Abstract Algebra. Math 6320. Bertram/Utah 2022-23.
Introducing Galois Theory

Let K be a field.

Definition. (a) A polynomial $f(x) \in K[x]$ is *separable* if it has no repeated roots as a polynomial in $L[x]$ for any extension $K \subset L$. .

(b) An element $\alpha \in L$ of an extension $K \subset L$ is *separable over* K if it is either transcendental for the irreducible $f(x) \in K[x]$ with $f(\alpha) = 0$ is separable.

(c) An extension $K \subset L$ is *separable* if each $\alpha \in L$ is separable over K.

(d) A field K is *perfect* if every field extension of K is separable.

Examples. If $f(x) \in K[x]$ has a repeated root α in *any* extension $K \subset L$, then

$$(x - \alpha) \text{ is a common divisor of } f(x) \text{ and } f'(x) \text{ in } L[x]$$

But the gcd belongs to $K[x]$ (by Euclid's algorithm) so if $f(x)$ has a repeated root in some field extension then either $f'(x) = 0$ (identically) or else $f(x)$ is *reducible*, with a factor dividing $f'(x)$. In particular, every irreducible polynomial with coefficients in a field of characteristic zero is separable. Thus all such fields are perfect.

Finite fields are also perfect although they support (reducible) polynomials with $f'(x) = 0$. If F is a finite field and $\alpha \in L$ for an extension $F \subset L$, then either $K(\alpha)$ is infinite, in which case α is transcendental over K, or else $K(\alpha) \subset \mathbb{F}_q$ for some field with q elements. But the elements of $\mathbb{F}_q$ are precisely the (distinct!) q roots of $x^q - x$, so the irreducible polynomial $f(x)$ with $f(\alpha) = 0$ must be a factor of $x^q - x$, and as such it has distinct roots (and its derivative is not zero).

On the other hand, the field $\mathbb{F}_p(t)$ is not perfect since the polynomial:

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

is irreducible and a pth power, when thought of as a polynomial in $\mathbb{F}_p(t^{\frac{1}{p}})[x]$.

Let $f(x) \in K[x]$.

Definition. A *splitting field* F/K for $f(x)$ is a splitting extension that is minimal, in the sense that there is no intermediate splitting extension $K \subset E \subset F$.

Note: There is a unique splitting field $F := K(\alpha_1, ..., \alpha_r)$ inside each splitting extension L, namely the smallest subextension that contains all the roots $\alpha_i \in L$.

By induction and Proposition 1 from the previous section,

$$K[x_1, ..., x_r] \to K(\alpha_1, ..., \alpha_r) \subset L$$

is a surjection from the polynomial ring onto the splitting field.

Definition. The *Galois group* of a splitting field F/K (for some $f(x) \in K[x]$) is:

$$\mathrm{Gal}(F/K) = \mathrm{Aut}_K(F)$$

the group of automorphisms of the field F that restrict to the identity on K.

We want to prove that this group is determined (up to isomorphism) by the polynomial $f(x)$ itself, and not just by the splitting field. Instead of comparing two splitting fields F_1/K and F_2/K for the same field K, it useful to think of them as splitting fields over isomorphic but distinct fields K_1 and K_2.

Proposition 1. Let $\tau : K_1 \to K_2$ be an isomorphism of fields and let

$$\widetilde{\tau} : K_1[x] \to K_2[x] \ \text{ be defined by } \ \widetilde{\tau}\left(\sum a_i x^i\right) = \sum \tau(a_i) x^i$$

Fix $f(x) \in K_1[x]$ and let F_1/K_1 and F_2/K_2 be splitting fields for f and $\widetilde{\tau}(f)$. Then:

(a) There is an isomorphism $\sigma : F_1 \to F_2$ such that $\sigma|_{K_1} = \tau$.

(b) If $f(x)$ is separable, there are $[F_1 : K_1]$ isomorphisms in (a). In particular:

$$|\mathrm{Gal}(F/K)| = [F : K]$$

for every splitting field of a separable polynomial $f(x) \in K[x]$.

(c) The Galois groups of the various splitting fields of an arbitrary $f(x) \in K[x]$ are all isomorphic to one another.

Proof. If $f(x)$ splits in K_1 then $\widetilde{\tau}(f)(x)$ splits in K_2, and $F_1 = K_1$ and $F_2 = K_2$ and there is nothing to prove in (a) or (b). Otherwise choose an irreducible factor $g(x)$ of $f(x)$ of degree > 1 and a root $\alpha_1 \in F_1$ of $g(x)$.

