

To prove that the sum and product $\alpha+\beta$ and $\alpha\beta$ are separable over K, consider the three intermediate fields between K and $K(\alpha,\beta)$:

$$K \subset K(\alpha), K(\alpha+\beta), K(\alpha\beta) \subset K(\alpha,\beta)$$

Following the separable path $K \subset K(\alpha) \subset K(\alpha,\beta)$, we get:

$$|\mathrm{Iso}_K(K(\alpha,\beta), K(\alpha,\beta))| = [K(\alpha,\beta) : K] = [K(\alpha,\beta) : K(\alpha)] \cdot [K(\alpha) : K]$$

from Proposition 1 (of the previous section). But conversely, note that:

$$|\mathrm{Iso}_K(K(\gamma), K(\gamma))| < [K(\gamma) : K]$$

if γ is not separable over K, since the polynomial for γ has coincidental roots. Thus, following the other paths:

$$K \subset K(\alpha+\beta) \subset K(\alpha,\beta) \text{ and } K \subset K(\alpha\beta) \subset K(\alpha,\beta)$$

we conclude that $\alpha+\beta$ and $\alpha\beta$ are separable over K. □

Proposition 2 (a) follows from the special case of F/K, the splitting field of $f(x)$, since $F = K(\alpha_1, ..., \alpha_r)$ is generated by the roots of $f(x)$, and so $F_{\mathrm{sep}} = F$ and every element of F is separable over K.

In a complementary direction, consider a splitting field F/K of $f(x)$, and let:

$$K \subset F_{\mathrm{insep}} = F^{\mathrm{Gal}(F/K)} \subset F$$

be the fixed field of the Galois group $\mathrm{Iso}_K(F,F)$. This fixed field is equal to K by the foundational theorem if $f(x)$ is separable, but not otherwise. In fact, each $\alpha \in F_{\mathrm{insep}}$ is "purely inseparable" over K, i.e. its polynomial has a **single** root.

Example. The splitting field F of the polynomial

$$f(x) = x^{2p} - x^p - t \in \mathbb{F}_p(t)[x]$$

has Galois group C_2 and two intermediate extensions, namely:

$F_{\mathrm{sep}} = \mathbb{F}_p(t)(\alpha)$ where α is a root of $x^2 - x - t$, and

$F_{\mathrm{insep}} = \mathbb{F}_p(t)(\sqrt[p]{t})$, which turns $f(x)$ into $(x^2 - x - \sqrt[p]{t})^p$.

Definition. K is *algebraically closed* if there is no finite field extension $K \subset L$.

Equivalently, K is algebraically closed if each $f(x) \in K[x]$ factors "completely:"

$$f(x) = c\prod(x-\alpha_i) \text{ for } c, \alpha_i \in K$$

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

Proof. First of all, given $f(x) \in \mathbb{C}[x]$, consider the real polynomial:

$$f(x)\overline{f}(x) \in \mathbb{R}[x]$$

where $\overline{f}(x)$ is the complex conjugate polynomial.

Then from a factorization of $f(x)\overline{f}(x)$ we obtain factorizations of $f(x)$ and $\overline{f}(x)$. Thus it suffices to show that each $g(x) \in \mathbb{R}[x]$ factors completely in $\mathbb{C}[x]$.

Next, by the intermediate value theorem and the quadratic formula:

- Each polynomial $g(x) \in \mathbb{R}[x]$ of odd degree has a (real) root
- Each quadratic polynomial in $\mathbb{C}[x]$ has a complex root.

These have the following field-theoretic consequences:

• Each non-trivial finite field extension $\mathbb{R} \subset E$ has even degree.

(otherwise each $\alpha \in E - \mathbb{R}$ would give an extension $\mathbb{R} \subset \mathbb{R}(\alpha)$ of odd degree with irreducible polynomial $f(x)$ of odd degree).

• There is no field extension $\mathbb{C} \subset L$ of degree two.

For each $g(x) \in \mathbb{R}[x]$, let $F/\mathbb{R}$ be a splitting field for $(x^2 + 1)g(x)$.

Let $G = \mathrm{Gal}(F/\mathbb{R})$ with $|G| = 2^d m$, and let $E = F^H$ be the fixed field of one of the 2-Sylow subgroups $H \subset G$. Then:

$$\mathrm{Gal}(F/E) = H \text{ and so } [E : \mathbb{R}] = m \text{ is odd}$$

But this is impossible unless $E = \mathbb{R}$, so $m = 1$ and G is a 2-group.

In that case, the splitting intermediate subfield:

$$\mathbb{R} \subset \mathbb{C} = \mathbb{R}(i) \subset F \text{ (from the root of } x^2 + 1)$$

has Galois group $N = \mathrm{Gal}(F/\mathbb{C}) \subset G$, which is a normal subgroup and a 2-group with $G/N = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$. Moreover, $F/\mathbb{C}$ is the splitting field of the polynomial $g(x)$.

If N is non-trivial, then by the super-solvability of p-groups, there is a normal subgroup $N' \subset N$ with quotient $N/N' = C_2$, and then:

$$\mathbb{C} = F^N \subset F^{N'}$$

is a field extension of degree two. But this is impossible, so $N = \{e\}$, which is to say that $\mathbb{C}$ itself is the splitting field of $g(x)$, i.e. all the roots of $g(x)$ are in $\mathbb{C}$! $\square$

The complex numbers thus give us the *algebraic closure*

$$\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ is algebraic over } \mathbb{Q}\}$$

which is a minimal field containing all splitting fields of all polynomials in $\mathbb{Q}[x]$.

Remark. Finite fields also have algebraic closures. We will investigate this later.

In fact, every field has an algebraic closure.