For each root $\beta \in F_2$ of $\widetilde{\tau}(g)(x)$, we obtain an extension of τ to:

$$\tau_\beta : K_1(\alpha_1) \to K_2(\beta) \subset F_2 \text{ defined by } \tau_\beta(\alpha_1) = \beta$$

an isomorphism of fields $K_1(\alpha_1)$ and $K(\beta)$. If $f_1(x)$ is separable, then there are:

$$[K_1(\alpha_1) : K_1] = \deg(g)$$

such maps to F_2 corresponding to the distinct roots of $\widetilde{\tau}(g)$.

For each choice of β (giving rise to τ_β) , we repeat the process with K_1 replaced with $K_1(\alpha_1)$ and K_2 replaced with $K_2(\beta)$ (and τ replaced with τ_β). Since

$$F_1 = K_1(\alpha_1, ..., \alpha_r)$$

for distinct roots α_i of a series of factors $g_i(x)$ with $\alpha_{i+1} \notin K(\alpha_1, ..., \alpha_i)$, we get (a) and (b) after r iterations, the point in (b) being that the isomorphism $\sigma : K(\alpha_1, ..., \alpha_r) \to F_2$ is uniquely determined by the images of $\alpha_1, ..., \alpha_r$.

As for (c), let F_1/K and F_2/K be two splitting fields for $f(x) \in K[x]$. Then the isomorphism σ guaranteed by (a) (and its inverse) may be used to define the isomorphism $\mathrm{Gal}(F_1/K)$ to $\mathrm{Gal}(F_2/K)$ by *conjugation*. Namely,

$$g \mapsto \sigma \circ g \circ \sigma^{-1}$$

defines the isomorphism of Galois groups with inverse defined by σ^{-1}. $\square$

Finite Fields

Corollary 1. Two finite fields with the same number of elements are isomorphic.

Proof. Let F be a field with q elements. By virtue of the fact that F^* is cyclic (of order $q-1$) it follows that $F/\mathbb{F}_p$ is a splitting field for $x^q - x$, which is a separable polynomial over the (fixed!) field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Now apply the Proposition.

Let $\mathbb{F}_q$ be "the" finite field with $q = p^d$ elements.

Corollary 2. The Galois group $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ is cyclic of order d, generated by:

$$\phi : \mathbb{F}_q \to \mathbb{F}_q \text{ defined by } \phi(\alpha) = \alpha^p$$

This is the *Frobenius element* of the Galois group.

Proof. The Frobenius element is an automorphism of $\mathbb{F}_q$ fixing $\mathbb{F}_q$ since:

$$\phi(a) = a \text{ for } a \in \mathbb{F}_p \quad \text{and} \quad \phi(\alpha\beta) = \phi(\alpha)\phi(\beta) \text{ and } \phi(\alpha+\beta) = \phi(\alpha) + \phi(\beta)$$

the last being the surprising result, following from the fact that:

$$(\alpha+\beta)^p = \alpha^p + \beta^p \text{ in } \textbf{any} \text{ field of characteristic } p$$

This element is not the identity (unless $d = 1$), and indeed,

$$\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p) = \{\phi, \cdots, \phi^{d-1}, \phi^d = \mathrm{id}_{\mathbb{F}_q}\} = C_d$$

with $\phi^d(\alpha) = \alpha^{p^d} = \alpha^q = \alpha$ for all $\alpha \in \mathbb{F}_q$ giving $\phi^d = \mathrm{id}$.

Notice that if e divides d, then:

$$\mathbb{F}_{p^e} = \{\alpha \in \mathbb{F}_q \mid \phi^e(\alpha) = \alpha^{p^e} = \alpha\} \subset \mathbb{F}_q$$

is the "fixed subfield" of the subgroup of the Galois group generated by ϕ^e.

This gives us a correspondence between the subgroups of the Galois group C_d and the subfields of $\mathbb{F}_q$. Moreover, notice that all the subgroups are normal and all the subfields of $\mathbb{F}_q$ are splitting fields of some polynomial in $\mathbb{F}_p[x]$. This is our first encounter with Galois Theory.

Cyclotomic Fields

Let $\omega_n = e^{2\pi i/n}$. Then $\mathbb{Q}(\omega_n)/\mathbb{Q}$ is a splitting field for $x^n - 1$, and so

$$\mathrm{Gal}(\mathbb{Q}(\omega_n)/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^* \text{ via } \omega_n \mapsto \omega_n^d$$

is once again an abelian group (though not necessarily cyclic), and then:

Corollary 3. The irreducible polynomial $\Phi_n(x) \in \mathbb{Q}[x]$ for ω_n has degree $\phi(n)$.

This is the *nth cyclotomic polynomial.*

Note. This $\phi(n)$ (surely the most overused greek letter in math) is the Euler totient, which is the size of the Galois group, hence also equal to $[\mathbb{Q}(\omega_n) : \mathbb{Q}] = \deg(\Phi_n(x))$.

Examples. For all primes p, the cyclotomic polynomial is: $\Phi_p(x) = (x^p - 1)/(x-1)$

$\Phi_4(x) = x^2 + 1$

$\Phi_6(x) = x^2 - x + 1$

$\Phi_8(x) = x^4 + 1$

$\Phi_9(x) = x^6 + x^3 + 1$

$\Phi_{12}(x) = x^4 - x^2 + 1$

Remark. The product formula $\prod_{d|n} \Phi_d(x) = x^n - 1$ for cyclotomic polynomials reprises the sum (taking degrees):

$$\sum_{d|n} \phi(d) = n \text{ that we saw earlier}$$

Let's explore some of these splitting fields $\mathbb{Q}(\omega_n)$ in more detail:

• $(\mathbb{Z}/8\mathbb{Z})^* = \{1, 3, 5, 7\}$ is isomorphic to K_4 and has three subgroups of order 2. Not coincidentally, there are three intermediate subfields:

$$\mathbb{Q} \subset E_i \subset \mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{i}), \text{ namely}$$

$E_1 = \mathbb{Q}(i) = \mathbb{Q}(\omega^2)$, $E_2 = \mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\omega + \omega^{-1})$ and $E_3 = \mathbb{Q}(\sqrt{-2}) = \mathbb{Q}(\omega - \omega^{-1})$ which are fixed subfields for the elements $\omega \mapsto \omega^5, \omega^7$ and ω^3 respectively!

- $(\mathbb{Z}/5\mathbb{Z})^* = C_4$, on the other hand, has only has one subgroup, and

$$\mathbb{Q}(\sqrt{5}) = \mathbb{Q}(\omega + \omega^{-1}) \subset \mathbb{Q}(\omega)$$

is the fixed field for $\omega \mapsto \omega^4$. The polynomial relation: $(\omega+\omega^4)^2 + (\omega+\omega^4) - 1 = 0$ gives us another computation of

$$\omega + \omega^{-1} = 2\cos(2\pi/5) = \frac{-1+\sqrt{5}}{2}$$

- $(\mathbb{Z}/7\mathbb{Z})^* = C_6$ has two subgroups C_2 and C_3, and

$$E_1 = \mathbb{Q}(\omega + \omega^{-1}) \text{ and } E_2 = \mathbb{Q}(\omega + \omega^2 + \omega^4)$$

are the subfields fixed by $\omega \mapsto \omega^6$ and $\omega \mapsto \omega^2$, respectively. Note that $\omega + \omega^2 + \omega^4$ is a root of $x^2 + x + 2 = 0$, giving us:

$$\omega + \omega^2 + \omega^4 = \frac{-1+\sqrt{-7}}{2} \text{ and } E_2 = \mathbb{Q}(\sqrt{-7})$$

while $\omega + \omega^6$ is a root of $x^3 + x^2 - 2x - 1 = 0$, so this irreducible cubic polynomial relation satisfied by $2\cos(2\pi/7)$ shows that $2\cos(2\pi/7)$ is not constructible.

We have a final corollary that is half of the cornerstone of Galois Theory.

Corollary 4. Fix a splitting field F/K for a polynomial $f(x) \subset K[x]$. Then:

(a) F/E is a splitting field of $f(x)$ for each intermediate field $K \subset E \subset F$, and:

$$\mathrm{Gal}(F/E) \subset \mathrm{Gal}(F/K)$$

is a subgroup whose right cosets are in bijection with the set $\mathrm{Hom}_K(E, F)$.

(b) If E/K is a splitting field for $g(x) \in K[x]$, then each element of the Galois group $\mathrm{Gal}(F/K)$ fixes the subfield $E \subset F$, giving rise to an exact sequence:

$$1 \to \mathrm{Gal}(F/E) \to \mathrm{Gal}(F/K) \to \mathrm{Gal}(E/K) \to 1$$

of Galois groups. In particular, $\mathrm{Gal}(F/E) \subset \mathrm{Gal}(F/K)$ is a normal subgroup.

Proof. It is clear that F/E is a splitting field for $f(x)$. The inclusion of Galois groups in (a) (and (b)) follows right away from the definition of the Galois group. After all, an automorphism of F fixing E must also fix K. Suppose $\iota : E \to F$ is a field embedding that fixes K. Let $\tau : E \to \iota(E)$ be the isomorphism. Then by Proposition 1 (a), τ lifts to an element $\sigma \in \mathrm{Gal}(F/K)$. Moreover, the cosets

$$\sigma \circ \mathrm{Gal}(F/E) \subset \mathrm{Gal}(F/K) \text{ are all the lifts of } \tau$$

This gives (a).

When E/K is a splitting field of $g(x) \in K[x]$ in (b), then E is mapped to E by every element of $\mathrm{Gal}(F/K)$ since the roots of $g(x)$ map to roots of $g(x)$, and the resulting group homomorphism $\mathrm{Gal}(F/K) \to \mathrm{Gal}(E/K)$ is surjective by (a). $\square$

nth Roots

Recall that every positive integer $b \in \mathbb{Z}$ has a full set of n complex nth roots. That is,

$$\mathbb{Q} \subset \mathbb{C} \text{ is a splitting extension for the polynomial } f(x) = x^n - b$$

and we let $F/\mathbb{Q}$ be the splitting field of $\mathbb{Q}$ for $x^n - b$ contained in $\mathbb{C}$. We seek to understand the Galois group of this splitting field.

Notice that $\omega_n \in F$ is a ratio of nth roots of b, and so:

$$\mathbb{Q}(\omega_n) \subset F, \text{ and indeed } F = \mathbb{Q}(\omega_n, \sqrt[n]{b})$$

where $\sqrt[n]{b}$ is the positive real nth root of b (this is the only reason we chose $b > 0$). This *might* seem to say everything we need to know about the splitting field $F/\mathbb{Q}$. But there's actually more work to be done. Since $\mathbb{Q}(\omega_n)/\mathbb{Q}$ is also a splitting field (for the cyclotomic polynomial), we get an exact sequence:

$$(*) \quad 1 \to \text{Gal}(F/\mathbb{Q}(\omega_n)) \to \text{Gal}(F/\mathbb{Q}) \to \text{Gal}(\mathbb{Q}(\omega_n)/\mathbb{Q}) \to 1$$

of Galois groups by Corollary 4. Moreover, this sequence is right-split via:

$$h : |(\mathbb{Z}/n\mathbb{Z})^*| = \text{Gal}(\mathbb{Q}(\omega_n)/\mathbb{Q}) \to \text{Gal}(F/\mathbb{Q}); \ h_d(\omega) = \omega^d \text{ and } h_d(\sqrt[n]{b}) = \sqrt[n]{b}$$

which only leaves us the problem of figuring out the Galois group of the splitting field $F/\mathbb{Q}(\omega_n) = \mathbb{Q}(\omega_n)(\sqrt[n]{b})/\mathbb{Q}(\omega_n)$ (and the details of the semidirect product).

This is contingent, of course, on the values of n and b. For example, if b is already a perfect nth power as an integer, then all the nth roots of b are already in $\mathbb{Q}(\omega_n)$, and h is an isomorphism. At the other extreme:

Case One. If $x^n - b$ remains irreducible in $\mathbb{Q}(\omega_n)[x]$, there must be an element $g \in \text{Gal}(F/\mathbb{Q}(\omega_n))$ with the property that

$$g(\sqrt[n]{b}) = (\sqrt[n]{b}) \cdot \omega_n$$

from which it follows (by the invariance of $\mathbb{Q}(\omega_n)$) that the effect of g on all roots is to rotate by an angle of $2\pi/n$. But

$$|\text{Gal}(F/\mathbb{Q}(\omega_n))| = [F : \mathbb{Q}(\omega_n)] = n$$

from the Proposition, and so the Galois group is the cyclic group, generated by g. Thus, the exact sequence $(*)$ is:

$$1 \to C_n \to \text{Gal}(F/\mathbb{Q}) \to \text{Aut}(C_n) \to 1$$

and the semi-direct product is "canonical" via $\phi = \text{id} : \text{Aut}(C_n) \to \text{Aut}(C_n)$ since:

$$h_d \circ g \circ h_d^{-1} = g^d \text{ is rotation of the roots by } 2\pi d/n$$

When $n = 3$, this gives S_3, and when $n = 5$, it is the "mystery" group of order 20.

Case Two. $x^n - b$ is irreducible in $\mathbb{Q}[x]$ (but might be reducible in $\mathbb{Q}(\omega_n)[x]$). Then the n cosets of the inclusion of Galois groups:

$$\text{Gal}(F/\mathbb{Q}(\sqrt[n]{b})) \subset \text{Gal}(F/\mathbb{Q})$$

from Corollary 4 correspond to the n different embeddings $\mathbb{Q}(\sqrt[n]{b}) \hookrightarrow F$.

In particular, $|\text{Gal}(F/\mathbb{Q})|$ is divisible by n. When $n = p$, this is enough to conclude that $x^p - b$ is also irreducible in $\mathbb{Q}(\omega_n)[x]$, and so we are in case one. But when n is not a prime, or more precisely, when n and $\phi(n)$ are not relatively prime, it is possible for $x^n - b$ to factor in $\mathbb{Q}(\omega_n)[x]$, in which case we can only conclude:

$$(\dagger) \ 1 \to G \to \text{Gal}(F/\mathbb{Q}) \to \text{Aut}(C_n) \to 1$$

for a group G that is the Galois group of the splitting field of an irreducible factor $g(x)$ of $f(x) = x^n - b \in \mathbb{Q}(\omega_n)[x]$, and such that:

$$n \text{ divides } |\text{Gal}(F/\mathbb{Q})| = |G| \cdot \phi(n) = \deg(g(x)) \cdot \phi(n)$$

Example. Consider the irreducible polynomial $x^8 - 2 \in \mathbb{Q}[x]$. We claim that:

$$x^8 - 2 \text{ is reducible in } \mathbb{Q}(\omega_8)[x]$$

We can see this from the subfield $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\omega_8 + \omega_8^{-1})$, showing that indeed:

$$x^8 - 2 = (x^4 + \sqrt{2})(x^4 - \sqrt{2}) \in \mathbb{Q}(\omega_8)[x]$$

and ω_8 is a root of the first of these polynomials. But could it factor any further? One way to see it doesn't is to apply Eisenstein's criterion with the Euclidean domain $D = \mathbb{Z}[\sqrt{2}]$, in which $\sqrt{2}$ is an irreducible element.

Thus the Galois group has order 16, and reasoning as in Case One gives us:

$$g(\sqrt[8]{2}) = (\sqrt[8]{2}) \cdot \omega_8^2 = (\sqrt[8]{2}) \cdot i$$

in $G \subset \mathrm{Gal}(F/\mathbb{Q})$, showing that $G = \mathrm{Gal}(F/\mathbb{Q}(\omega_8))$ is the cyclic group C_4.

One could now analyze the semi-direct product in (†) to get the Galois group. We can also pass to the sub-splitting field $\mathbb{Q}(i) \subset F$, and use Corollary 4 to obtain:

$$(**)\ 1 \to \mathrm{Gal}(F/\mathbb{Q}(i)) \to \mathrm{Gal}(F/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) \to 1$$

This is right-split by complex conjugation $c \in \mathrm{Gal}(F/\mathbb{Q})$, and in addition,

$$|\mathrm{Gal}(F/\mathbb{Q}(i))| = 16/2 = 8$$

so $x^8 - 2$ is irreducible in $\mathbb{Q}(i)[x]$. This Galois group is also cyclic, but is **not** generated by the rotation by ω_8 (since that would be an element of G). Instead, it "has to be" a lift of the element $\omega \mapsto \omega^5$ from the Galois group of $\mathbb{Q}(\omega_8)/\mathbb{Q}(i)$. I.e.

$$\gamma(\sqrt[8]{2}) = (\sqrt[8]{2}) \cdot \omega \text{ and } \gamma(\omega) = \omega^5 (= -\omega)$$

Then

$$c \circ \gamma \circ c^{-1} = \gamma^3$$

as one is invited to check, and in particular, $\mathrm{Gal}(F/\mathbb{Q})$ is **not** dihedral group!

Miscellaneous

Let F/K be a splitting field for a separable polynomial $f(x) \in K[x]$ of degree d. Then:

Proposition 2. (a) The Galois group of F/K is a subgroup of S_d.

(b) If p is prime and $f(x)$ is irreducible, then $\mathrm{Gal}(F/K)$ contains a p-cycle.

Proof. The Galois group takes roots of $f(x)$ to roots of $f(x)$ and is completely determined by the image of the roots, giving (a). In (b), choose a root α of $f(x)$ in F. Then there are p cosets for the subgroup:

$$\mathrm{Gal}(F/K(\alpha)) \subset \mathrm{Gal}(F/K)$$

and so p divides the order $|\mathrm{Gal}(F/K)|$, and then by Cauchy's Theorem, there is an element of order p. Finally, the only elements of order p in S_p are the p-cycles. $\square$

Corollary 5. Supppose $f(x) \in \mathbb{Q}[x]$ is irreducible of prime degree p that splits in $\mathbb{C}[x]$ with exactly two complex roots. Then the Galois group of $F/\mathbb{Q}$ is S_p.

Remark. Every polynomial splits in $\mathbb{C}[x]$. This is the fundamental theorem of algebra, which you may have seen proved in a complex analysis class. We will also prove it using the intermediate value theorem and Galois theory in the next section.

Proof. By the Corollary, the Galois group $\text{Gal}(F/\mathbb{Q})$ contains a p-cycle which, without loss of generality, we write as $g = (1\ 2\ \cdots\ p) \in$. It also contains complex conjugation, which (via the single pair of complex roots) is a transposition $(i\ j)$. But then this this transposition (repeatedly) by the p-cycle gives:

$$(1\ d), (d\ 2d), ..., ((p-2)d\ (p-1)d) \in \text{Gal}(F/\mathbb{Q}) \subset S_p \text{ for } d = |j-i|+1$$

and these generate the full symmetric group. □

The reader is invited to find polynomials of degree 5 that satisfy this criterion. In particular, notice that the Galois group is not solvable for these polynomials.

Suppose instead that $f(x)$ has four complex roots. Then:

$$g = (1\ 2\ \cdots\ p) \in\ \text{Gal}(F/\mathbb{Q}),\ \text{and}\ c = (i\ j)(k\ l) \in \text{Gal}(F/\mathbb{Q})$$

are both elements of the alternating group. However this shows neither that the Galois group is contained in the alternating group A_p nor that it contains the alternating group. For example, when:

$$f(x) = x^5 - b$$

we've seen that the Galois group has order 20 (and contains a 4-cycle).

The *inverse Galois problem* asks whether every finite group is the Galois group of a splitting field $F/\mathbb{Q}$ of some (irreducible) polynomial $f(x)$. As far as I know, this is still open. However, it makes sense to ask for some examples.

Cyclic Galois Groups (of odd prime order). These need to come from irreducible polynomials $f(x)$ of degree p (since the degree divides the order of the Galois group), all of whose roots are real (otherwise complex conjugation would add elements of order two). But if $\alpha_1, ..., \alpha_d \in F$ are the roots of a polynomial $f(x)$, then:

$$\prod_{i<j} (\alpha_j - \alpha_i) \in F$$

and the square of this is the *discriminant* $\Delta(f)$, which is a polynomial in the coefficients of f (hence in $\mathbb{Q}$). Thus, if $\Delta(f) \in \mathbb{Q}$ is not a perfect square, then:

$$\mathbb{Q}(\sqrt{\Delta(f)}) \subset F$$

and the Galois group $\text{Gal}(F/K)$ is divisible by two (hence not cyclic of order p).

For example among polynomials of degree three with no quadratic term, we have:

$$f(x) = x^3 + px + q \text{ and } \Delta(f) = -4p^3 - 27q^2$$

Can $\Delta(f)$ be a perfect square while $f(x)$ remains irreducible? Sure. For example:

$$f(x) = x^3 - 7x + 6 \text{ has discriminant } \Delta(f) = 400 = 20^2$$

and it is certainly irreducible by Eisenstein (or the roots test). And this works!

Alternatively, one might look at the cyclotomic polynomial:

$$\Phi_{p^2}(x) \text{ with Galois group } |(\mathbb{Z}/p^2\mathbb{Z})^*| = C_{(p-1)p} = C_{p-1} \times C_p$$

and prove the existence of splitting sub-field $E \subset \mathbb{Q}(\omega_{p^2})$ with $\text{Gal}(F/E) = C_{p-1}$ which will imply that:

$$\text{Gal}(E/\mathbb{Q}) = C_{(p-1)p}/C_{p-1} = C_p$$

We'll see how to do this in the next section.